Acronis®
COMPUTE WITH CONFIDENCE
WWW.ACRONIS.ES

# Acronis® Backup & Recovery ™ 10 Advanced Workstation

Update 5

## Guía del usuario

# Contenido


**1 Introducción de Acronis® Backup & Recovery™ 10 ..... 7**

1.1 Generalidades de Acronis Backup & Recovery 10 ..... 7

1.2 Cómo empezar ..... 8

1.2.1 Uso de la consola de gestión ..... 10

1.3 Componentes de Acronis Backup & Recovery 10 ..... 17

1.3.1 Agente para Windows ..... 18

1.3.2 Componentes para una gestión centralizada ..... 19

1.3.3 Management Console ..... 22

1.3.4 Generador de dispositivos de inicio ..... 22

1.3.5 Acronis WOL Proxy ..... 22

1.4 Sistemas de archivos compatibles ..... 23

1.5 Sistemas operativos compatibles ..... 23

1.6 Requisitos del sistema ..... 25

1.7 Soporte técnico ..... 26

**2 Comprensión de Acronis Backup & Recovery 10 ..... 27**

2.1 Conceptos básicos ..... 27

2.2 Copias de seguridad completas, incrementales y diferenciales ..... 31

2.3 Privilegios de usuario en un equipo administrado ..... 33

2.4 Propietarios y credenciales ..... 33

2.5 Esquema GFS de copia de seguridad ..... 35

2.6 Esquema de copias de seguridad Torres de Hanói ..... 39

2.7 Reglas de retención ..... 42

2.8 Realización de copias de seguridad de volúmenes dinámicos (Windows) ..... 44

2.9 Soporte de cintas ..... 47

2.9.1 Tabla de compatibilidad de cintas ..... 47

2.9.2 Uso de una sola unidad de cinta ..... 48

2.10 Compatibilidad con SNMP ..... 49

2.11 Tecnologías propias de Acronis ..... 50

2.11.1 Acronis Secure Zone ..... 50

2.11.2 Acronis Startup Recovery Manager ..... 51

2.11.3 Universal Restore (Acronis Backup & Recovery 10 Universal Restore) ..... 52

2.11.4 Acronis Active Restore ..... 53

2.12 Comprensión de la gestión centralizada ..... 55

2.12.1 Conceptos básicos ..... 55

2.12.2 Configurar la protección de datos centralizada en una red heterogénea ..... 57

2.12.3 Agrupar los equipos registrados ..... 60

2.12.4 Políticas sobre equipos y grupos ..... 61

2.12.5 Estado y estatus de la política de copias de seguridad ..... 65

2.12.6 Deduplicación ..... 69

2.12.7 Privilegios para la gestión centralizada ..... 73

2.12.8 Comunicación entre los componentes de Acronis Backup & Recovery 10 ..... 78

**3 Opciones ..... 85**

3.1 Opciones de Consola ..... 85

3.1.1 Página de inicio ... 85
3.1.2 Mensajes emergentes ... 85
3.1.3 Alertas según el momento ... 86
3.1.4 Cantidad de tareas ... 86
3.1.5 Fuentes ... 87
3.2 Opciones de Management Server ... 87
3.2.1 Nivel de registro ... 87
3.2.2 Reglas de limpieza de los registros ... 87
3.2.3 Seguimiento de sucesos ... 88
3.2.4 Credenciales de acceso al dominio ... 89
3.2.5 Acronis WOL Proxy ... 89
3.2.6 Opciones de protección de las máquinas virtuales ... 90
3.2.7 Proxy de copia de seguridad en línea ... 91
3.3 Opciones del equipo ... 91
3.3.1 Gestión del equipo ... 91
3.3.2 Seguimiento de sucesos ... 92
3.3.3 Reglas de limpieza de los registros ... 94
3.3.4 Proxy de copia de seguridad en línea ... 95
3.3.5 Programa de Experiencia del Cliente ... 95
3.4 Opciones predeterminadas de copia de seguridad y recuperación ... 96
3.4.1 Opciones de copia de seguridad predeterminadas ... 96
3.4.2 Opciones predeterminadas de recuperación ... 121
**4 Bóvedas ... 130**
4.1 Bóvedas centralizadas ... 131
4.1.1 Cómo trabajar con la vista "Bóveda centralizada" ... 132
4.1.2 Acciones en bóvedas centralizadas ... 133
4.1.3 Bibliotecas de cintas ... 139
4.2 Bóvedas personales ... 165
4.2.1 Cómo trabajar con la vista "Bóveda personal" ... 166
4.2.2 Acciones en bóvedas personales ... 167
4.3 Operaciones comunes ... 169
4.3.1 Operaciones con archivos comprimidos almacenados en una bóveda ... 169
4.3.2 Operaciones con copias de seguridad ... 169
4.3.3 Eliminación de archivos comprimidos y copias de seguridad ... 171
4.3.4 Filtrado y ordenamiento de archivos comprimidos ... 171
**5 Programación ... 173**
5.1 Programación diaria ... 174
5.2 Programación semanal ... 176
5.3 Programación mensual ... 178
5.4 Configuraciones de programación avanzadas ... 181
5.5 Al producirse un evento del Registro de sucesos de Windows ... 182
5.6 Cuando se produzca una alerta de Acronis Drive Monitor ... 184
5.7 Condiciones ... 185
5.7.1 El usuario está inactivo ... 186
5.7.2 El servidor de ubicación no está disponible ... 186
5.7.3 Coincidir con intervalo ... 187
5.7.4 El usuario cerró la sesión ... 188
5.7.5 Tiempo transcurrido desde la última copia de seguridad ... 188

**6 Gestión directa ..... 190**
6.1 Administrar un equipo gestionado ..... 190
6.1.1 Tablero ..... 190
6.1.2 Planes y tareas de la copia de seguridad ..... 192
6.1.3 Registro ..... 204
6.2 Crear un plan de copias de seguridad ..... 207
6.2.1 ¿Por qué este programa me pide la contraseña? ..... 210
6.2.2 Credenciales del plan de copias de seguridad ..... 210
6.2.3 Tipo de fuente ..... 210
6.2.4 Elementos para incluir en la copia de seguridad ..... 211
6.2.5 Credenciales de acceso a los datos de origen ..... 212
6.2.6 Exclusiones ..... 213
6.2.7 Archivo comprimido ..... 214
6.2.8 Asignación simplificada de nombre a los archivos de copia de seguridad ..... 216
6.2.9 Credenciales de acceso para la ubicación del archivo comprimido ..... 221
6.2.10 Esquemas de copia de seguridad ..... 221
6.2.11 Validación de archivos comprimidos ..... 232
6.2.12 Configuración de una conversión normal a una máquina virtual ..... 232
6.3 Recuperación de datos ..... 234
6.3.1 Credenciales de la tarea ..... 236
6.3.2 Selección de archivos comprimidos ..... 237
6.3.3 Tipo de datos ..... 238
6.3.4 Selección del contenido ..... 238
6.3.5 Credenciales de acceso para la ubicación ..... 239
6.3.6 Selección del destino ..... 240
6.3.7 Credenciales de acceso para el destino ..... 248
6.3.8 Cuándo recuperar ..... 248
6.3.9 Universal Restore ..... 248
6.3.10 Cómo convertir una copia de seguridad del disco en un equipo virtual ..... 250
6.3.11 Solución de problemas de capacidad de inicio ..... 251
6.3.12 Recuperación del nodo de almacenamiento ..... 255
6.4 Validar bóvedas, archivos comprimidos y copias de seguridad ..... 255
6.4.1 Credenciales de la tarea ..... 257
6.4.2 Selección de archivos comprimidos ..... 257
6.4.3 Selección de la copia de seguridad ..... 258
6.4.4 Selección de la ubicación ..... 259
6.4.5 Credenciales de acceso para el origen ..... 259
6.4.6 Cuándo validar ..... 260
6.5 Montaje de una imagen ..... 260
6.5.1 Selección de archivos comprimidos ..... 261
6.5.2 Selección de la copia de seguridad ..... 262
6.5.3 Credenciales de acceso ..... 262
6.5.4 Selección de volúmenes ..... 263
6.6 Gestión de imágenes montadas ..... 263
6.7 Exportación de archivos comprimidos y copias de seguridad ..... 264
6.7.1 Credenciales de la tarea ..... 267
6.7.2 Selección de archivos comprimidos ..... 267
6.7.3 Selección de la copia de seguridad ..... 268
6.7.4 Credenciales de acceso para el origen ..... 269
6.7.5 Selección de la ubicación ..... 269
6.7.6 Credenciales de acceso para el destino ..... 271
6.8 Acronis Secure Zone ..... 271
6.8.1 Creación de Acronis Secure Zone ..... 271

6.8.2 Gestión de Acronis Secure Zone ... 274
6.9 Acronis Startup Recovery Manager ... 275
6.10 Dispositivo de arranque ... 276
6.10.1 Cómo crear dispositivos de inicio ... 277
6.10.2 Conexión a un equipo que se inició desde un dispositivo ... 285
6.10.3 Trabajo desde dispositivo de arranque ... 285
6.10.4 Lista de comandos y utilidades disponibles en los dispositivos de inicio basados en Linux ... 287
6.10.5 Recuperación de los dispositivos MD y los volúmenes lógicos ... 288
6.10.6 Acronis PXE Server ... 293
6.11 Gestión del disco ... 294
6.11.1 Precauciones posibles ... 295
6.11.2 Ejecución de Acronis Disk Director Lite ... 295
6.11.3 Elección del sistema operativo para la gestión de discos ... 296
6.11.4 Vista "Administración del disco" ... 296
6.11.5 Operaciones del disco ... 297
6.11.6 Operaciones del volumen ... 304
6.11.7 Operaciones pendientes ... 311
6.12 Recolección de información del sistema ... 311
**7 Gestión centralizada ... 313**
7.1 Administración de Acronis Backup & Recovery 10 Management Server ... 313
7.1.1 Tablero ... 313
7.1.2 Políticas de copia de seguridad ... 315
7.1.3 Equipos físicos ... 321
7.1.4 Máquinas Virtuales ... 338
7.1.5 Nodos de almacenamiento ... 343
7.1.6 Tareas ... 347
7.1.7 Registro ... 349
7.1.8 Generación de informes ... 353
7.2 Configuración de los componentes de Acronis Backup & Recovery 10 ... 359
7.2.1 Parámetros establecidos a través de la plantilla administrativa ... 360
7.2.2 Parámetros configurados a través de la GUI ... 375
7.2.3 Parámetros establecidos a través del registro de Windows ... 375
7.3 Creación de una política de copias de seguridad ... 377
7.3.1 Credenciales de la política ... 379
7.3.2 Elementos de los cuales realizará la copia de seguridad ... 380
7.3.3 Credenciales de acceso al origen ... 385
7.3.4 Exclusiones ... 386
7.3.5 Archivo comprimido ... 387
7.3.6 Credenciales de acceso a la ubicación ... 388
7.3.7 Selección del esquema de copia de seguridad ... 389
7.3.8 Validación de archivos comprimidos ... 399
**8 Glosario ... 400**

# 1 Introducción de Acronis® Backup & Recovery™ 10

## 1.1 Generalidades de Acronis Backup & Recovery 10

Basado en la imagen de disco y las tecnologías de restauración completa patentadas de Acronis, Acronis Backup & Recovery 10 es el sucesor de Acronis True Image Echo como la solución de recuperación de catástrofes de la próxima generación.

**Acronis Backup & Recovery 10 Advanced Workstation hereda los beneficios de la familia de productos de Acronis True Image Echo:**

- Copia de seguridad de un disco o volumen entero, incluyendo el sistema operativo, todas las aplicaciones y datos.
- Recuperación completa de cualquier hardware.
- Copia de seguridad y recuperación de archivos y carpetas.
- Escalabilidad desde un único equipo a una empresa.
- Gestión centralizada para estaciones de trabajo distribuida.
- Servidores dedicados para la optimización de recursos de almacenamiento.

**Acronis Backup & Recovery 10 Advanced Workstation ofrece nuevos beneficios que ayudan a las organizaciones a cumplir con los objetivos de tiempo de recuperación desafiantes mientras reducen tanto el coste de capital como el coste de mantenimiento del software.**

- **Aprovechamiento de la infraestructura de TI existente**

  Desduplicación de datos para reducir el consumo de almacenamiento y la utilización del ancho de banda de la red.

  Mecanismo de desduplicación flexible que permite la desduplicación de datos de la copia de seguridad en el origen y en el almacenamiento.

  Asistencia mejorada para las bibliotecas robotizadas de cintas.

  Totalmente compatible y fácil de actualizar desde Acronis True Image Echo.

- **Protección de datos altamente automatizada**

  Planificación completa de la protección de datos (copia de seguridad, retención y validación de copias de seguridad) dentro de una política de copias de seguridad.

  Esquemas de copia de seguridad Torres de Hanói y Abuelo-Padre-Hijo incorporados con parámetros adaptables.

  Se puede escoger entre una variedad de eventos y condiciones para dar inicio a una copia de seguridad.

- **Gestión centralizada basada en políticas**

  Aplicar políticas de copias de seguridad a los grupos de equipos.

  Agrupación estática y dinámica de equipos.

- **Funcionamiento fácil en entornos virtuales**

  Conversión de una copia de seguridad a un equipo virtual VMware, Microsoft, Parallels, Citrix o Red Hat KVM completamente configurado.

- **Interfaz gráfica de usuario rediseñada**

  Tablero de control para una rápida toma de decisiones operativas.

  Generalidades de todas las operaciones configuradas y ejecutándose, con codificación por color para operaciones correctas y con fallos.
- **Nivel de seguridad corporativo**

  Control de los permisos de usuarios para llevar a cabo operaciones y acceder a las copias de seguridad.

  Ejecución de servicios con permisos de usuario mínimos.

  Acceso remoto restringido a un agente de copia de seguridad.

  Comunicación segura entre los componentes del producto.

  Uso de certificados de terceros para la autenticación de los components.

  Opciones de cifrado de datos para la transmisión y el almacenamiento de datos.

  Copia de seguridad de equipos remotos a un nodo de almacenamiento centralizado detrás de los cortafuegos.

## 1.2 Cómo empezar

### Gestión directa

1. Instale Acronis Backup & Recovery 10 Management Console y Acronis Backup & Recovery 10 Agente.
2. Inicio de la consola.

   **Windows**

   Inicie la consola seleccionándola desde el menú de inicio.
3. Conecte la consola al equipo en el que está instalado el agente.

**A dónde ir desde aquí**

Para saber cuál es el próximo paso consulte "Conceptos básicos (pág. 27)".

Para comprender los elementos de la GUI consulte "Uso de la consola de gestión (pág. 10)".

### Gestión centralizada

Recomendamos que primero intente gestionar un solo equipo utilizando la gestión directa como se describió anteriormente.

***Para iniciar con la gestión centralizada:***

1. Instale Acronis Backup & Recovery 10 Management Server (pág. 19).
2. Instale Acronis Backup & Recovery 10 Agents en los equipos que requieren protección de datos. Al instalar los agentes, registre cada uno de los equipos en el servidor de gestión. Para hacerlo, introduzca la IP o el nombre del servidor y las credenciales del administrador centralizado en una de las ventanas del asistente para la instalación.
3. Instale Acronis Backup & Recovery 10 Management Console (pág. 22) en el equipo desde el que prefiere operar. Recomendamos que utilice la consola que se instala en Windows si puede elegir entre distribuciones de consola de Windows y Linux. Instale Acronis Bootable Media Builder.
4. Inicio de la consola. Cree el dispositivo de inicio.
5. Conecte la consola en el servidor de gestión.

**El método simplificado de gestión centralizada**

- **Crear copia de seguridad**

Uso del control **Copia de seguridad**, seleccione el equipo del que quiere realizar una copia de seguridad y cree un plan de copia de seguridad (pág. 411) en el mismo. Puede crear planes de copia de seguridad en varios equipos a la vez.

- **Recuperación**

Uso del control **Recuperar**, seleccione el equipo del que se deben recuperar los datos y cree una tarea de recuperación en el mismo. Puede crear tareas de recuperación en varios equipos a la vez.

Para recuperar el equipo entero o el sistema operativo que no puede iniciarse, utilice los dispositivos de inicio (pág. 410). No puede controlar las operaciones con dispositivos de inicio utilizando el servidor de gestión pero puede desconectar la consola del servidor y conectarla al equipo que se ha iniciado desde el dispositivo.

- **Gestión de planes y tareas de la copia de seguridad**

Para gestionar los planes y tareas que se encuentran en los equipos registrados, seleccione **Equipos > Todos los equipos** en el árbol de **Navegación** y después seleccione cada equipo en orden. El panel de **Información** mostrado a continuación muestra el estado y los detalles de los planes y tareas que se encuentran en cada equipo y le permite iniciarlos, detenerlos, editarlos y eliminarlos.

También puede utilizar la vista **Tareas** que muestra todas las tareas que hay en los equipos registrados. Las tareas se pueden filtrar por equipos, planes de copia de seguridad y otros parámetros. Para obtener más detalles, consulte la ayuda interactiva.

- **Vista Registro**

Para ver el registro centralizado, recopilado de los equipos registrados, seleccione **Registro** en el árbol de **Navegación**. Las entradas del registro se pueden filtrar por equipos, planes de copia de seguridad y otros parámetros. Para obtener más detalles, consulte la ayuda interactiva.

- **Creación de bóvedas centralizadas**

Si opta por almacenar todos los archivos comprimidos de copia de seguridad en una única o en unas pocas ubicaciones de red, cree bóvedas centralizadas en estas ubicaciones. Una vez que se ha creado una bóveda, puede ver y administrar su contenido seleccionando **Bóvedas > Centralizadas > "Nombre de la bóveda"** en el árbol de **Navegación**. El acceso directo a la bóveda se implementará en todos los equipos registrados. La bóveda se puede especificar como un destino de la copia de seguridad en cualquier plan de copia de seguridad que usted o los usuarios de los equipos registrados hayan creado.

**El método avanzado de gestión centralizada**

Para maximizar el uso de las capacidades de gestión centralizada que ofrece Acronis Backup & Recovery 10, puede elegir:

- **Uso de la desduplicación**
  1. Instale Acronis Backup & Recovery 10 Storage Node (pág. 20) y añádalo al servidor de gestión.
  2. Cree la bóveda gestionada de desduplicación en el nodo de almacenamiento.
  3. Instale el complemento Acronis Deduplication en el agente de todos los equipos que contendrán copias de seguridad de la bóveda de deduplicación.
  4. Asegúrese de que los planes de copia de seguridad que cree utilizan la bóveda gestionada como destino de sus archivos comprimidos de copia de seguridad.

- **Creación de una política de copias de seguridad en lugar de planes de copia de seguridad**

Configure una política de copias de seguridad centralizada y aplíquela al grupo **Todos los equipos**. Así implementará planes de copia de seguridad en todos los equipos con una única acción. Seleccione **Acciones > Crear política** de copias de seguridad desde el menú superior y después consulte la ayuda interactiva.

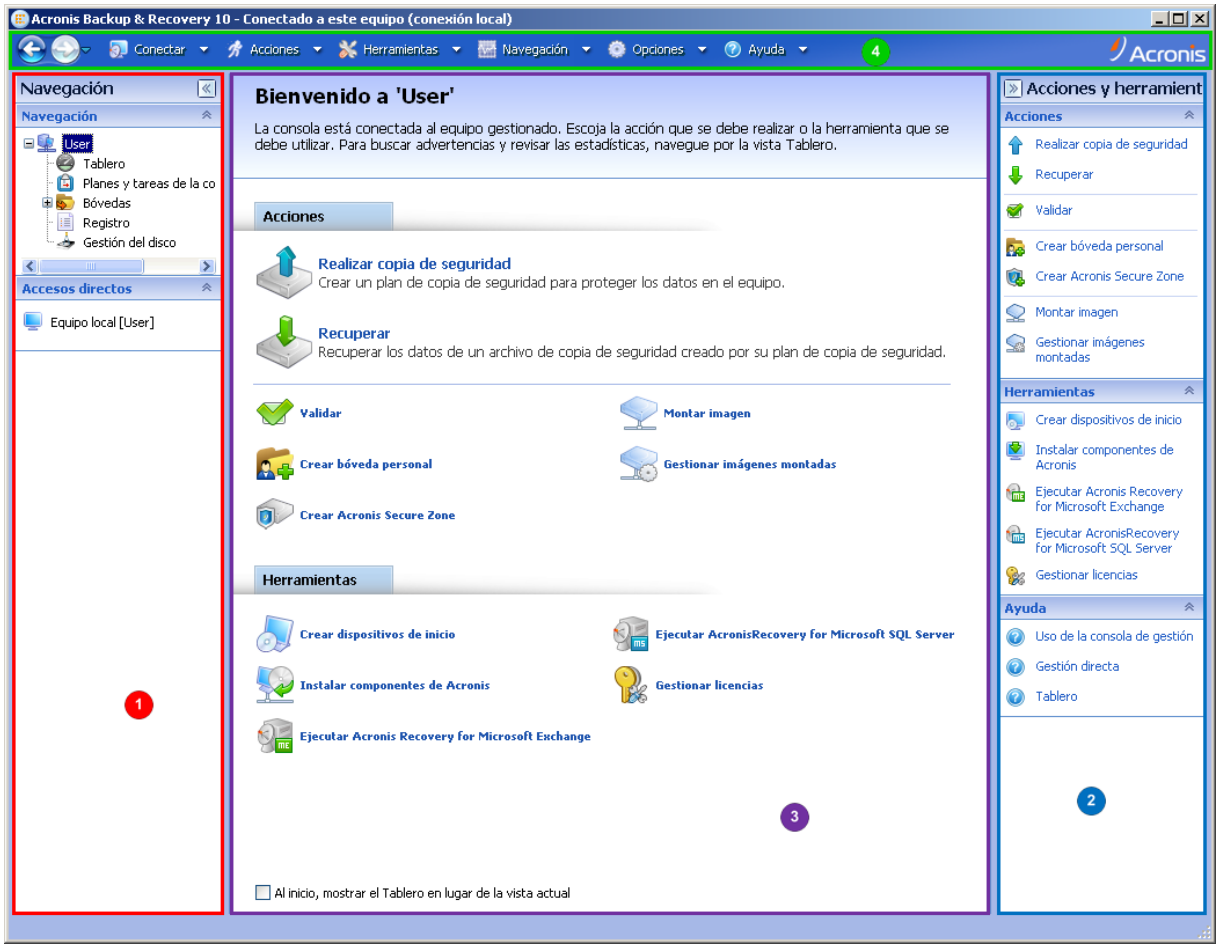
- **Agrupación de los equipos registrados en el servidor de gestión**

Agrupe los equipos registrados con parámetros apropiados, cree varias políticas y aplique cada política al grupo de equipos correspondiente. Para obtener más información, consulte "Agrupación de los equipos registrados (pág. 60)".

El ejemplo completo de la gestión centralizada avanzada se proporciona en la sección "Configuración de protección de datos centralizada en una red heterogénea (pág. 57)".

### 1.2.1 Uso de la consola de gestión

En cuanto se conecta la consola a un equipo gestionado (pág. 405) o a un servidor de gestión (pág. 409), los elementos correspondientes aparecen en el espacio de trabajo de la consola (en el menú, en el área principal con la pantalla de **Bienvenida**, el panel de **Navegación**, el panel de **Acciones y herramientas**) permitiéndole llevar a cabo operaciones específicas del agente o del servidor.




**Acronis Backup & Recovery 10 Management Console: Pantalla de Bienvenida**

**Elementos clave del espacio de trabajo de la consola**

| | Nombre | Descripción |
|---|---|---|
| 1 | Panel de **Navegación** | Contiene el árbol de **Navegación** y la barra de **Accesos directos** y le permite navegar por las diferentes vistas (consulte la sección Panel de navegación (pág. 11)). |
| 2 | Panel **Acciones y herramientas** | Contiene barras con un conjunto de acciones que pueden llevarse a cabo y herramientas (consulte la sección Panel acciones y herramientas (pág. 12)). |
| 3 | Área **principal** | El espacio de trabajo principal, donde puede crear, editar y gestionar planes, políticas y tareas de copia de seguridad y llevar a cabo otras operaciones. Muestra las diferentes vistas y páginas de acción (pág. 14) de acuerdo con los elementos seleccionados en el menú, el árbol de **Navegación** o el panel **Acciones y herramientas**. |
| 4 | Barra de **menú** | Aparece en la parte superior de la ventana del programa y le permite llevar a cabo todas las operaciones disponibles en ambos paneles. Los elementos del menú cambian de forma dinámica. |

Es necesario tener una resolución de 1024x768 o mayor para trabajar de forma cómoda con la consola de gestión.

## Panel de "Navegación"

El panel de navegación incluye el árbol de **Navegación** y la barra de **Accesos directos**.

### Árbol de navegación

El árbol de **Navegación** le permite navegar por las vistas de los programas. Las vistas dependen de si la consola está conectada a un equipo gestionado o al servidor de gestión.

### Vistas para un equipo gestionado

Cuando la consola está conectada a un equipo gestionado, las siguientes vistas están disponibles en el árbol de navegación.

- **[Nombre del equipo]**. Raíz del árbol, también llamada vista **Bienvenida**. Muestra el nombre del equipo al cual está conectada la consola en ese momento. Utilice esta vista para tener un acceso rápido a las operaciones principales, disponibles en el equipo gestionado.
  - **Tablero de control**. Utilice esta vista para calcular rápidamente si los datos están protegidos correctamente en el equipo gestionado.
  - **Planes y tareas de la copia de seguridad**. Utilice esta vista para gestionar planes y tareas de la copia de seguridad en el equipo gestionado: ejecutar, editar, detener y eliminar planes y tareas, ver sus estados y estatus, supervisar planes.
  - **Bóvedas**. Utilice esta vista para gestionar bóvedas personales y los archivos comprimidos almacenados en ellas, añadir nuevas bóvedas, renombrar y eliminar las ya existentes, validar bóvedas, explorar el contenido de las copias de seguridad, montar copias de seguridad como unidades virtuales, etc.
  - **Registro**. Utilice esta vista para examinar la información sobre operaciones llevadas a cabo por el programa en el equipo gestionado.
  - **Gestión del disco**. Utilice esta vista para llevar a cabo operaciones sobre las unidades de disco duro del equipo.

### Vistas para un servidor de gestión

Cuando la consola está conectada a un servidor de gestión, las siguientes vistas están disponibles en el árbol de navegación.

- **[Nombre del servidor de gestión]**. Raíz del árbol, también llamada vista **Bienvenida**. Muestra el nombre del servidor de gestión al cual está conectada la consola en ese momento. Utilice esta vista para tener un acceso rápido a las operaciones principales, disponibles en el servidor de gestión.
  - **Tablero de control**. Utilice esta vista para calcular rápidamente si los datos están protegidos correctamente en los equipos registrados del servidor de gestión.
  - **Políticas de copia de seguridad**. Utilice esta vista para gestionar las políticas de copia de seguridad existentes en el servidor de gestión.
  - **Equipos físicos**. Utilice esta vista para gestionar los equipos registrados en el servidor de gestión.
  - **Bóvedas**. Utilice esta vista para gestionar bóvedas centralizadas y los archivos comprimidos almacenados en ellas: crear nuevas bóvedas gestionadas y sin gestionar, renombrar y eliminar las ya existentes.
  - **Nodos de almacenamiento**. Utilice esta vista para gestionar los nodos de almacenamiento. Añada un nodo de almacenamiento para poder crear bóvedas centralizadas que serán gestionadas por el nodo.
  - **Tareas**. Utilice esta vista para gestionar las tareas, ejecutarlas, editarlas, detenerlas y eliminarlas, supervisar sus estados, examinar sus historiales.
  - **Registro**. Utilice esta vista para examinar el historial de operaciones de gestión centralizada como, por ejemplo, la creación de un grupo de entidades gestionadas, la aplicación de una política, la gestión de una bóveda centralizada, así como el historial de operaciones recopiladas en los registros locales de los equipos registrados y los nodos de almacenamiento.

### Barra de accesos directos

La barra de **Accesos directos** aparece debajo del árbol de navegación. La misma le brinda un método fácil y conveniente para conectarse con los equipos solicitados añadiéndolos a los accesos rápidos.

#### *Para añadir un acceso rápido a un equipo*

1. Conecte la consola a un equipo gestionado.
2. En el árbol de navegación, haga clic con el botón derecho en el nombre del equipo (un elemento raíz del árbol de navegación) y después seleccione **Crear acceso directo**.

   Si la consola y el agente se instalan en el mismo equipo, el acceso directo a este equipo se añadirá a la barra de accesos directos automáticamente como **Equipo local [Nombre del equipo]**.

   Si la consola ya se ha conectado alguna vez a Acronis Management Server, el acceso directo se añade automáticamente como **[Nombre del equipo] AMS**.

## Panel "Acciones y herramientas"

El panel **Acciones y herramientas** le permite trabajar fácil y eficazmente con Acronis Backup & Recovery 10. Las barras del panel proporcionan un acceso rápido a las operaciones y herramientas de los programas. Todos los elementos de la barra de **Acciones y herramientas** están duplicados en el menú del programa.

## Barras

### Acciones de "[nombre del elemento]"

Contiene un conjunto de acciones que pueden llevarse a cabo sobre los elementos seleccionados en cualquiera de las vistas de navegación. Al hacer clic en la acción se abre la página de acción (pág. 16) correspondiente. Los elementos de las diferentes vistas de navegación tienen su propio conjunto de acciones. El nombre de la barra cambia de acuerdo con el elemento que se selecciona. Por ejemplo, si selecciona el plan de copia de seguridad denominado *Copia de seguridad del sistema* en la vista **Planes y tareas de la copia de seguridad**, la barra de acciones se denominará **Acciones de la "copia de seguridad del sistema"** y contendrá el conjunto de acciones típico de los planes de copia de seguridad.

También es posible acceder a todas las acciones a través de los elementos del menú correspondientes. Un elemento del menú aparece en la barra de menú cuando se selecciona un elemento en cualquiera de las vistas de navegación.


**Ejemplos de barras de "acciones de 'nombre del elemento'"**

### Acciones

Contiene una lista de operaciones comunes que se pueden llevar a cabo en un equipo gestionado o en un servidor de gestión. Siempre las mismas para todas las vistas. Al hacer clic en la operación se abre la página de acción correspondiente (consulte la sección Páginas de acción (pág. 16)).

También es posible acceder a todas las acciones a través del menú **Acciones**.


**Barra de "Acciones" en un equipo gestionado y en un servidor de gestión**

### Herramientas

Contiene una lista de las herramientas de Acronis. Siempre la misma en todas las vistas de los programas.

También es posible acceder a todas las herramientas a través del menú **Herramientas**.


**Barra de "Herramientas"**

### Ayuda

Contiene una lista de los temas de ayuda. Diferentes vistas y páginas de acción de Acronis Backup & Recovery 10 proporcionadas con listas de temas de ayuda específicos.

## Operaciones con paneles

### *Cómo expandir/minimizar paneles*

De manera predeterminada, el panel de **Navegación** aparece expandido y el de **Acciones y herramientas** minimizado. Es posible que tenga que minimizar el panel para liberar un poco de espacio de trabajo adicional. Para esto, haga clic en la flecha tipo (  , para el panel de **Navegación**;  , para el panel **Acciones y herramientas**). El panel se minimizará y la flecha tipo cambiará su dirección. Haga clic en la flecha tipo nuevamente para expandir el panel.

### *Cómo cambiar los bordes de los paneles*

1. Posicione el ratón sobre el borde del panel.
2. Cuando el puntero se transforme en una flecha de dos puntas, arrástrelo para mover el borde.

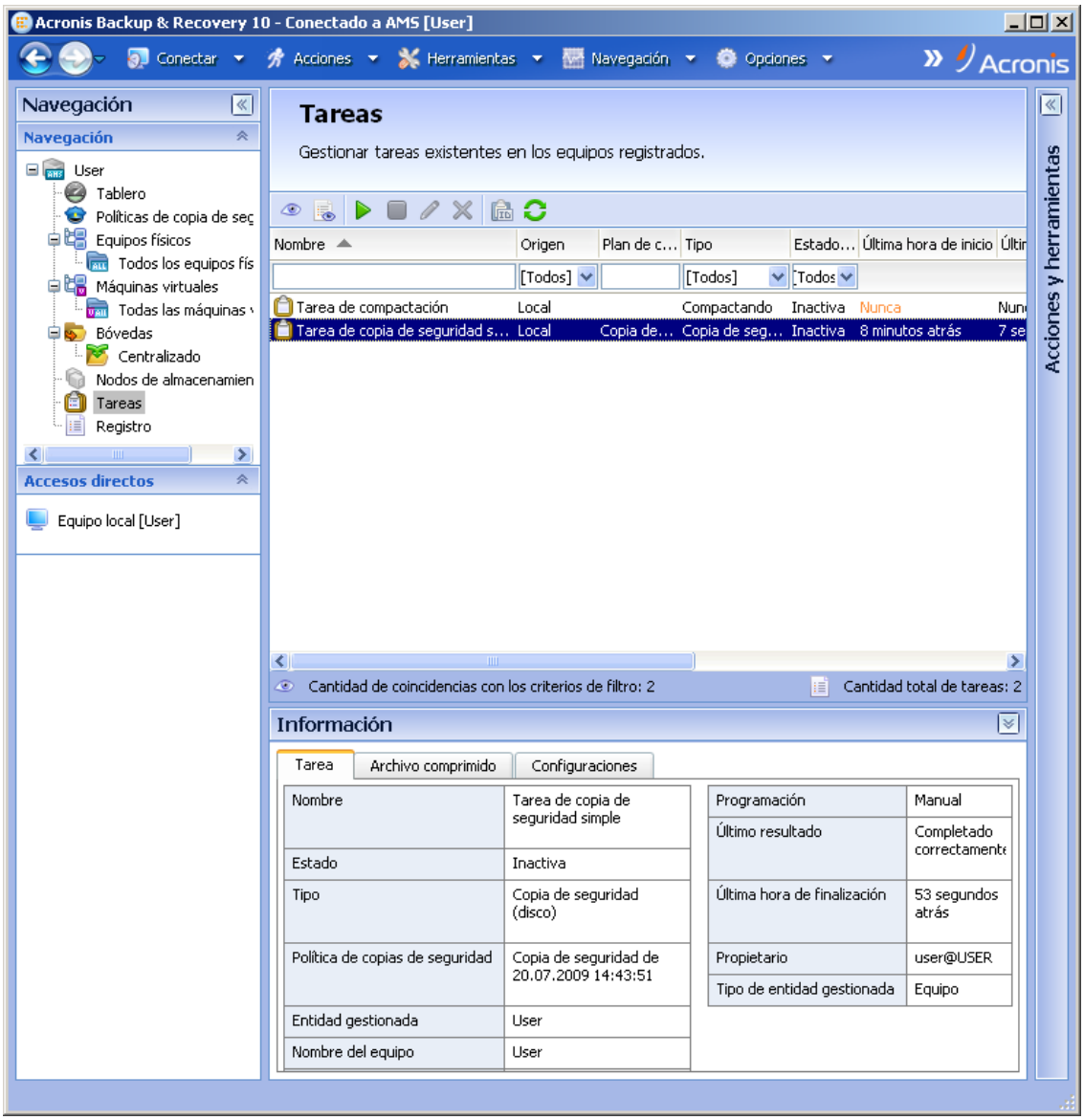
La consola de gestión "recuerda" cómo se configura los bordes de los paneles. La próxima vez que ejecute la consola de gestión, todos los bordes de los paneles estarán en la misma posición que se había configurado previamente.

## Área principal, vistas y páginas de acción

El área principal es un sitio básico en el que trabajará con la consola. Aquí se crean, editan y administran los planes, políticas, tareas de respaldo del sistema y se realizan otras operaciones. El área principal muestra vistas y páginas de acciones diversas de acuerdo con los elementos que selecciona en el menú y, en el árbol de **Navegación**, o en el panel de **Acciones y Herramientas.**

## Vistas

Una vista aparece en el área principal al hacer clic en cualquier elemento del árbol de **Navegación** del Panel de navegación (pág. 11).




**Vista "Tareas"**

### La manera más común de trabajar con las vistas

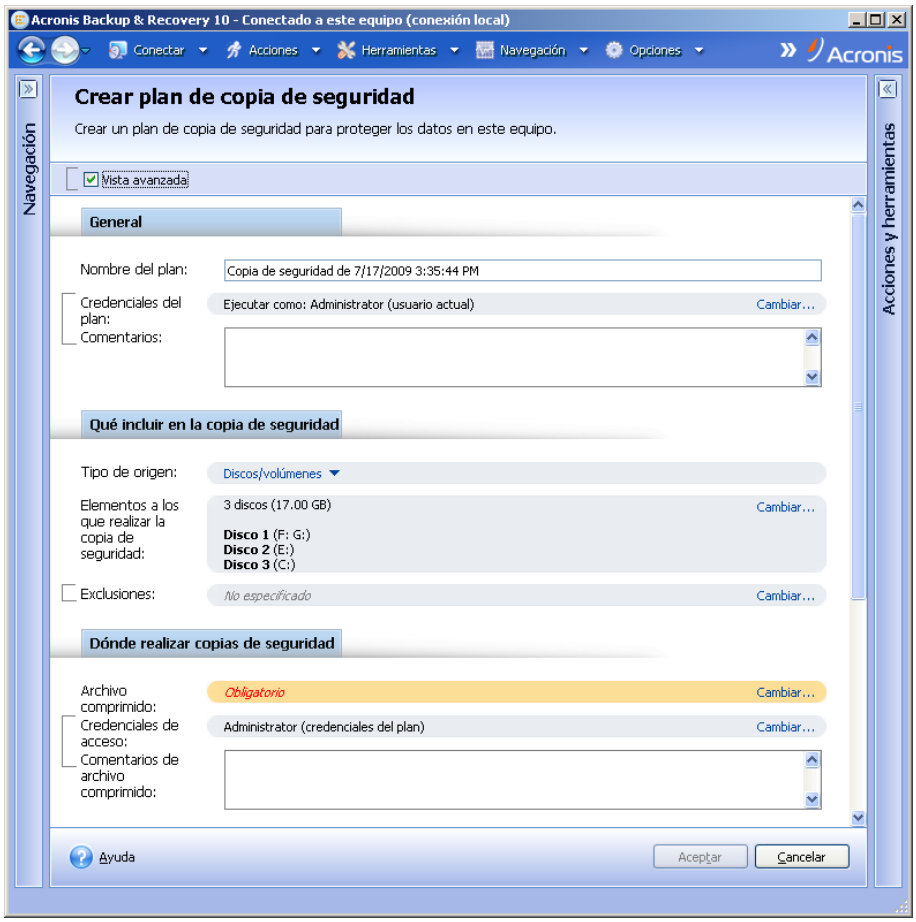
En general, cada vista contiene una tabla de elementos, una barra de herramientas con botones y el panel **Información**.

- Utilice las capacidades de filtro y organización para buscar el elemento en cuestión dentro de la tabla
- En la tabla, seleccione el elemento deseado
- En el panel **Información** (minimizado de manera predeterminada), vea los detalles del elemento
- Lleve a cabo acciones sobre el elemento seleccionado. Hay varias formas de llevar a cabo la misma acción en diferentes elementos seleccionados:
  - Al hacer clic en los botones de la barra de tareas,
  - Al hacer clic en los elementos de la barra de **Acciones** de **[Nombre del elemento]** (en el panel **Acciones y herramientas**),
  - Al seleccionar los elementos en el menú **Acciones**,

- Al hacer clic con el botón derecho en el elemento y seleccionar la operación en el menú contextual.

## Páginas de acción

En el área principal aparece una página de acción al hacer clic en un elemento de cualquiera de las acciones del menú **Acciones** o de la barra de **Acciones** del panel de **Acciones y herramientas**. La misma contiene los pasos que hay que llevar a cabo para crear e iniciar cualquier tarea, plan de copia de seguridad o política de copias de seguridad.

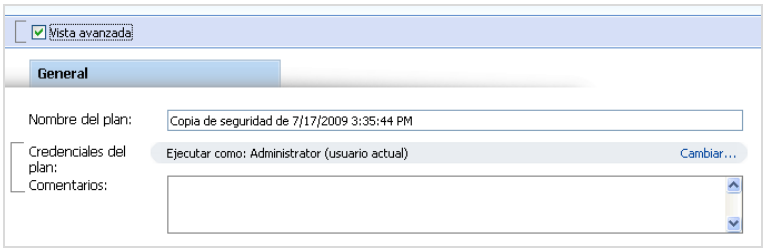



**Página de acción: Crear plan de copia de seguridad**

### Uso de controles y especificación de configuraciones

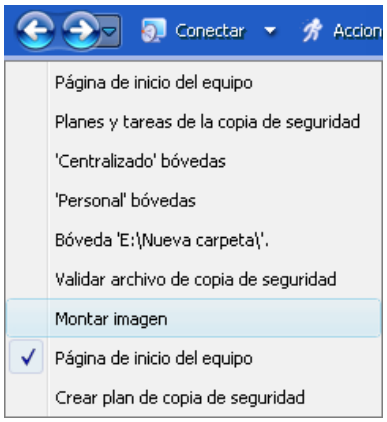
Las páginas de acción ofrecen dos formas de representación: básica y avanzada. La representación básica esconde campos como credenciales, comentarios, etc. Cuando se habilita la representación avanzada, se muestran todos los campos disponibles. Puede intercambiar las vistas seleccionando la casilla de verificación **Vista avanzada** en la parte superior de la página de acción.

La mayoría de las configuraciones se configuran haciendo clic en los enlaces **Cambiar…** que se encuentran a la derecha. Otros se seleccionan en la lista desplegable o se escriben manualmente en los campos de la página.




**Página de acción: Controles**

Acronis Backup & Recovery 10 recuerda los cambios que se hacen en las páginas de acción. Por ejemplo, si empezase a crear un plan de copias de seguridad y luego por cualquier motivo cambiase a otra vista sin completar la creación del plan, puede hacer clic en el botón de navegación **Atrás** del menú. O, si ha avanzado algunos pasos, haga clic en la flecha **Abajo** y seleccione de la lista la página en donde empezó la creación del plan. Por lo tanto, puede llevar a cabo los pasos que faltan y completar la creación del plan de copia de seguridad.




**Botones de navegación**

## 1.3 Componentes de Acronis Backup & Recovery 10

Esta sección contiene una lista de los componentes de Acronis Backup & Recovery 10 con una descripción breve de su funcionalidad.

Acronis Backup & Recovery 10 incluye tres tipos principales de componentes.

### Componentes para un equipo gestionado (agentes)

Estas aplicaciones realizan copias de seguridad, recuperación y otras operaciones con los datos de los equipos gestionados con Acronis Backup & Recovery 10. Los agentes deben tener una licencia para llevar a cabo operaciones en cada equipo gestionado. Los agentes tienen múltiples funciones o complementos que permiten una funcionalidad adicional y por lo tanto pueden requerir licencias adicionales.

Con el generador de dispositivos de inicio, puede crear dispositivos de inicio para utilizar los agentes y otras utilidades de rescate en un entorno de rescate. La disponibilidad de los complementos del agente en un entorno de rescate depende de si el complemento está instalado en el equipo en donde el generador de dispositivos está funcionando.

### Componentes para una gestión centralizada

Estos componentes, que se entregan con las ediciones avanzadas, brindan la capacidad de gestión centralizada. No se requieren licencias para el uso de estos componentes.

### Consola

La consola proporciona la Interfaz gráfica del usuario y la conexión remota con los agentes y otros componentes de Acronis Backup & Recovery 10.

## 1.3.1 Agente para Windows

Este agente permite la protección de datos de nivel de disco y de nivel de archivos con Windows.

### Copia de seguridad del disco

La protección de datos de nivel de disco se basa en la realización de copias de seguridad de un disco o de un sistema de archivos de un volumen en conjunto, junto con toda la información necesaria para que el sistema operativo se inicie, o todos los sectores del disco que utilicen el enfoque sector por sector (modo sin procesar). Una copia de seguridad que contiene una copia de un disco o un volumen en una forma compacta se denomina una copia de seguridad de disco (volumen) o una imagen de disco (volumen). Es posible recuperar discos o volúmenes de forma completa a partir de estas copias de seguridad, así como carpetas o archivos individuales.

### Copia de seguridad del archivo

La protección de datos de nivel de archivos se basa en la realización de copias de seguridad de archivos y carpetas que se encuentran en el equipo en el que está instalado el agente o en una red compartida. Los archivos se pueden recuperar en su ubicación original o en otro lugar. Es posible recuperar todos los archivos y carpetas con los que se realizó la copia de seguridad o seleccionar cuál de ellos recuperar.

### Otras operaciones

#### Conversión a máquina virtual

Más que convertir una copia de seguridad de disco a un archivo de disco virtual, lo cual requiere operaciones adicionales para volver utilizable el disco virtual, el Agente para Windows realiza la conversión recuperando una copia de seguridad de disco a una nueva máquina virtual de uno de los siguientes tipos: VMware Workstation, Microsoft Virtual PC, Parallels Workstation o Citrix XenServer Open Virtual Appliance (OVA). Los archivos del equipo ya completamente configurado y funcional se colocarán en la carpeta que usted seleccione. Puede iniciar el equipo con el correspondiente software de virtualización o preparar los archivos del equipo para otros usos.

#### Gestión del disco

El Agente para Windows incluye Acronis Disk Director Lite - una utilidad de gestión de disco muy manejable. Las operaciones de gestión de disco, como clonación de discos, conversión de discos; creación, formateo y eliminación de volúmenes; modificación del estilo de partición de un disco entre MBR y GPT o de la etiqueta del disco; pueden realizarse tanto en el sistema operativo como utilizando un dispositivo de inicio.

### Universal Restore

El complemento Universal Restore le permite utilizar la restauración para funcionalidad de hardware diferentes en el equipo en el que está instalado el agente y crear dispositivos de inicio con esta

funcionalidad. Universal Restore controla las diferencias en los dispositivos que son críticos para el inicio de Windows como, por ejemplo, controladores de almacenamiento, placa madre o conjunto de chips.

### Deduplicación

Este complemento le permite al agente realizar copias de seguridad de datos en bóvedas de desduplicación gestionadas por Acronis Backup & Recovery 10 Storage Node.

## 1.3.2 Componentes para una gestión centralizada

Esta sección enumera los componentes que se incluyen en las ediciones Acronis Backup & Recovery 10 que brindan la capacidad de gestión centralizada. Además de estos componentes, los agentes de Acronis Backup & Recovery 10 deben instalarse en todos los equipos que requieren protección de datos.

### Management Server

Acronis Backup & Recovery 10 Management Server es el servidor central que gestiona la protección de datos dentro de la red empresarial. El servidor de gestión proporciona al administrador lo siguiente:

- Un único punto de acceso a la infraestructura de Acronis Backup & Recovery 10
- Una manera fácil de proteger los datos en varios equipos (pág. 405) con políticas de copia de seguridad (pág. 412) y agrupación
- Funcionalidad de supervisión y generación de informes en toda la empresa
- La capacidad de crear bóvedas centralizadas (pág. 402) para guardar los archivos comprimidos de copias de seguridad (pág. 401) de la empresa.
- La capacidad de gestionar los nodos de almacenamiento (pág. 410).

Si hay varios servidores de gestión en la red, funcionan independientemente, gestionan diferentes equipos y utilizan las bóvedas centralizadas para almacenamiento de archivos comprimidos.

#### Las bases de datos del servidor de gestión

El servidor de gestión utiliza tres bases de datos de Microsoft SQL:

- La base de datos de configuración, que almacena la lista de equipos registrados y demás información de configuración, incluyendo las políticas de copia de seguridad creadas por el administrador.
- La base de datos de sincronización, que se utiliza para la sincronización del servidor de gestión con equipos registrados y nodos de almacenamiento. Esta base de datos incluye datos operativos que cambian frecuentemente.
- La base de datos de informes, que almacena el registro centralizado. Esta base de datos puede llegar a tener un tamaño importante. El mismo dependerá del nivel de registro que configure.

Las bases de datos de configuración y sincronización deben encontrarse en el mismo Microsoft SQL Server (denominado servidor operativo), que debe estar instalado preferentemente en el mismo equipo que el servidor de gestión. La base de datos de informes se puede configurar en el mismo servidor SQL o en uno diferente.

Al instalar un servidor de gestión, es posible seleccionar qué servidor utilizar tanto para el servidor operativo como para el de informes. Las siguientes opciones están disponibles:

1. Microsoft SQL Server 2005 Express, que está incluido en el paquete de instalación y se instala en el mismo equipo. En este caso, se creará una instancia de servidor SQL con tres bases de datos en el equipo.
2. Microsoft SQL Server 2008 (cualquier edición), instalado previamente en cualquier equipo.
3. Microsoft SQL Server 2005 (cualquier edición), instalado previamente en cualquier equipo.

### Integración de VMware vCenter

Esta función proporciona la capacidad de ver equipos virtuales gestionados por un VMware vCenter Server en la interfaz gráfica de usuario del servidor de gestión, ver el estado de la copia de seguridad de dichos equipos en el vCenter y registrar automáticamente los equipos virtuales creados por Acronis Backup & Recovery 10 en el vCenter.

La integración está disponible en todas las ediciones avanzadas de Acronis Backup & Recovery 10; no se necesita una licencia para Virtual Edition. No se necesita ninguna instalación de software en el vCenter Server.

Esta función también permite una implementación y configuración automáticas de Agent para ESX/ESXi en cualquier servidor ESX/ESXi gestionado o no por el vCenter.

## Nodo de almacenamiento

Acronis Backup & Recovery 10 Storage Node es un servidor que permite optimizar el uso de diversos recursos (como, por ejemplo, la capacidad de almacenamiento corporativo, el ancho de banda de la red o la carga de la CPU de los equipos gestionados) necesarios para la protección de datos de la empresa. Este objetivo se consigue gracias a la organización y la gestión de ubicaciones que funcionan como almacenamientos dedicados de los archivos comprimidos de copia de seguridad de la empresa (bóvedas gestionadas).

Los nodos de almacenamiento permiten crear una infraestructura de almacenamiento muy escalable y flexible, en términos de compatibilidad con el hardware. Se pueden configurar hasta 20 nodos de almacenamiento y cada uno puede gestionar hasta 20 bóvedas. El administrador controla los nodos de almacenamiento de forma central desde Acronis Backup & Recovery 10 Management Server (pág. 409). No es posible establecer una conexión directa entre la consola y un nodo de almacenamiento.

### Configuración de la infraestructura de almacenamiento

Instale los nodos de almacenamiento, añádalos al servidor de gestión (el procedimiento es similar al del registro (pág. 412) del equipo gestionado) y cree bóvedas centralizadas (pág. 402). Al crear una bóveda centralizada, especifique la ruta a la bóveda, el nodo de almacenamiento que gestionará la bóveda y las operaciones de gestión que deben llevarse a cabo en la bóveda.

Se puede organizar una bóveda gestionada:

- en unidades del disco duro locales al nodo de almacenamiento
- en una red compartida
- en una Red de área de almacenamiento (SAN)
- en un Almacenamiento conectado a la red (NAS)
- en una biblioteca de cintas conectada de forma local al nodo de almacenamiento.

Las operaciones de gestión son las siguientes.

### Limpieza y validación del lado del nodo de almacenamiento

Los archivos comprimidos, almacenados en bóvedas sin gestionar, se mantienen por los agentes (pág. 400) que los crean. Esto significa que cada agente no solo realiza copias de seguridad de datos en los archivos comprimidos, sino que también ejecuta tareas de servicio que se aplican al archivo comprimido, basándose en las reglas de retención y validación que especifica el plan de copia de seguridad (pág. 411). Para evitar la carga innecesaria de la CPU de los equipos gestionados, se puede delegar la ejecución de las tareas de servicio al nodo de almacenamiento. Como la programación de tareas se encuentra en el equipo en el que está ubicado el agente y que por lo tanto utiliza las fechas y eventos de ese equipo, el agente tiene que iniciar la limpieza del lado del nodo de almacenamiento (pág. 409) y la validación del lado del nodo de almacenamiento (pág. 414) de acuerdo con la programación. Para hacerlo, el agente debe estar en línea. Los procesos posteriores se llevan a cabo mediante el nodo de almacenamiento.

Esta funcionalidad no puede desactivarse en una bóveda de seguridad. Las próximas dos operaciones son opcionales.

### Deduplicación

Una bóveda gestionada se puede configurar como una bóveda de desduplicación. Esto significa que se realizará sólo una copia de seguridad de los datos idénticos en esta bóveda para minimizar el uso del espacio que ocupan las copias de seguridad y el almacenamiento de los archivos comprimidos en la red. Por mayor información, consulte la sección "Desduplicación (pág. 69)" de la Guía para el Usuario.

### Cifrado

Una bóveda gestionada se puede configurar para que el nodo de almacenamiento cifre todo lo que se escribe en ella y descifre todo lo que se lee de ella de forma transparente, utilizando una clave de cifrado específica de la bóveda almacenada en el servidor del nodo. En caso de que una persona no autorizada robe el dispositivo de almacenamiento o acceda al mismo, no podrá descifrar los contenidos de la bóveda si no tiene acceso a este nodo de almacenamiento en específico.

Si el agente ya ha cifrado el archivo comprimido, el cifrado del lado del nodo de almacenamiento se aplica sobre el cifrado realizado por el agente.

## Servidor PXE

Acronis PXE Server permite iniciar equipos mediante los componentes de inicio de Acronis a través de la red.

El inicio en red:

- Elimina la necesidad de un técnico en situ para instalar el dispositivo de inicio (pág. 410) en el sistema que debe iniciarse.
- Durante las operaciones de los grupos, reduce el tiempo necesario para el inicio de múltiples equipos en comparación con el uso de dispositivos de inicio.

## Servidor de licencias

El servidor le permite gestionar licencias de los productos Acronis e instalar los componentes que requieren licencias.

Para obtener más información acerca de Acronis License Server, consulte "Uso de Acronis License Server".

### 1.3.3 Management Console

Acronis Backup & Recovery 10 Management Console es una herramienta administrativa para el acceso local o remoto a los agentes Acronis Backup & Recovery 10 y, en las ediciones de productos que incluyen la capacidad de gestión centralizada, al Acronis Backup & Recovery 10 Management Server.

La consola tiene dos distribuciones para la instalación en Windows y en Linux. Si bien ambas distribuciones permiten la conexión con cualquier agente Acronis Backup & Recovery 10 y Acronis Backup & Recovery 10 Management Server, recomendamos que utilice la consola para Windows si puede elegir entre las dos. La consola que se instala en Linux tiene una funcionalidad limitada:

- la instalación remota de los componentes de Acronis Backup & Recovery 10no está disponible
- las funciones relacionadas con Active Directory como, por ejemplo, la exploración de AD, no están disponibles.

### 1.3.4 Generador de dispositivos de inicio

El generador de dispositivos de inicio de Acronis es una herramienta dedicada para la creación de dispositivos de inicio (pág. 410). El generador de dispositivos que se instala en Windows puede crear dispositivos de inicio basados tanto en el entorno de preinstalación de Windows como en el núcleo de Linux.

El complemento Universal Restore (pág. 18) le permite crear dispositivos de inicio con la funcionalidad de restauración en hardware diferente. Universal Restore controla las diferencias en los dispositivos que son críticos para el inicio de Windows como, por ejemplo, controladores de almacenamiento, placa madre o conjunto de chips.

El complemento Deduplicación (pág. 19) le permite crear dispositivos de inicio con la copia de seguridad en la funcionalidad de bóveda de deduplicación.

### 1.3.5 Acronis WOL Proxy

Esta opción también funciona combinada con la configuración avanzada de programación **Utilizar Wake-On-LAN** (pág. 181). Utilice esta opción si el management server debe activarse para realizar copias de seguridad de equipos ubicados en otra subred.

Cuando la operación programada está a punto de comenzar, el management server envía paquetes mágicos para activar los equipos adecuados. (un paquete mágico es un paquete que contiene 16 copias contiguas de la dirección MAC de la tarjeta NIC receptora). El Acronis WOL Proxy, instalado en otra subred, transfiere los paquetes a los equipos ubicados en esa subred.

El valor predeterminado: **Deshabilitado**.

***Para utilizar esta opción:***

1. Instale Acronis WOL Proxy en cualquier servidor de la subred donde se encuentren los equipos que se deben activar. El servidor debe proporcionar disponibilidad de servicios continuos. Con múltiples subredes, instale Acronis WOL Proxy en cada subred donde necesite utilizar la funcionalidad de Wake-On-LAN.
2. Habilite el **Acronis WOL Proxy** en las **Opciones de management server** de la siguiente manera:
   a. Seleccione la casilla de verificación **Utilizar los siguientes proxies**.

b. Haga clic en **Añadir** y luego introduzca el nombre o la dirección IP del equipo donde el Acronis WOL Proxy está instalado. Proporcione las credenciales de acceso para el equipo.

c. Repita este paso si hay varios Acronis WOL Proxies.

3. Al programar una política de copias de seguridad, habilite la configuración **Utilizar Wake-On-LAN**.

También tiene la capacidad para eliminar proxys de la lista. Tenga en cuenta que cualquier cambio en esta opción afecta al management server completo. Si elimina un proxy de la lista, la funcionalidad Wake-On-LAN en la subred correspondiente se deshabilitará para todas las políticas, incluyendo las políticas ya aplicadas.

## 1.4 Sistemas de archivos compatibles

Acronis Backup & Recovery 10 puede realizar copias de seguridad y recuperar los siguientes sistemas de archivos con las siguientes limitaciones:

- FAT16/32.
- NTFS.
- Ext2/Ext3/Ext4.
- ReiserFS3: los archivos específicos no se pueden recuperar de las copias de seguridad del disco ubicadas en Acronis Backup & Recovery 10 Storage Node.
- ReiserFS4: recuperación del volumen sin la capacidad de cambiar el tamaño del mismo, los archivos específicos no se pueden recuperar de las copias de seguridad del disco ubicadas en Acronis Backup & Recovery 10 Storage Node.
- XFS: recuperación del volumen sin la capacidad de cambiar el tamaño del mismo, los archivos específicos no se pueden recuperar de las copias de seguridad del disco ubicadas en Acronis Backup & Recovery 10 Storage Node.
- JFS: los archivos específicos no se pueden recuperar de las copias de seguridad del disco ubicadas en el nodo de almacenamiento Acronis Backup & Recovery 10.
- Linux SWAP.

Acronis Backup & Recovery 10 puede realizar copias de seguridad y recuperar sistemas de archivos dañados o incompatibles utilizando el enfoque sector por sector.

## 1.5 Sistemas operativos compatibles

**Acronis License Server**

- Windows XP Professional SP2+ (x86, x64)
- Windows 2000 SP4 - todas las ediciones excepto para la edición Datacenter
- Windows Server 2003/2003 R2 - las ediciones Standard y Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2 (x86)
- Windows Vista - todas las ediciones excepto Vista Home Basic y Vista Home Premium (x86, x64)
- Windows 7 SP1 - todas las ediciones excepto las ediciones Starter y Home (x86, x64)
- Windows Server 2008 - las ediciones Standard y Enterprise (x86, x64)
- Windows Small Business Server 2008 (x64)
- Windows Small Business Server 2011
- Windows Server 2008 R2 SP1 - las ediciones Standard, Enterprise, Datacenter, Foundation

- Windows MultiPoint Server 2010

### Acronis Backup & Recovery 10 Management Console

- Windows XP Professional SP2+ (x86, x64)
- Windows 2000 SP4 - todas las ediciones excepto para la edición Datacenter
- Windows Server 2003/2003 R2 - las ediciones Standard y Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2 (x86)
- Windows Vista - todas las ediciones (x86, x64)
- Windows 7 SP1 - todas las ediciones (x86, x64)
- Windows Server 2008 - las ediciones Standard y Enterprise (x86, x64)
- Windows Small Business Server 2008 (x64)
- Windows Small Business Server 2011
- Windows Server 2008 R2 SP1 - las ediciones Standard, Enterprise, Datacenter, Foundation
- Windows MultiPoint Server 2010

### Acronis Backup & Recovery 10 Management Server y Acronis Backup & Recovery 10 Storage Node

- Windows XP Professional SP3 (x86, x64)
- Windows 2000 SP4 - todas las ediciones excepto para la edición Datacenter
- Windows Server 2003/2003 R2 - las ediciones Standard y Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2 (x86)
- Windows Vista - todas las ediciones excepto Vista Home Basic y Vista Home Premium (x86, x64)
- Windows 7 SP1* - todas las ediciones excepto las ediciones Starter y Home (x86, x64)
- Windows Server 2008 - las ediciones Standard y Enterprise (x86, x64)
- Windows Small Business Server 2008 (x64)
- Windows Small Business Server 2011
- Windows Server 2008 R2 SP1* - las ediciones Standard, Enterprise, Datacenter, Foundation
- Windows MultiPoint Server 2010*

* Acronis Backup & Recovery 10 Storage Node maneja las bibliotecas de cintas y los autocargadores al utilizar el Gestor de almacenamiento extraíble (RSM). Como Windows 7, Windows Server 2008 R2 y Windows MultiPoint Server 2010 no son compatibles con RSM, un nodo de almacenamiento instalado en estos sistemas operativos no es compatible con las bibliotecas de cintas y los autocargadores.

### Acronis Backup & Recovery 10 Agent para Windows

- Windows 2000 Professional SP 4
- Windows XP Professional SP2+ (x86, x64)
- Windows Vista - todas las ediciones excepto Vista Home Basic y Vista Home Premium (x86, x64)
- Windows 7 SP1 - todas las ediciones excepto las ediciones Starter y Home (x86, x64)

---

*Los productos de Acronis no son compatibles con Extensible Firmware Interface (EFI). A pesar de que es posible restaurar una partición GPT con Acronis si Windows está instalada en la misma, el sistema restaurado no podrá arrancarse. Acronis Backup & Recovery 10 puede realizar la copia de seguridad y restaurar sistemas operativos si están instalados en el modo BIOS/MBR, incluso si se ejecutan en servidores compatibles con EFI. La mayoría de los servidores poseen configuraciones de BIOS que permiten arrancar el CD de instalación en modo*

*BIOS/MBR en vez de en modo EFI. El modo MBR garantiza que después de la instalación, el disco de arranque se particiones en MBR estándar, no GPT.*

## 1.6 Requisitos del sistema

Los componentes instalados en Windows

| Componente | Memoria (sobre el SO y las aplicaciones en ejecución) | Espacio de disco necesario durante la instalación o la actualización | Espacio de disco ocupado por los componentes | Adicional |
|---|---|---|---|---|
| Instalación completa | 300 MB | 2,7 GB | 1,7 GB<br>incluyendo SQL Express Server | |
| Agente de Windows | 120 MB | 700 MB | 260 MB | |
| Generador de dispositivos de inicio | 80 MB | 700 MB | 300 MB | Unidad CD-RW o DVD-RW |
| Management Console | 30 MB | 950 MB | 450 MB | Resolución de la pantalla de 1024*768 píxeles o mayor |
| Management Server | 40 MB | 250 MB<br>400 MB para SQL Express Server | 250 MB<br>400 MB para SQL Express Server | |
| Proxy de Wake-On-LAN | Sin importancia | 30 MB | 5 MB | |
| Nodo de almacenamiento | 100 MB | 150 MB | 150 MB<br>Al utilizar una biblioteca de cintas, el espacio necesario para la base de datos de cintas es de: alrededor de 1 MB cada 10 archivos | Hardware recomendado:<br>4 GB de RAM<br>Almacenamiento de alta velocidad, como, por ejemplo, el hardware RAID |
| Servidor de licencias | Sin importancia | 25 MB | 25 MB | |
| Servidor PXE | 5 MB | 80 MB | 15 MB | |

Disponer de la tarjeta de interfaz de red o el adaptador de red virtual es un requisito común para todos los componentes.

### Medio de inicio

| Tipo de medio | Memoria | Tamaño de imagen ISO | Adicional |
|---|---|---|---|
| Basado en Windows PE | 512 MB | 300 MB | |
| Basado en Linux | 256 MB | 130 MB | |

## 1.7 Soporte técnico

### Programa de asistencia y mantenimiento

Si necesita ayuda con su producto de Acronis, vaya a http://www.acronis.es/support/.

### Actualizaciones de productos

Puede descargar las últimas actualizaciones para sus productos de software de Acronis registrado desde nuestra página web en cualquier momento después de iniciar sesión en su **Cuenta** (https://www.acronis.es/my/) y registrar el producto. Consulte **Registro de productos de Acronis en el sitio web** (http://kb.acronis.com/content/4834) y **Guía de usuario de la página web de Acronis** (http://kb.acronis.com/content/8128).

# 2 Comprensión de Acronis Backup & Recovery 10

Esta sección tiene como objetivo brindar una clara comprensión del producto para que se lo pueda usar en varias circunstancias sin las instrucciones "paso a paso".

## 2.1 Conceptos básicos

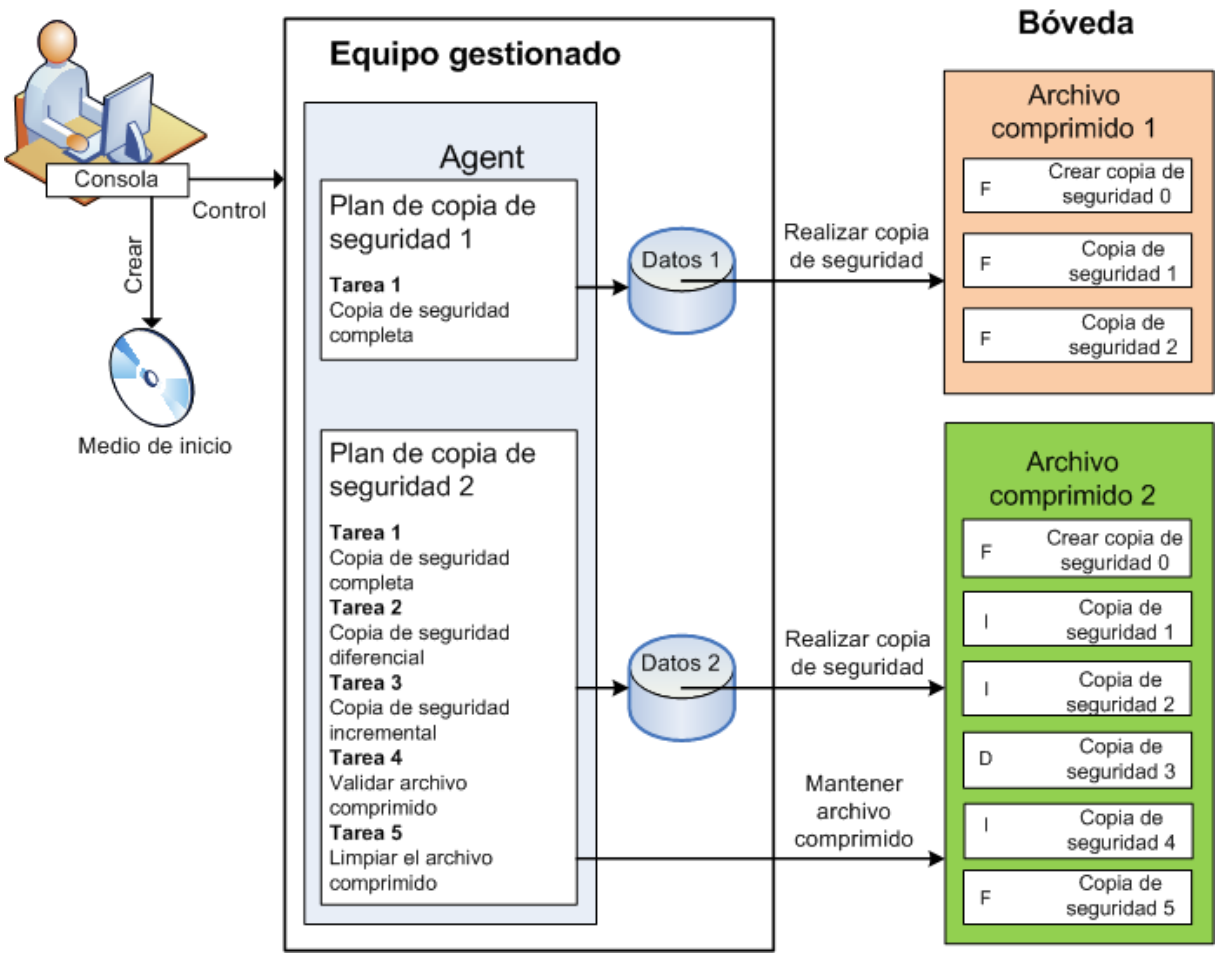
Familiarícese con los conceptos básicos de la interfaz gráfica de usuario y la documentación de Acronis Backup & Recovery 10. Los usuarios avanzados pueden utilizar esta sección como una guía de inicio rápida "paso a paso". Puede encontrar los detalles en la ayuda interactiva.

**Copias de seguridad con sistema operativo**

1. Para proteger los datos en un equipo, instale el agente (pág. 400) Acronis Backup & Recovery 10 en el equipo que a partir de ese momento será administrado (pág. 405).
2. Para poder administrar este equipo con la Interfaz gráfica de usuario, instale la Consola (pág. 403) de administración de Acronis Backup & Recovery 10 en el equipo desde donde desee operar. Si tiene la versión autónoma del producto, ignore este paso porque en su caso, la consola se instala con el agente.
3. Ejecute la consola. Debe crear un medio de inicio (pág. 410) para poder recuperar el sistema operativo del equipo, si no se puede iniciar el sistema.
4. Conecte la consola al equipo administrado.
5. Cree un plan de copia de seguridad (pág. 411).

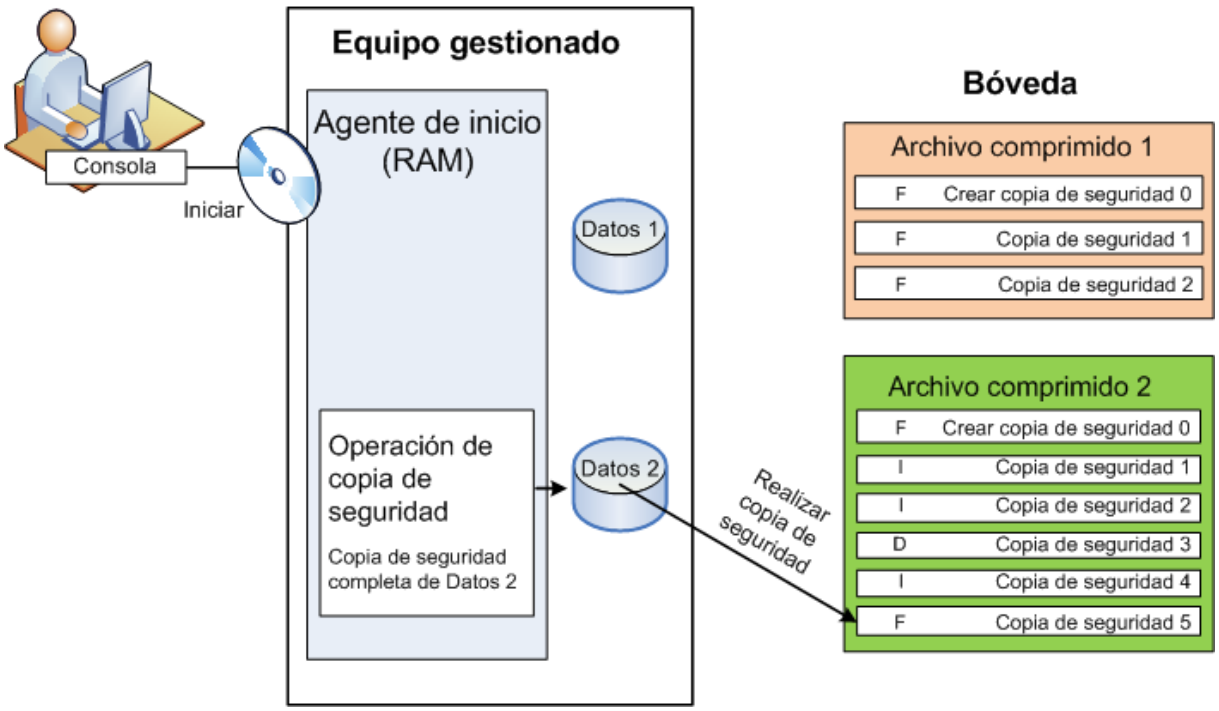
   Para hacerlo, por lo menos, debe especificar los datos a proteger y la ubicación en donde guardar el archivo de copia de seguridad (pág. 401). Esto ayudará a crear un plan de copia de seguridad con una sola tarea (pág. 413) que creará una copia de seguridad (pág. 404) completa de sus datos cada vez que se inicie manualmente la tarea. Un plan complejo de copias de seguridad tiene varias tareas programadas, crean copias completas de seguridad incrementales o diferenciales (pág. 31), realizan operaciones de mantenimiento de archivos como validación (pág. 414) de copias de seguridad o eliminación de copias de seguridad desactualizadas (limpieza (pág. 408) de archivos). Puede personalizar las operaciones de copia de seguridad con varias opciones, como comandos antes y después de copia de seguridad, control del ancho de banda de la red, manejo de errores u opciones de notificación.
6. Use la página de **planes y tareas de la copia de seguridad** para ver la información de sus planes y tareas de copia de seguridad y supervisar su ejecución. Use la página de registro para buscar en el **registro** de las operaciones.
7. La bóveda (pág. 401) es el lugar donde se guardn los archivos de copia de seguridad. Navegue hasta la página de **bóvedas** para ver la información sobre sus bóvedas. Navegue hasta la bóveda específica para ver los archivos y las copias de seguridad y realice operaciones manuales con ellos (montaje, validación, eliminación, visualización de contenidos). También puede seleccionar una copia de seguridad para recuperar sus datos.

El siguiente diagrama ilustra las nociones que se mostraron anteriormente.. Para obtenermás información, consulte el Glosario.



### Realice la copia de seguridad con dispositivos de arranque

Puede iniciar el equipo con un medio de inicio, configurar la operación de copias de seguridad de la misma manera que en un plan simple de copia de seguridad y ejecutar la operación. Esto lo ayudará a extraer archivos y los volúmenes lógicos de un sistema que no inicia, a tomar una imagen del sistema fuera de línea o a realizar copias de seguridad sector por sector en un sistema de archivos incompatible.



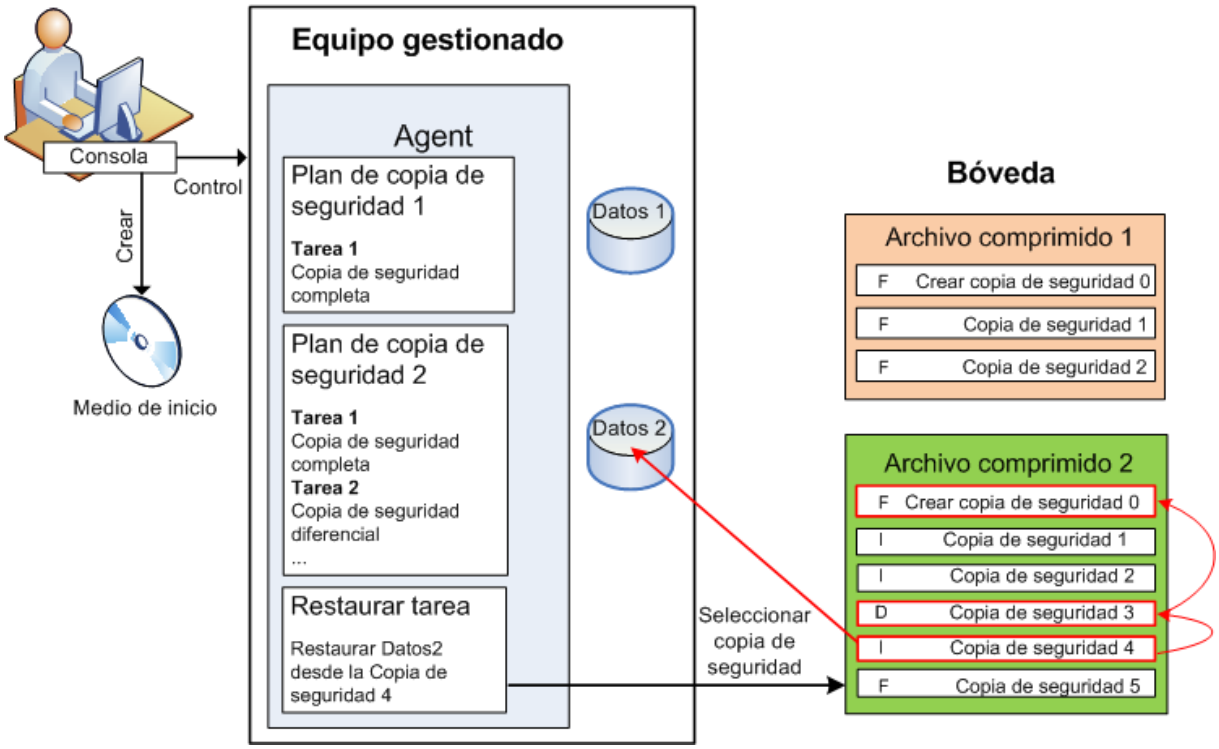

### Recuperación con sistema operativo

En cuanto a la recuperación de datos, puede crear una tarea de recuperación en el equipo administrado. Puede especificar la bóveda y seleccionar el archivo y después seleccionar la copia de seguridad en cuanto a la fecha y hora de la creación de la copia de seguridad, o más precisamente, la hora cuando se comenzó la creación. En la mayoría de los casos, se revertirán los datos hasta ese momento.

***Ejemplos de excepciones a esta regla:***
*La recuperación de una base de datos desde una copia de seguridad que contiene un registro de transacción (una sola copia de seguridad proporciona puntos múltiples de recuperación y así puede realizar selecciones adicionales).*
*La recuperación de varios archivos desde un archivo de copia de seguridad sin instantánea (se revertirá cada archivo al momento en que se copió a la copia de seguridad).*

También puede especificar el destino desde donde recuperar los datos. Puede personalizar la operación de recuperación por medio de opciones de recuperación, como los comandos antes y después de recuperación, manejo de errores o las opciones de notificación.

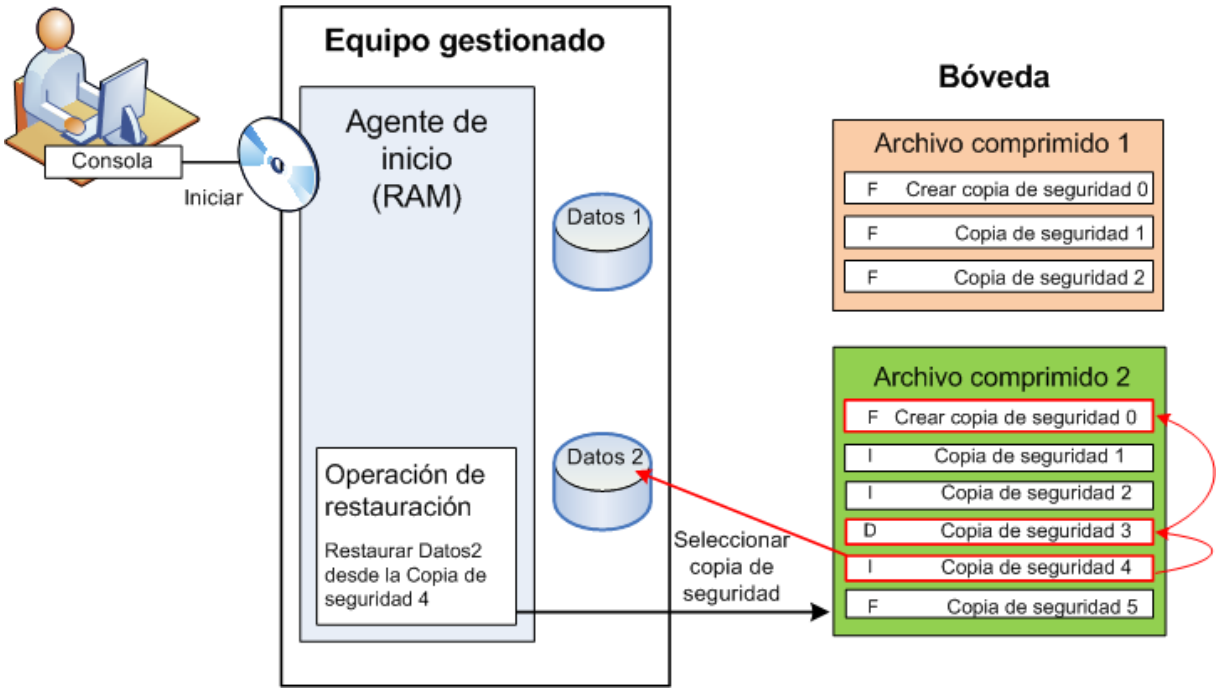
El siguiente diagrama ilustra la recuperación de datos bajo el sistema operativo (en línea). No se puede realizar una copia de seguridad en el equipo mientras se realiza la operación de recuperación. Si fuera necesario, puede conectar la consola a otro equipo y configurar la operación de recuperación en ese equipo. Esta capacidad (recuperación paralela remota) apareció por primera vez en Acronis Backup & Recovery 10; los productos anteriores de Acronis no lo proporcionan.




### Recuperación por medio de dispositivos de arranque

La recuperación a partir de un volumen bloqueado por el sistema operativo, como el volumen en donde reside el sistema, requiere de un reinicio en el entorno de arranque que es parte del agente. Después de completar la recuperación, el sistema operativo recuperado se conecta en línea automáticamente.

Si falla el inicio del equipo o si necesita recuperar los datos desde cero, puede iniciar el equipo que tiene los dispositivos de arranque y puede configurar la operación de recuperación del mismo modo como tarea de recuperación. El siguiente diagrama ilustra la recuperación por medio de los dispositivos de arranque.




## 2.2 Copias de seguridad completas, incrementales y diferenciales

Acronis Backup & Recovery 10 proporciona la capacidad para usar los esquemas de la copia de seguridad populares, como abuelo-padre-hijo y Torres de Hanói, y también para crear esquemas de copia de seguridad personalizados. Todos los esquemas de copia de seguridad están basados en métodos de copia de seguridad diferenciales, incrementales o completos. El término "esquema" denota el algoritmo para aplicar estos métodos para el algoritmo de limpieza del archivo.

Los métodos de comparación entre sí no parecen tener mucho sentido porque los métodos funcionan como un equipo en un esquema de copias de seguridad. Cada método debería tener un rol específico de acuerdo con sus ventajas. Un esquema de copia de seguridad competente podrá sacar provecho de las ventajas de todos los métodos de copias de seguridad y atenúa la influencia de deficiencias de todos los métodos. Por ejemplo, una copia de seguridad diferencial semanal facilita la limpieza del archivo porque se puede borrar fácilmente junto con el conjunto semanal de la copia de seguridad incremental de la que depende.

La realización de la copia de seguridad con los métodos de respaldo completo, incre (pág. 404)mental o diferencial genera una copia de seguridad del tipo correspondiente.

### Copia de seguridad completa

Una copia de seguridad completa almacena todos los datos seleccionados para la copia de seguridad. Una copia de seguridad completa está por debajo del nivel de archivo y forma la base para una copia de seguridad incremental y diferencial. Un archivo puede contener múltiples copias de seguridad completas o sólo copias de seguridad completas. Una copia de seguridad es autosuficiente: no

necesita acceso a ninguna otra copia de seguridad para recuperar los datos desde otra copia de seguridad completa.

Se acepta ampliamente que una copia de seguridad es lo más lento pero es lo más rápido de restaurar. Con las tecnologías de Acronis, la recuperación de una copia de seguridad incremental no puede ser más lenta que la recuperación desde una copia completa.

Una copia de seguridad completa es muy útil cuando:

- se debe restaurar el sistema a su estado inicial,
- este estado inicial no cambia con frecuencia, entonces no necesita una copia de seguridad regular.

Ejemplo: Un cibercafé o un laboratorio de una escuela o universidad en donde el administrador debe deshacer los cambios realizados con frecuencia por los estudiantes o invitados y rara vez actualiza la copia de seguridad de referencia (de hecho, lo hacesolamente después de instalar las actualizaciones de software). En este caso, el tiempo de la copia de seguridad no es importante y el tiempo de recuperación será mínimo cuando recupere los sistemas desde la copia de seguridad completa. El administrador puede tener varias copias de la copia de seguridad completa para mayor confiabilidad.

### Copia de seguridad incremental

Una copia de seguridad incremental almacena todos los cambios desde la **última copia de seguridad**. Necesita tener acceso a otras copias de seguridad desde el mismo archivo para recuperar los datos con una copia de seguridad incremental.

Una copia de seguridad incremental es muy útil cuando:

- tiene la necesidad de volver a uno de los múltiples estados guardados,
- los cambios de los datos tienden a ser pequeños cuando se lo compara con el tamaño total de los datos.

Se acepta ampliamente que las copias de seguridad incrementales son menos confiables que los completos porque si un "eslabón de la cadena" está dañado, no se puede usar los demás. Sin embargo, guardar varias copias de seguridad múltiples no es una opción cuando necesita múltiples versiones anteriores de sus datos, porque la confiabilidad de un archivo extra grande es más dudoso.

Ejemplo: La realización de una copia de seguridad del registro de transacciones de la base de datos.

### Copia de seguridad diferencial

Una copia de seguridad diferencial almacena todos los cambios desde la **última copia de seguridad completa**. Necesita tener acceso a una copia de seguridad completa correspondiente para recuperar los datos desde una copia de seguridad diferencial. Una copia de seguridad diferencial es muy útil cuando:

- usted está interesado en guardar sólo el estado de datos más reciente,
- los cambios de los datos tienden a ser pequeños cuando se lo compara con el tamaño total de los datos.

La conclusión típica es: "Una copia de seguridad diferencial lleva más tiempo para realizar y son más rápidas de recuperar, mientras que las incrementales son las más rápidas de realizar y llevan más para recuperar". De hecho, no hay diferencia física entre la copia de seguridad incremental agregada a la copia de seguridad completa y una copia de seguridad diferencial agregada a la misma copia de seguridad completa en un mismo momento. La diferencia antes mencionada, implica la creación de una copia de seguridad después, o en vez de, crear múltiples copias de seguridad incremental.

*Una copia de seguridad incremental o diferencial creada después de la defragmentación de disco podría ser considerablemente más grande de lo normal porque el programa de defragmentación cambia las ubicaciones de los archivos en el disco y las copias de seguridad reflejan estos cambios. Se recomienda crear nuevamente una copia de seguridad completa después de la desfragmentación del disco.*

La siguiente tabla resume las ventajas y desventajas de cada tipo de seguridad como aparecen ser de dominio público. En la vida real, estos parámetros dependen de varios factores, como la cantidad, velocidad y patrón de los cambios de los datos, la naturaleza de los datos, las especificaciones de los dispositivos, las opciones que se establecen para la copia de seguridad y recuperación, entre otras. La práctica es la mejor guía para seleccionar el esquema óptimo para la copia de seguridad.

| Parámetro | Copia de seguridad completa | Copia de seguridad diferencial | Copia de seguridad incremental |
|---|---|---|---|
| Espacio de almacenamiento | Máximo | Mediano | Mínimo |
| Hora de creación | Máximo | Mediano | Mínimo |
| Tiempo de recuperación | Mínimo | Mediano | Máximo |

## 2.3 Privilegios de usuario en un equipo administrado

Cuando se administra un equipo donde se ejecute Windows, el alcance de los derechos de administración del usuario dependen de los privilegios del usuario en el equipo.

**Usuarios comunes**

Un usuario común, como un miembro del grupo de usuarios, tiene los siguientes derechos de administración:

- Realizar la copia de seguridad a nivel de archivo y la recuperación de los archivos para los que el usuario tiene permiso de acceso; pero sin usar la instantánea de la copia de seguridad a nivel de archivo.
- Crear y administrar los planes de copia de seguridad y tareas.
- Ver (pero no gestionar) los planes y tareas de copia de seguridad creados por otros usuarios.
- Ver los registros de sucesos locales.

**Usuarios administrativos**

Un usuario que tiene privilegios administrativos en el equipo, como un miembro del grupo de Administradores u Operadores de copia de seguridad, además tiene los siguientes derechos de administración:

- Realizar una copia de seguridad y recuperación de todo el equipo o cualquier dato en el equipo, con o sin la instantánea de un equipo.

Los miembros del grupo de Administradores también pueden:

- Ver y gestionar los planes y tareas de la copia de seguridad que pertenecen al usuario en el equipo.

## 2.4 Propietarios y credenciales.

Esta sección explica el concepto de propietario y el significado de las credenciales del plan (o tarea) de la copia de seguridad.

### Propietario del plan (tarea)

El propietario del plan local de la copia de seguridad es del último usuario que modificó o creó la tarea.

El propietario del plan centralizado de la copia de seguridad es el administrador del management server que creó o fue el último en modificar la política centralizada que generó el plan.

La tareas que pertenecen a un plan de copia de seguridad, tanto local como centralizado, son del propietario del plan de la copia de seguridad.

Las tareas no pertenecen al plan de copia de seguridad, como sucede con las tareas de recuperación, sino que son propiedad del último usuario que modificó o creó la tarea.

### Administración de un plan (tarea) que es propiedad de otro usuario

Si un usuario tiene derechos de Administrador en un equipo, puede modificar las tareas y los planes de copia de seguridad locales que cualquier usuario registró en el sistema operativo.

Cuando un usuario abre un plan o tarea para edición, que es propiedad de otro usuario, se borran todas las contraseñas de la tarea. Esto evita el truco "modificar la configuración, dejar la contraseña". El programa muestra una advertencia cada vez que intenta editar un plan (tarea) que fue modificada por otro usuario. Al ver la advertencia, tiene dos opciones:

- Hacer clic en **Cancelar** y cree su propio plan o tarea. La tarea original permanecerá intacta.
- Continuar con la edición. Deberá ingresar todas las credenciales requeridas para la ejecución del plan o tarea.

### Propietario del archivo

El propietario del archivo es el usuario que guardó el archivo en su destino. Para más exactitud, es el usuario cuya cuenta se especificó cuando se creó el plan de copia de seguridad en el paso **Dónde realizar copias de seguridad**. Por defecto, su usan las credenciales del plan.

### Las credenciales del plan y las de las tareas.

Es cualquier tarea que se ejecute en un equipo por arte de un usuario. Cuando crea un plan o una tarea, tiene la opción de especificar claramente una cuenta en la que se ejecutará dicho plan o la tarea. Su opción depende de si el plan o la tarea se utilizan para un inicio manual o para la ejecución programada.

#### Inicio manual

Puede evitar el paso sobre **credenciales de planes (tareas)**. Cada vez que comienza la tarea, la tarea se ejecutará con las credenciales con las que ingresó actualmente. Cualquier persona que tenga privilegios administrativos en el equipo también puede iniciar la tarea. Se ejecutará la tarea con las credenciales de las personas.

La tarea siempre ejecutará con las mismas credenciales, independientemente del usuario que inició la tarea, si especifica las credenciales de las tareas explícitamente. Para hacerlo, en la página de creación del plan (tarea) debe:

1. Seleccionar la casilla de verificación **Vista avanzada**.
2. Seleccionar: **Cambio general -> Credenciales del plan (tarea)**.
3. Ingrese las credenciales con las que se ejecutará el plan (tarea).

**Inicio programado o postergado.**

Las credenciales del plan (tarea) son obligatorias. Si evita el paso de las credenciales, se le pedirá las credenciales después de terminar la creación del plan (tarea).

**¿Por qué el programa obliga a especificar las credenciales?**

Se debe ejecutar una tarea programada o postergada de todos modos, independientemente de si el usuario está conectado o no (por ejemplo, el sistema en la ventana de "Bienvenida" de Windows) o si hay otro usuario conectado además del propietario de la tarea. Basta que el equipo esté encendido (es decir, no en modo espera o hibernación) a la hora que se programó la tarea. Esa es la razón por lo que el programador de Acronis necesita que las credenciales especificadas explícitamente para que pueda cargar la tarea.

## 2.5 Esquema GFS de copia de seguridad

Esta sección cubre la implementación del esquema de copia de seguridad del tipo "abuelo-padre-hijo" (GFS) en Acronis Backup & Recovery 10.

Con este esquema de copia de seguridad no puede realizar copias de seguridad más de una vez por día. El esquema le permite marcar los ciclos diarios, semanales y mensuales en su programa diario de copia de seguridad y especificar los períodos de retención para las copias de seguridad diarias, semanales y mensuales. A las copias de seguridad se las llama "hijos", a las semanales "padres" y a las copias de seguridad de más larga vida se las llama "abuelos".

### GFS como esquema de rotación de cintas

Al principio, se creó a GFS como un esquema de rotación de cintas. Los esquemas de rotación de cintas, como tales, no están automatizados. Sólo determinan:

- la cantidad de cintas que se necesitan para permitir la recuperación con la resolución deseada (el intervalo de tiempo entre los puntos de recuperación) y el período de restauración.
- qué cintas se deben sobrescribir con la siguiente copia de seguridad.

El esquema de rotación de cintas le permite arreglárselas con la cantidad mínima de cartuchos en vez de estar sepultado en cintas usadas. Hay muchas fuentes en Internet que describen las variedades de los esquemas GFS de cintas. Tiene la libertad para usar cualquiera de las variables al hacer las copias de seguridad con un dispositivo de cinta conectado a nivel local.

### GFS de Acronis

Con Acronis Backup & Recovery 10, puede establecer fácilmente un plan de copia de seguridad que realizará regularmente copias de seguridad de los datos y realizará una limpieza del archivo comprimido resultante de acuerdo con el esquema GFS.

Cree el plan de copia de seguridad como siempre. Para el destino de la copia de seguridad, seleccione un dispositivo de almacenamiento en que se pueda realizar la limpieza, como un dispositivo de almacenamiento basado en HDD o un sistema robotizado de cintas. (Como no se puede usar el espacio liberado en la cinta después de la limpieza, hasta que la cinta esté libre, tenga en cuenta ciertas consideraciones adicionales cuando use el esquema GFS en un sistema robotizado (pág. 151).)

La siguiente es una explicación de las configuración que es específica para el esquema de GFS de copias de seguridad.

## Las configuraciones relacionadas a GFS del plan de copia de seguridad

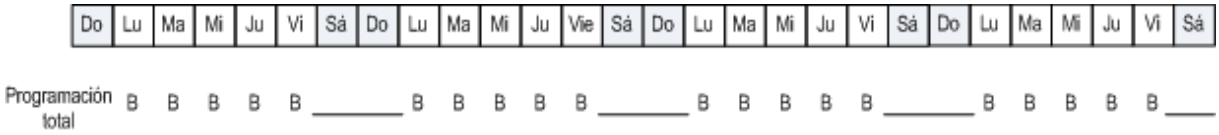
**Comienzo de la copia de seguridad en:**

**Copia de seguridad en:**

Este paso crea el total del programa de la copia de seguridad, es decir, define todos los días en los que se necesita la copia de seguridad.

Asumiremos que se selecciona la copia de seguridad a las 20:00 en los días laborales. Aquí está el programa completo que definió.

“B” significa “Copia de seguridad”.




**Programa completo.**
**Programa: Días laborales a las 20:00.**

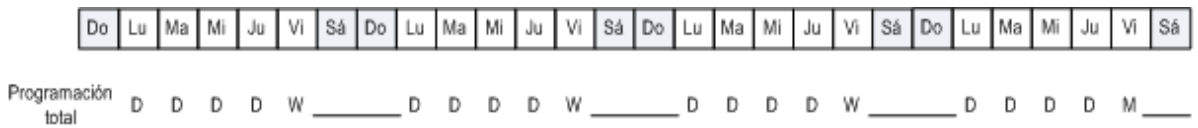
**Semanalmente/mensualmente**

Este paso crea los ciclos diario, semanales y mensuales del programa.

Seleccione un día de la semana de los que seleccionó en el paso anterior. Cada 1era, 2da y 3era copia de seguridad realizada en este día de la semana, será considerado como una copia de seguridad semanal. La 4ª copia de seguridad realizada en este día de la semana se considerará como una copia de seguridad semanal. Las copias de seguridad realizadas en otros días se considerarán como copias de seguridad diarios.

Asumiremos que se selecciona "Viernes" para las copias de seguridad semanales. Aquí se tiene el total del programa marcado de acuerdo a la selección.

“D” significa que a la copia de seguridad se la considera diaria. “W” significa que a la copia de seguridad se la considera semanal. “M” significa que a la copia de seguridad se la considera mensual.

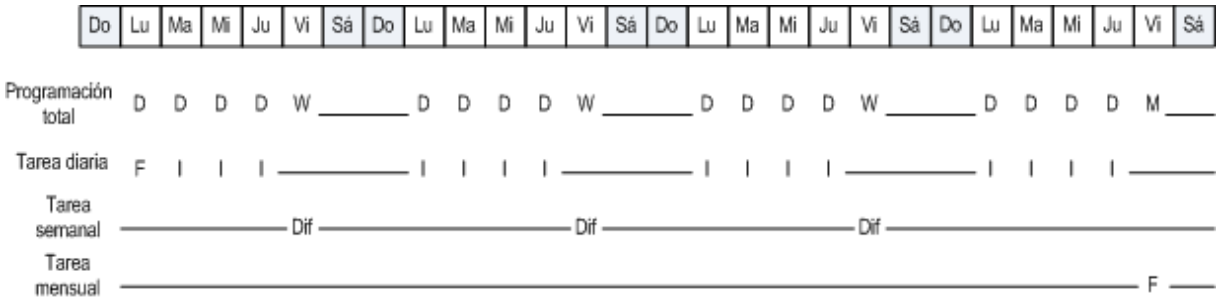



**El programa marcado de acuerdo al esquema GFS.**
**Programa: Días laborales 20:00.**
**Semanal/mensual: Viernes**

Acronis utiliza las copias de seguridad incrementales y diferenciales que ayudan a ahorrar espacio de almacenamiento y optimiza la limpieza que necesita la consolidación. En cuanto a métodos de copias de seguridad, la copia de seguridad semanal es diferencial (Dif.), la copia de seguridad mensual es completa (F) y las copias de seguridad diarias son incrementales (I). La primera copia de seguridad siempre es completa.

El parámetro semanal/mensual divide el esquema total en programas diarios, semanales y mensuales.

Asumiremos que se selecciona "Viernes" para las copias de seguridad semanales. Aquí está el programa real de las tareas de copias de seguridad que se realizarán.




**Las áreas de copias de seguridad realizadas de acuerdo con esquema GFS de Acronis Backup & Recovery 10.**
**Programa: Días laborales 20:00.**
**Semanal/mensual: Viernes**

**Mantener copias de seguridad: Diariamente**

Este paso define la regla de retención para copias de seguridad diarias. La tarea de limpieza se ejecutará después de cada copia de seguridad diaria y se eliminarán las copias de seguridad que sean anteriores a la fecha indicada.

**Mantener copias de seguridad: Semanalmente**

Este paso define la regla de retención para copias de seguridad semanales. La tarea de limpieza se ejecutará después de cada copia de seguridad semanal y se eliminarán las copias de seguridad que sean anteriores a la fecha indicada. El período de retención de las copias de seguridad semanales no puede ser menor al período de retención de las copias de seguridad diarias. Por lo general, son varias veces más largas.

**Mantener copias de seguridad: Mensualmente**

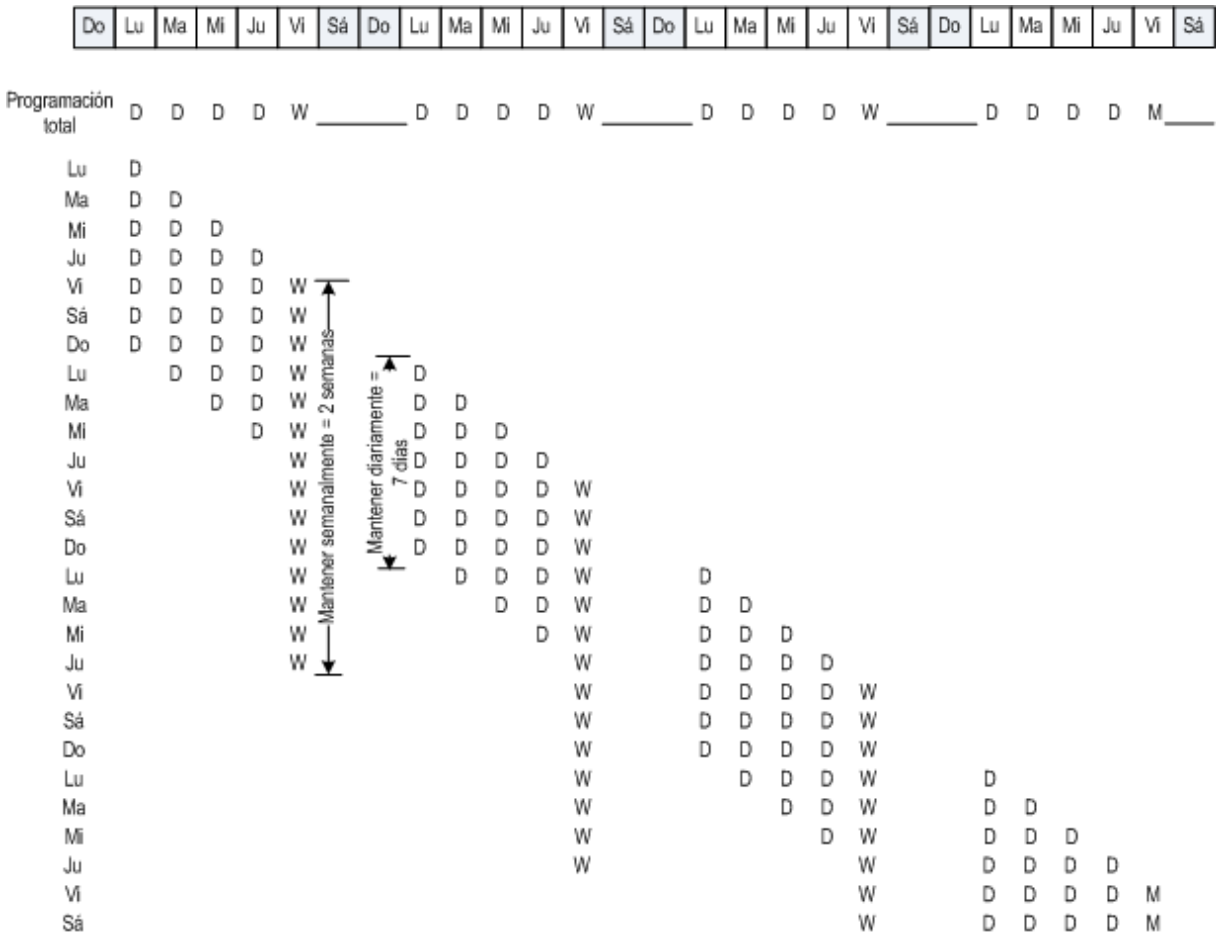
Este paso define la regla de retención para copias de seguridad mensuales. La tarea de limpieza se ejecutará después de cada copia de seguridad mensual y se eliminarán las copias de seguridad que sean anteriores a la fecha indicada. El período de retención de las copias de seguridad mensuales no puede ser menor al período de retención de las copias de seguridad semanales. Por lo general, son varias veces más largas. Es posible mantener las copias de seguridad mensuales infinitamente.

## Archivo comprimido resultante: Ideal

Asumiremos que se mantienen las copias de seguridad diarias durante siete días, las semanales durante 2 semanas y las mensuales durante 6 meses. Así se quedaría el archivo después de que se inicie el plan de copia de seguridad si todas las copias de seguridad son completas y entonces se las podrían eliminar tan pronto como lo requiera el programa.

La columna izquierda muestra los días de la semana. Por cada día de la semana, el contenido del archivo después de la copia de seguridad y se muestra la limpieza posterior.

“D” significa que a la copia de seguridad se la considera diaria. “W” significa que a la copia de seguridad se la considera semanal. “M” significa que a la copia de seguridad se la considera mensual.




**Un archivo ideal creado de acuerdo al esquema GFS.**
**Programa: Días laborales 20:00.**
**Semanal/mensual: Viernes**
**Mantener las copias de seguridad diarias: 7 días**
**Mantener las copias de seguridad semanales: 2 semanas**
**Mantener las copias de seguridad mensuales: 6 meses**

Al comenzar desde la tercera semana, se eliminará regularmente las copias de seguridad semanales. Después de seis meses, se comenzarán a eliminar las copias de seguridad mensuales. El diagrama para las copias de seguridad semanal y mensual se parecerán a la escala de tiempo.

### Archivo comprimido resultante: Real

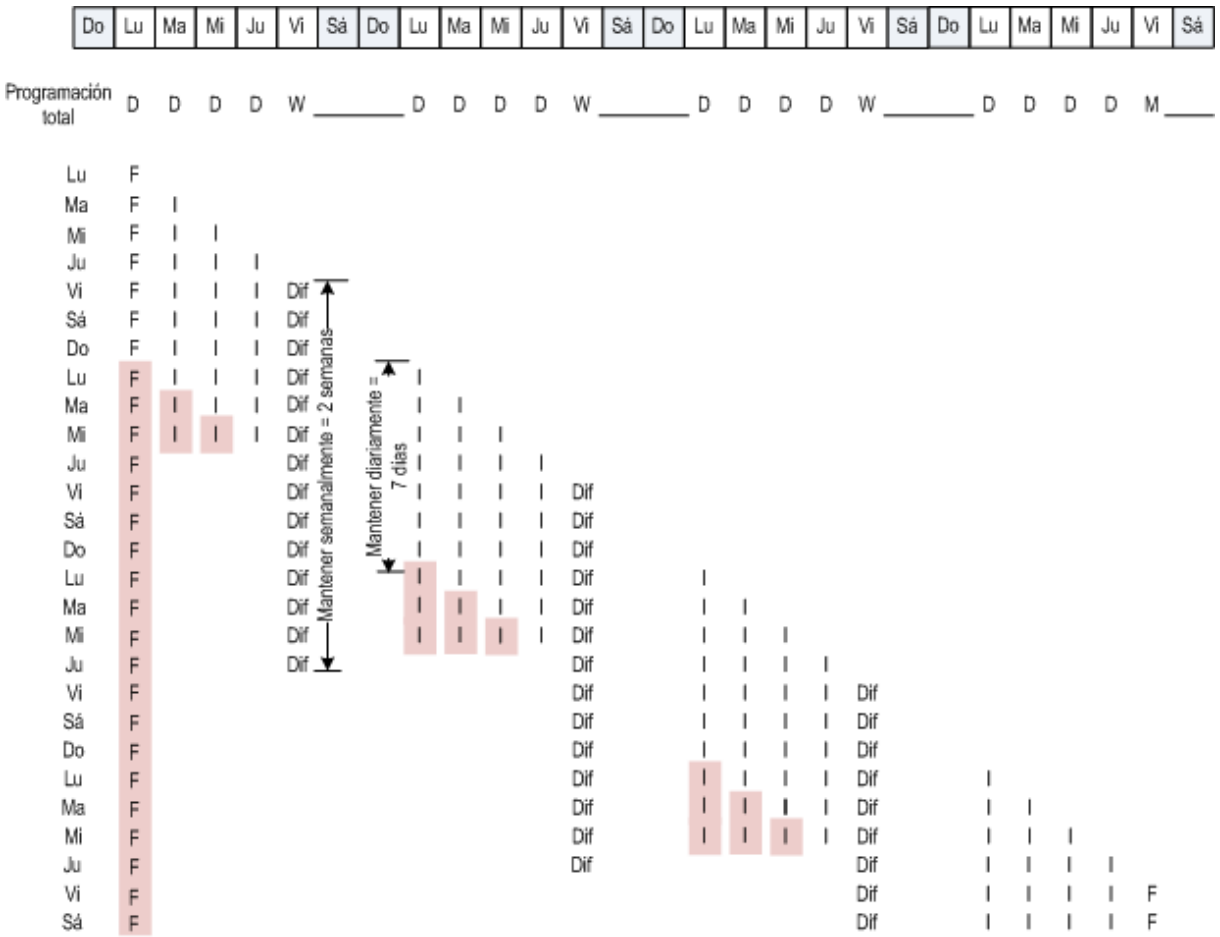
En realidad, el contenido del archivo será un poco diferente al programa ideal.

Cuando se use los métodos de copias de seguridad incrementales y diferenciales, no podrá eliminar las copias de seguridad tan pronto como lo requiera el esquema si las copias de seguridad posteriores se basan en esa copia. Una consolidación regular no es aceptable porque requiere de muchos recursos del sistema. El programa debe esperar hasta que el esquema requiera de la eliminación de todas las copias de seguridad dependientes y entonces allí podrá eliminar la cadena completa.

Aquí se muestra como se verá el primer mes de su plan de copias de seguridad en la vida real. “F” significa copia de seguridad completa. “Dif.” significa copia de seguridad diferencial. “I” significa copia de seguridad incremental.

Las copias de seguridad que sobreviven a su vida útil nominal debido a dependencias, están marcadas con rosa. La copia de seguridad completa inicial será eliminada tan pronto como se eliminen todas las copias de seguridad incrementales y diferenciales basadas en esa copia de seguridad.




**Un archivo creado de acuerdo al esquema GFS de Acronis Backup & Recovery 10.**
**Programa: Días laborales 20:00.**
**Semanal/mensual: Viernes**
**Mantener las copias de seguridad diarias: 7 días**
**Mantener las copias de seguridad semanales: 2 semanas**
**Mantener las copias de seguridad mensuales: 6 meses**

## 2.6 Esquema de copias de seguridad Torres de Hanói

La necesidad de copias de seguridad frecuentes siempre entra en conflicto con el costo de mantenerlas por un período largo. El esquema de copias de seguridad Torres de Hanói (ToH) es unarreglo útil.

### Generalidades de Torres de Hanói

El esquema de la Torres de Hanói se basa en un juego matemático del mismo nombre. En el juego hay varios aros guardados de acuerdo con su tamaño, los más grandes en el fondo, en una de las tres estacas. El objetivo es mover los aros a la tercera estaca. Sólo puede mover un aro a la vez y está prohibido ubicar un aro más grande arriba de otro más pequeño. La solución es cambiar el primer aro en cada movimiento (mueve 1, 3, 5, 7, 9, 11...), el segundo aro a intervalos de cuatro

movimientos (mueve 2, 6, 10...), el tercer aro en intervalos de ocho movimientos (mueve 4, 12...), y así.

Por ejemplo, si hay cinco aros con la etiqueta A, B, C, D, y E en el juego, la solución es la siguiente cadena de movimientos:

| Aro \ Mover | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | A | | A | | A | | A | | A | | A | | A | | A | | A | | A | | A | | A | | A | | A | | A | | A |
| 2 | | B | | | | B | | | | B | | | | B | | | | B | | | | B | | | | B | | | | B | |
| 3 | | | | C | | | | | | | | C | | | | | | | | C | | | | | | | | C | | | |
| 4 | | | | | | | | D | | | | | | | | | | | | | | | | D | | | | | | | |
| 5 | | | | | | | | | | | | | | | | E | | | | | | | | | | | | | | | |

El esquema de la Torres de Hanói para copias de seguridad se basa en los mismos patrones. Funciona con **Sessions** en vez de **Movimientos** y **niveles de Copia de seguridad** en vez de **Aros.** Por lo general, un patrón de esquema de nivel-N, contiene las sesiones (N-th potencia de dos).

Entonces, el esquema de la Torres de Hanói para copias de seguridad de cinco niveles, consiste en 16 sesiones (mueve de 1 a 16 en la ilustración anterior).

La tabla muestra el patrón para el esquema de copia de seguridad. El patrón consiste en 16 sesiones.

| Nivel de copia de seguridad \ Sesión | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | A | | A | | A | | A | | A | | A | | A | | A | |
| 2 | | B | | | | B | | | | B | | | | B | | |
| 3 | | | | C | | | | | | | | C | | | | |
| 4 | | | | | | | | D | | | | | | | | |
| 5 | | | | | | | | | | | | | | | | E |

El esquema de la Torres de Hanói para copias de seguridad mantiene sólo una copia de seguridad por nivel. Se debe eliminar todas las copias de seguridad desactualizadas. Entonces el esquema permite el almacenamiento eficiente de datos: la mayoría de copias de seguridad se acumula hacia el tiempo presente. Si se tienen 4 copias de seguridad, puede recuperar los datos desde hoy, ayer o hace media semana atrás, o una semana atrás. Para el esquema de cinco niveles, también puede recuperar los datos respaldados hasta dos semanas atrás. Cada copia de seguridad adicional duplica el período máximo de restauración de sus datos.

### Torres de Hanói por Acronis

Por lo general, el esquema de la Torres de Hanói para copias de seguridad es muy complejo como para calcular mentalmente el siguiente medio a usar. Pero Acronis Backup & Recovery 10 proporciona la automatización del uso de esquemas Puede establecer el esquema de copias de seguridad mientras crea el plan de copia de seguridad.

Implementación de Acronis para las siguientes características:

- hasta 16 niveles de copias de seguridad
- las copias de seguridad incrementales en el primer nivel (A): para ganar tiempo y ahorrar almacenamiento para las operaciones más frecuentes de copias de seguridad; pero la

recuperación de datos de dichas copias de seguridad lleva más tiempo porque requiere acceso a tres copias de seguridad

- las copias de seguridad completas del último nivel (E para el patrón de cinco niveles): las copias de seguridad más raras en el esquema, lleva más tiempo y ocupa más espacio en el almacenamiento
- las copias de seguridad diferenciales en todos los niveles intermedios (B, C y D para el patrón de cinco niveles)
- la configuración comienza con una copia de seguridad debido a que la primera copia de seguridad no puede ser incremental
- el esquema obliga a cada nivel de copia de seguridad a mantener sólo la copia de seguridad más reciente, se debe eliminar otras copias de seguridad del nivel; sin embargo, se pospone la eliminación de la copia de seguridad en los casos donde la copia de seguridad es la base para otra incremental o diferencial
- se mantiene una copia de seguridad anterior en un nivel hasta que se haya creado copia de seguridad satisfactoriamente en el nivel.

La tabla muestra el patrón para el esquema de copia de seguridad. El patrón consiste en 16 sesiones.

| Nivel de copia de seguridad \ Sesión | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 (Incremental) | | A | | A | | A | | A | | A | | A | | A | | A |
| 2 (Diiferencial) | | | B | | | | B | | | | B | | | | B | |
| 3 (Diiferencial) | | | | | C | | | | | | | | C | | | |
| 4 (Diiferencial) | | | | | | | | | D | | | | | | | |
| 5 (Completo) | E | | | | | | | | | | | | | | | |

Como resultado de usar copias de seguridad incrementales y diferenciales, es posible que haya una copia de seguridad cuya eliminación se posponga porque es la base para otras copias de seguridad. La tabla siguiente indica el caso cuando se pospone en la sesión 17 la eliminación de una copia de seguridad completa en la sesión 1 hasta la sesión 25 porque la copia de seguridad diferencial (D) creada en la sesión 9 todavía es actual. En la tabla, las celdas con copias de seguridad eliminadas están desactivadas.

| Nivel de copia de seguridad \ Sesión | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 (Incremental) | | A | | A | | A | | A | | A | | A | | A | | A | | A | | A | | A | | A | |
| 2 (Diferencial) | | | B | | | | B | | | | B | | | | B | | | | B | | | | B | | |
| 3 (Diferencial) | | | | | C | | | | | | | | C | | | | | | | | C | | | | |
| 4 (Diferencial) | | | | | | | | | D | | | | | | | | | | | | | | | | D |
| 5 (Completo) | E | | | | | | | | | | | | | | | | E | | | | | | | | |

La copia de seguridad diferencial (D), creada en la sesión 9, será eliminada en la sesión 25 después de que se complete la creación de una nueva copia de seguridad diferencial. De esta manera, un archivo de copia de seguridad creado con el esquema de Torres de Hanói por Acronis puede incluir hasta dos copias adicionales de seguridad de acuerdo a la implementación clásica del esquema.

Para obtener más información sobre el uso de la Torres de Hanói con bibliotecas de cintas, consulte Uso del esquema de rotación de cintas con Torres de Hanói (pág. 157).

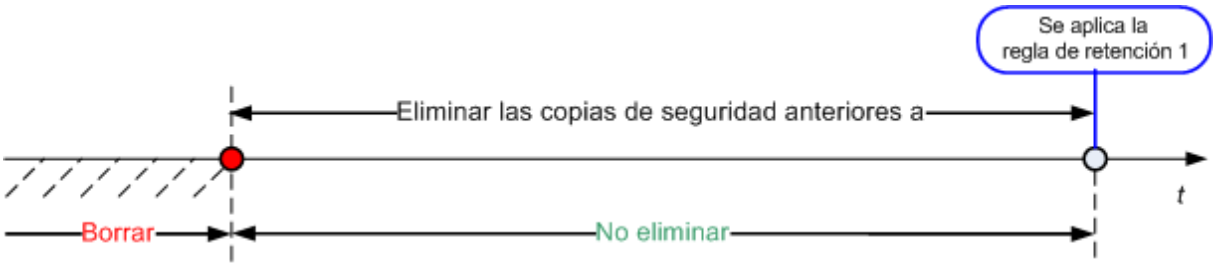
## 2.7 Reglas de retención

Las copias de seguridad realizadas por un plan de copias de seguridad crean un archivo comprimido. Las dos reglas de retención que se describen en esta sección le permiten limitar el tamaño del archivo comprimido y establecer su vida útil (período de retención) de las copias de seguridad.

Las reglas de retención son eficaces si el archivo comprimido tiene más de una copia de seguridad. Esto significa que se guardará la última copia de seguridad del archivo comprimido aunque se detecte una violación a una regla de retención. No intente borrar la única copia de seguridad de la que dispone al aplicar las reglas de retención *antes* de realizar la copia de seguridad. No funcionará. Utilice la configuración alternativa **Limpiar archivo comprimido** > **Cuando no haya espacio suficiente al realizar la copia de seguridad** (pág. 229) si acepta el riesgo de perder la última copia de seguridad.

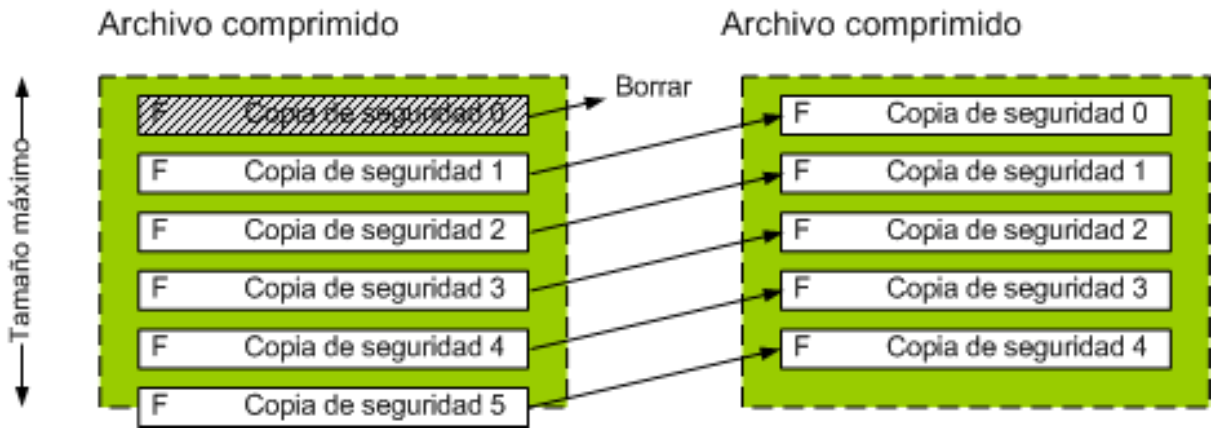
### 1. Eliminar las copias de seguridad anteriores a:

Es un intervalo de tiempo que se calcula desde el momento que se aplicaron las reglas de retención. Cada vez que se aplica una regla de retención, el programa calcula la fecha y hora en el pasado que corresponde a ese intervalo y elimina todas las copias de seguridad anteriores a ese momento. No se eliminará ninguna de las copias de seguridad creadas después de ese momento.



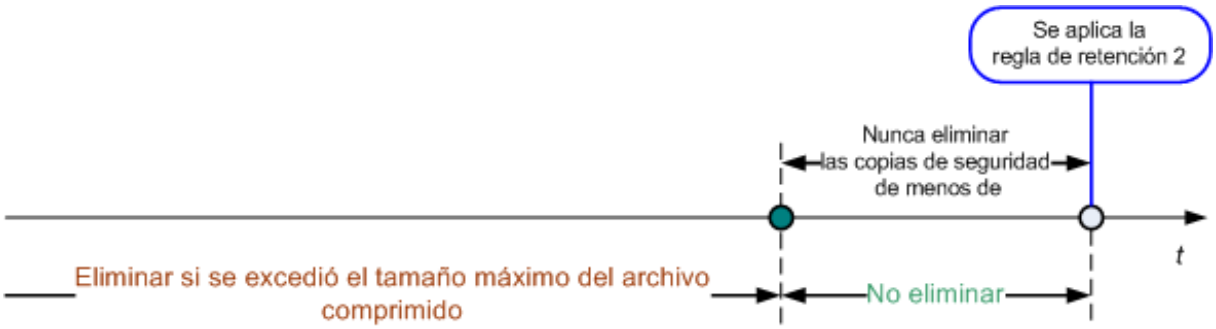

### 2. Mantener el tamaño del archivo comprimido en:

Este es el tamaño máximo del archivo comprimido: cada vez que se aplica una regla de retención, el programa compara el tamaño actual del archivo comprimido con el valor que estableció y elimina las copias de seguridad más viejas para mantener el tamaño del archivo comprimido dentro de ese valor. El siguiente diagrama muestra el contenido del archivo comprimido antes y después de la eliminación.



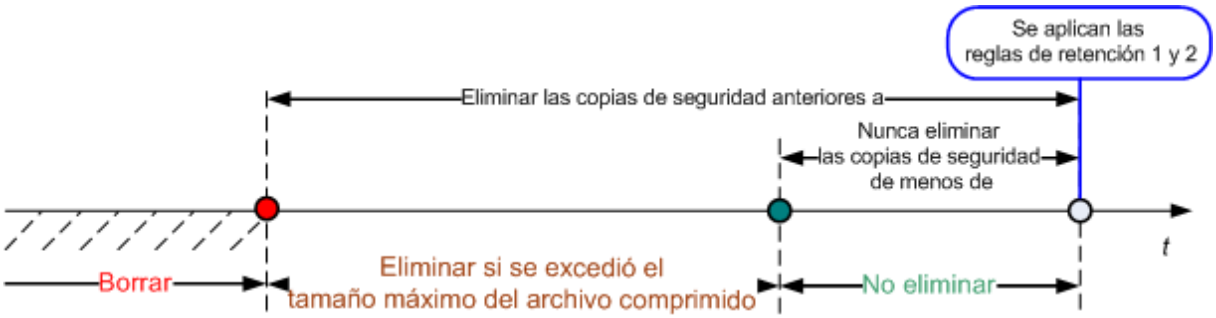

Existe el riesgo de que se eliminen todas las copias de seguridad menos una si se estableció de manera incorrecta el tamaño del archivo comprimido (demasiado pequeño) o una copia de seguridad resulta ser demasiado grande. Seleccione la casilla de verificación **No eliminar las copias de**

**seguridad de menos de** y especifique el tiempo máximo que se deben retener las copias de seguridad para evitar que se eliminen las copias de seguridad recientes. El siguiente diagrama ilustra la regla resultante.




### Combinación de reglas 1 y 2.

Puede limitar la vida útil de ambas copias de seguridad y el tamaño del archivo comprimido. El siguiente diagrama ilustra la regla resultante.




#### Ejemplo

Eliminar las copias de seguridad con más de: 3 meses.

Mantener el tamaño del archivo comprimido en: 200 GB

No eliminar las copias de seguridad menores a: 10 días.

- Cada vez que se aplica una regla de retención, el programa eliminará las copias de seguridad creadas que tengan más de 3 meses (o concretamente, 90 días).
- Si después de la eliminación, el tamaño del archivo es más de 200 GB y la última copia de seguridad tiene más de 10 días, el programa eliminará la copia de seguridad.
- Después, si es necesario, se eliminará la siguiente copia de seguridad hasta que el tamaño del archivo comprimido alcance el límite prestablecido o la copia de seguridad más antigua tenga 10 días.

### Eliminación de las dependencias de las copias de seguridad

Ambas reglas de retención presumen la eliminación de algunas copias de seguridad y la retención de otras. ¿Que sucede si un archivo contiene copias de seguridad incrementales y diferenciales que dependen de la otra y de la completa en la que se basan? No se puede eliminar una copia de seguridad completa desactualizada y mantener a sus "secundarias" incrementales.

Cuando la eliminación de la copia de seguridad afecta a otras copias de seguridad, se aplica una de las siguientes reglas:

- **Se retiene la copia de seguridad hasta que se puedan eliminar las dependientes**

  Se mantendrá la copia de seguridad desactualizada hasta que se actualicen todas las copias de seguridad dependientes. Entonces, se eliminará toda la cadena durante una limpieza regular. Este modo ayuda a evitar una potencial consolidación que requiera mucho tiempo pero que requiera de espacio adicional para almacenar las copias de seguridad cuya eliminación se postergó. El tamaño del archivo comprimido y su antigüedad pueden superar los valores especificados.

- **Consolidar la copia de seguridad**

  El programa consolidará la copia de seguridad que está sujeta a eliminación en la siguiente copia de seguridad dependiente. Por ejemplo, las reglas de retención requieren la eliminación de una copia de seguridad completa pero retienen la siguiente incremental. Las copias de seguridad se combinarán en una sola copia de seguridad completa que tendrá la fecha de la copia de seguridad incremental. Cuando se elimina una copia de seguridad incremental o diferencial de la mitad de la cadena, el tipo de copia de seguridad resultante será incremental.

  Este modo asegura que después de cada limpieza, el tamaño del archivo y su antigüedad estarán dentro de los límites especificados. Sin embargo, la consolidación puede tomar mucho tiempo y muchos recursos del sistema. Y necesitará espacio adicional en la bóveda para los archivos temporales creados durante la consolidación.

  **Lo que necesita saber sobre consolidación**

  Tenga en cuenta que la consolidación es solo un método para eliminar y no una alternativa a la eliminación. La copia de seguridad resultante no tendrá los datos que estaban en la copia de seguridad eliminada y que no estaban en la copia de seguridad incremental o diferencial retenida.

  Las copias de seguridad resultantes de la consolidación siempre usarán la compresión máxima. Esto significa que todas las copias de seguridad en un archivo comprimido usarán la compresión máxima como resultado de una limpieza repetida con consolidación.

### Las mejores prácticas

Mantenga el equilibrio entre la capacidad del dispositivo de almacenamiento, los parámetros restrictivos que establece y la frecuencia de limpieza. Las reglas de retención lógica asumen que la capacidad del dispositivo de almacenamiento es mucho mayor al de una copia de seguridad promedio y que el tamaño máximo del archivo comprimido no se acerca a la capacidad física de almacenamiento, pero deja una reserva razonable. Debido a esto, si se excede el tamaño del archivo comprimido entre las ejecuciones de las tareas de limpieza, no será un problema para el proceso comercial. Cuanto menor sea la cantidad de ejecuciones de limpieza, mayor será el espacio necesario para almacenar las copias de seguridad que ya pasaron su vida útil.

La página Bóvedas (pág. 130) le proporciona información sobre espacio libre disponible en cada bóveda. Compruebe esta página periódicamente. Si el espacio libre (que en definitiva es el espacio libre en el dispositivo de almacenamiento) se acerca a cero, es posible que deba aumentar las restricciones o los archivos en la bóveda.

## 2.8 Realización de copias de seguridad de volúmenes dinámicos (Windows)

Esta sección explica brevemente como realizar copias de seguridad y recuperar volúmenes dinámicos (pág. 414) con Acronis Backup & Recovery 10. También se detallan los discos básicos que usan la Tabla de partición GUID (GPT).

El volumen dinámico es un volumen ubicado en discos dinámicos (pág. 404), o más exactitud, un grupo de discos (pág. 407). Acronis Backup & Recovery 10 es compatible con el siguiente tipo de volúmenes dinámicos/niveles RAID:

- simple/extendido
- segmentado (RAID 0)
- replicado (RAID 1)
- una réplica de segmentos (RAID 0+1)
- RAID 5.

Acronis Backup & Recovery 10 puede realizar una copia de seguridad y la recuperación de volúmenes dinámicos, con menos limitaciones, volúmenes GPT básicos.

### Realización de copias de seguridad de volúmenes dinámicos

A los volúmenes GPT dinámicos y básicos se les realizan copias de seguridad de la misma manera que a los volúmenes MBR básicos. Cuando cree un plan de copia de seguridad a partir de la interfaz GUI, todos los tipos de volúmenes están disponibles para la selección como **elementos para realizar la copia de seguridad**. Cuando esté en la línea de comandos, especifique los volúmenes dinámicos GPT con el prefijo DYN.

#### Ejemplos de línea de comandos

```
trueimagecmd /create /partition:DYN1,DYN2 /asz
```

Esto realizará una copia de seguridad de los volúmenes DYN1 y DYN2 en Acronis Secure Zone.

```
trueimagecmd /create /harddisk:DYN /asz
```

Esto realizará una copia de seguridad de todos los volúmenes dinámicos del sistema en Acronis Secure Zone.

No se realizan copias de seguridad o recuperación del código de inicio en los volúmenes GPT básicos.

### Recuperación de volúmenes dinámicos

Se puede recuperar un volumen dinámico

- con cualquier tipo de volumen existente
- en un espacio no asignado de espacio en un grupo de discos
- en un espacio no asignado de un disco básico.

#### Recuperación sobre un volumen existente

Cuando se recupera un volumen dinámico en un volumen existente, tanto básico o dinámico, el volumen de destino de datos se sobrescribe el contenido de la copia de seguridad. El tipo de volumen de destino (básico, simple/extendido, segmentado, replicado, RAID 0+1, RAID 5) no cambiará. El tamaño del volumen de destino debe ser suficiente para incluir el contenido de la copia de seguridad.

#### La recuperación al espacio no asignado de un grupo de disco

Cuando se recupera un volumen dinámico en un espacio no asignado de un grupo de discos, se recupera tanto el tipo de contenido y tipo del volumen resultante. El tamaño del espacio no asignado debe ser suficiente para incluir el contenido de la copia de seguridad. Es importante la manera en que se distribuye el espacio no asignado entre los discos.

**Ejemplo**

Los volúmenes segmentados consumen porciones equivalentes de espacio en cada disco.

Suponga que va a recuperar un volumen segmentado de 30 GB en un grupo que tiene dos discos. Cada disco tiene volúmenes y cierta cantidad de espacio no asignado. El tamaño total de espacio no asignado es de 40 GB. La recuperación siempre será un volumen segmentado si el espacio no asignado se distribuye incluso entre los disco (20 GB y 20 GB).

Si uno de los discos tiene 10 GB y el otro tiene 30 GB de espacio no asignado, entonces el resultado de la recuperación depende del tamaño de los datos que se recuperen.

- Si el tamaño de datos es menor que 20 GB, entonces un disco puede soportar 10 GB; el otro soportará los restantes 10GB. De esta manera, se creará un volumen en ambos discos y quedarán 20 GB en el segundo disco sin asignación.
- Si el tamaño de los datos es mayor a 20 GB, no se pueden distribuir los datos uniformemente entre los dos discos, pero pueden caber en un volumen simple. Se creará un volumen simple que incluye todos los datos en el segundo disco. El primer disco quedará intacto.

| | **Copia de seguridad (destino):** | | |
|---|---|---|---|
| **Recuperar en:** | **Volumen dinámico** | **Volumen MBR básico** | **Volumen GPT básico** |
| **Volumen dinámico** | Volumen dinámico<br>Tipo como destino | Volumen dinámico<br>Tipo como destino | Volumen dinámico<br>Tipo como destino |
| **Espacio no asignado (grupo de disco)** | Volumen dinámico<br>Tipo como destino | Volumen dinámico<br>Simple | N/A |
| **Volumen MBR básico** | Volumen MBR básico | Volumen MBR básico | Volumen MBR básico |
| **Volumen GPT básico** | Volumen GPT básico | Volumen GPT básico | Volumen GPT básico |
| **Espacio no asignado (disco básico MBR)** | Volumen MBR básico | Volumen MBR básico | Volumen MBR básico |
| **Espacio no asignado (disco básico GPT)** | Volumen GPT básico | Volumen GPT básico | Volumen GPT básico |

**Movimiento y redimensionamiento de volúmenes durante la recuperación**

Puede redimensionar el volumen básico resultante, tanto con MBR como GPT durante la recuperación o para cambiar la ubicación del volumen en el disco. No se puede mover ni redimensionar el volumen dinámico resultante.

## Preparación de grupos de discos y volúmenes

Antes de recuperar volúmenes dinámicos, debería crear un grupo de discos en el hardware de destino.

Es posible que también necesite crear o aumentar el espacio no asignado en un grupo de disco existente. Se puede realizar al eliminar volúmenes o convertir los discos básicos a dinámicos.

Es posible que quiera cambiar el tipo del volumen de destino (básico, simple o extendido, segmentado, replicado, RAID 0+1, RAID 5). Esto se logra al eliminar el volumen de destino y crear un nuevo volumen en el espacio no asignado resultante.

Acronis Backup & Recovery 10 incluye una utilidad de administración del disco muy útil que permite realizar las operaciones mencionadas tanto con sistemas operativos o desde cero. Para obtener más información Acronis Disk Director Lite, consulte la sección Administración del disco (pág. 294).

## 2.9 Soporte de cintas

Acronis Backup & Recovery 10 es compatible con bibliotecas de cintas, cargadores automáticos, SCSI y unidades de cinta USB como dispositivos de almacenamiento. Un dispositivo de cinta se puede conectar a nivel local a un equipo administrado (en este caso, el agente Acronis Backup & Recovery 10 escribe y lee las cintas) o se puede acceder desde el nodo de almacenamiento de Acronis Backup & Recovery 10 (pág. 20). Los nodos de almacenamiento aseguran el funcionamiento completamente automático de Bibliotecas de cintas y cargadores automáticos (pág. 139).

Los archivos de copia de seguridad creados con varias maneras de acceder a la cinta tienen diferentes formatos. Un agente no puede leer una cinta escrita con un nodo de almacenamiento.

Los medios basados en Linux y PE permiten la copia de seguridad y recuperación con acceso local y acceso por el nodo de almacenamiento. Se puede recuperar las copias de seguridad creadas con dispositivos de arranque con el agente de Acronis Backup & Recovery 10 que se ejecuta en el sistema operativo.

### 2.9.1 Tabla de compatibilidad de cintas

La siguiente tabla resume la legibilidad de las cintas escritas por Acronis True Image Echo y la familia de productos Acronis True Image 9.1 en Acronis Copia de seguridad de & Recovery 10. La tabla también ilustra la compatibilidad de las cintas escritas de varios componentes de Acronis Copia de seguridad de & Recovery 10.

| | | | **...es legible en un dispositivo de cinta conectado en un equipo con...** | | | |
|---|---|---|---|---|---|---|
| | | | Medio de inicio de ABR10 | Agente de Windows ABR10 | Agente de Linux ABR10 | Nodo de almacenamiento ABR10 |
| **Cinta escrita en un dispositivo de cinta conectado a nivel local (unidad de cinta o biblioteca de cintas) por...** | Medio de inicio | ATIE 9.1 | + | + | + | + |
| | | ATIE 9.5 | + | + | + | + |
| | | ATIE 9.7 | + | + | + | + |
| | | ABR10 | + | + | + | + |
| | Agente para Windows | ATIE 9.1 | + | + | + | + |
| | | ATIE 9.5 | - | - | - | + |
| | | ATIE 9.7 | - | - | - | + |
| | | ABR10 | + | + | + | + |
| | Agente para Linux | ATIE 9.1 | + | + | + | + |
| | | ATIE 9.5 | + | + | + | + |
| | | ATIE 9.7 | + | + | + | + |
| | | ABR10 | + | + | + | + |
| **Cinta escrita en un dispositivo de cinta por...** | Servidor de copia de seguridad | ATIE 9.1 | + | + | + | + |
| | | ATIE 9.5 | - | - | - | + |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | ATIE 9.7 | - | - | - | + |
| | Nodo de almacenamiento | ABR10 | - | - | - | + |

## 2.9.2 Uso de una sola unidad de cinta

Una unidad de cinta que está conectada a nivel local a un equipo administrado y se puede usar con los planes de copias de seguridad locales, como dispositivo de almacenamiento. La funcionalidad de un cargador automático conectado a nivel local o la biblioteca de cintas está limitada a la unidad de cinta. Esto significa que el programa sólo puede funcionar con la cinta que se encuentra montada y debe montar las cintas manualmente.

### Creación de una copia de seguridad en un dispositivo de cinta conectado a nivel local

Cuando se crea un plan de copia de seguridad, puede seleccionar el dispositivo de cinta conectado a nivel local como el destino para la copia de seguridad. No se necesita el nombre del archivo cuando se crea una copia de seguridad en una cinta.

Un archivo puede abarcar múltiples cintas pero puede contener sólo una copia de seguridad completa y un número ilimitado de copias de seguridad incremental. Cada vez que se cree una copia de seguridad completa, comience con una nueva cinta y cree un nuevo archivo. Una vez que la cinta esté llena, aparecerá una ventana de diálogo donde se solicita la colocación de una nueva cinta.

El contenido de cintas que no están en blanco, se sobrescribirán cuando se lo pida. Tiene la opción de desactivar los comandos, consulte Configuraciones adicionales (pág. 119).

**Solución alternativa**

En caso de que desee conservar más de un archivo comprimido en la cinta, por ejemplo, si desea realizar copias de seguridad del volumen C y el D por separado, seleccione el modo de copia de seguridad incremental en lugar de copia de seguridad completa cuando cree la primera copia de seguridad para el segundo disco. En otras situaciones, la copia de seguridad incremental se utiliza para añadir cambios al archivo creado anteriormente.

Es posible que experimente pausas breves que son necesarias para rebobinar la cinta. Una cinta de baja calidad o vieja así como un cabezal magnético sucio pueden provocar pausas que pueden durar hasta varios minutos.

**Limitaciones**

1. Copias de seguridad completas dentro de un archivo no son compatibles.
2. Los archivos individuales no se pueden recuperar desde la copia de seguridad del disco.
3. Las copias de seguridad no se pueden eliminar de una cinta manualmente o automáticamente durante la limpieza. Las reglas de retención y los esquemas de copia de seguridad que usan limpieza automática (GPS, Torres de Hanói) están deshabilitados en la interfaz GUI cuando se realice una copia de seguridad a una cinta conectada a nivel local.
4. La bóveda personal no se puede crear en los dispositivos de cinta.
5. Debido a que la presencia de un sistema operativo no se puede detectar en la copia de seguridad en una cinta, se propone a Acronis Universal Restore (pág. 413) en la recuperación de cada disco o volumen, incluso cuando se recupera en un volumen de Linux o sin sistema de Windows.
6. Acronis Active Restore (pág. 400) no está disponible cuando se recupera desde una cinta.

### Creación de una recuperación en un dispositivo de cinta conectado a nivel local

Antes de crear una tarea de recuperación, inserte o monte la cinta con la copia de seguridad que necesita recuperar. Cuando cree una tarea de recuperación, seleccione el dispositivo de cinta de la lista de ubicaciones disponibles y después seleccione la copia de seguridad. Después de comenzar una recuperación, se le pedirá otras cintas si se necesita otras cintas para la recuperación.

## 2.10 Compatibilidad con SNMP

### Objetos SNMP

Acronis Backup & Recovery 10 proporciona los siguientes objetos del Protocolo simple de administración de red (SNMP) para las aplicaciones de gestión SNMP:

- Tipo de evento.

  Identificador de objeto (OID): 1.3.6.1.4.1.24769.100.200.1.0.

  Sintaxis: OctetString.

  El valor puede ser "Información", "Advertencia", 'Error" y "Desconocido". "Desconocido" se envía únicamente en el mensaje de prueba.
- Descripción del texto del evento

  Identificador de objeto (OID): 1.3.6.1.4.1.24769.100.200.2.0.

  Sintaxis: OctetString.

  El valor contiene la descripción del texto del evento (tiene el mismo aspecto que los mensaje publicados por Acronis Backup & Recovery 10 en su registro).

**Ejemplo de valores varbind:**

1.3.6.1.4.1.24769.100.200.1.0:Information.

1.3.6.1.4.1.24769.100.200.2.0:I0064000B.

### Operaciones compatibles

Acronis Backup & Recovery 10 **es compatible únicamente con operaciones TRAP**. no es posible gestionar Acronis Backup & Recovery 10 usando solicitudes GET- y SET. Esto significa que necesita utilizar un receptor SNMP Trap para recibir mensajes TRAP.

### Acerca de la base de información de gestión (MIB)

El archivo MIB **acronis-abr.mib** se encuentra ubicado en el directorio de instalación Acronis Backup & Recovery 10. De forma predeterminada: %ProgramFiles%\Acronis\BackupAndRecovery en Windows y /usr/lib/Acronis/BackupAndRecovery en Linux.

Este archivo puede ser leído por un explorador MIB o por un simple editor de texto como el Notepad.

### Acerca del mensaje de prueba

Cuando configure notificaciones SNMP, puede enviar un mensaje de prueba para comprobar si sus configuraciones son correctas.

Los parámetros del mensaje de prueba son como se describe a continuación:

- Tipo de evento

  OID: 1.3.6.1.4.1.24769.100.200.1.0

  Valor: "Desconocido"

- Descripción del texto del evento
  OID: 1.3.6.1.4.1.24769.100.200.2.0
  Valor: "?00000000"

## 2.11 Tecnologías propias de Acronis

En esta sección se describen las tecnologías propias heredadas de los productos de la familia de Acronis Backup & Recovery 10 de Acronis True Image Echo y Acronis True Image 9.1.

### 2.11.1 Acronis Secure Zone

Acronis Secure Zone es una partición segura que permite mantener archivos comprimidos de copia de seguridad en el espacio de disco de un equipo gestionado y, por lo tanto, recuperar un disco del mismo disco en el que reside la copia de seguridad.

Algunas aplicaciones de Windows, como las herramientas de gestión de disco de Acronis, pueden acceder a la zona.

Si el disco tuviera una falla física, se perderían la zona y los archivos ubicados allí. Esa es la razón por la que Acronis Secure Zone no debe ser la única ubicación donde se almacene una copia de seguridad. En entornos empresariales, se puede pensar en Acronis Secure Zone como una ubicación intermedia utilizada para realizar copias de seguridad cuando una ubicación normal no está disponible temporalmente o se conecta a partir de un canal lento u ocupado.

#### Ventajas

Acronis Secure Zone

- Permite la recuperación de un disco en el mismo disco en donde reside la copia de seguridad del disco.
- Ofrece un método rentable y útil para la protección de datos por funcionamiento defectuoso del software, ataque de virus, error del operador.
- Como es un almacenamiento interno de archivos, elimina la necesidad de separar los medio o conexión de red para realizar la copia de seguridad o recuperar los datos. Esto es muy útil para los usuarios móviles.
- Puede funcionar como destino primario cuando se use copia de seguridad de doble destino (pág. 114).

#### Limitaciones

- La zona no se puede organizar en un disco dinámico o un disco que use el estilo de partición GPT.

#### Administración de Acronis Secure Zone

Acronis Secure Zone se considera una bóveda (pág. 401) personal. Una vez que se crea en un equipo gestionado, la zona está presente siempre en la lista de **Bóvedas personales**. Los planes de copias de seguridad centralizados (pág. 411) pueden utilizar tanto Acronis Secure Zone como planes locales (pág. 412).

Si ha utilizado Acronis Secure Zone anteriormente, tenga en cuenta que se ha producido un cambio radical en su funcionamiento. La zona ya no realiza limpiezas automáticas, es decir, ya no elimina archivos comprimidos antiguos. Use esquemas de copia de seguridad con limpieza automática para realizar copias de seguridad en la zona, o elimine las copias de seguridad desactualizadas manualmente con la funcionalidad de administración de archivos.

Con el nuevo comportamiento de Acronis Secure Zone, puede conseguir:

- la lista de archivos ubicados en la zona y la copia de seguridad en cada archivo
- examen del contenido de la copia de seguridad
- el montaje de la copia de seguridad del disco para copiar los archivos de la copia de seguridad a un disco físico
- eliminar de manera segura los archivos comprimidos y las copias de seguridad de los archivos comprimidos.

Para obtener más información sobre funciones disponibles en Acronis Secure Zone, consulte la sección Bóvedas personales (pág. 165).

#### Actualización desde Acronis True Image Echo

Cuando se actualiza desde Acronis True Image Echo a Acronis Backup & Recovery 10, Acronis Secure Zone mantendrá los archivos comprimidos creados con Echo. La zona aparecerá en la lista de bóveda personal y los archivos antiguos estarán disponibles para recuperación.

### 2.11.2 Acronis Startup Recovery Manager

Se puede modificar el agente de inicio (pág. 401) del disco del sistema y se puede configurar para arrancar en el momento de inicio, cuando se pulse F11. Esto elimina la necesidad de los medios de recuperación o conexión de red para iniciar la utilidad de rescate de inicio. La característica tiene el nombre comercial "Acronis Startup Recovery Manager".

Acronis Startup Recovery Manager es muy útil para los usuarios móviles. En caso de fallo, el usuario reinicia el equipo, pulsa F11 cuando aparezca el aviso "Press F11 for Acronis Startup Recovery Manager..." y realiza recuperación de datos en la misma manera que con un medio de inicio común. El usuario también puede realizar copias de seguridad con Acronis Startup Recovery Manager, mientras está en movimiento.

En equipos con el cargador de inicio GRUB instalado, el usuario selecciona Acronis Startup Recovery Manager del menú de inicio en lugar de pulsar F11.

#### La activación y desactivación de Acronis Startup Recovery Manager

La operación que permite el uso de Acronis Startup Recovery Manager se denomina "activación". Para activar Acronis Startup Recovery Manager, seleccione **Acciones > Activar Acronis Startup Recovery Manager** en el menú del programa.

Puede activar o desactivar Acronis Startup Recovery Manager en cualquier momento desde el menú **Herramientas**. La desactivación deshabilitará el mensaje de tiempo de inicio "Pulse F11 para Acronis Startup Recovery Manager..." (o elimina la entrada correspondiente del menú de inicio GRUB correspondiente). Esto significa que necesitará dispositivos de arranque en caso que se deba iniciar el sistema.

#### Limitación

Después de activar Acronis Startup Recovery Manager es necesario reactivar cargadores de terceros.

#### Actualización de Acronis True Image Echo

Después de la actualización de Acronis True Image Echo a Acronis Backup & Recovery 10, Acronis Startup Recovery Manager aparece como desactivado independientemente de su estado antes de la actualización. Puede activar Acronis Startup Recovery Manager nuevamente en cualquier momento.

### 2.11.3 Universal Restore (Acronis Backup & Recovery 10 Universal Restore)

Acronis Backup & Recovery 10 Universal Restore es la tecnología propia de Acronis que ayuda a recuperar e iniciar Windows con hardware diferente o máquina virtual. Universal Restore maneja diferentes dispositivos que son críticos para el inicio del sistema operativo, como controladores de almacenamiento, placa madre o conjunto de chips.

#### Propósito de Acronis Backup & Recovery 10 Universal Restore

Se puede recuperar fácilmente un sistema desde una copia de seguridad de un sistema (imagen) al mismo sistema o hardware idéntico. No obstante, si cambia la placa madre o utiliza otra versión de procesador, algo probable en caso de un fallo de hardware, quizá no pueda iniciar el sistema restaurado. Un intento de transferir el sistema a un equipo nuevo y mucho más potente suele producir el mismo resultado dado que el nuevo hardware es incompatible con los controladores críticos incluidos en la imagen.

Con Herramienta de preparación del sistema para Microsoft (Sysprep) no se soluciona el problema, porque Sysprep permite la instalación de controladores sólo para dispositivos Plug and Play (tarjetas de sonido, adaptadores de red, tarjetas de vídeo, etc). En cuanto a la capa de abstracción del hardware del sistema (HAL, por sus siglas en inglés) y los controladores de dispositivos de almacenamiento masivo, deben ser idénticos en los equipos de origen y destino (consulte la Base de conocimiento de Microsoft (Microsoft Knowledge Base, artículos 302577 y 216915)).

La tecnología de Universal Restore proporciona una solución eficaz para la restauración de sistemas, independientemente del hardware, al sustituir la capa de abstracción de hardware (HAL) y los controladores de dispositivos de almacenamiento masivo.

Universal Restore se aplica en:

1. Recuperación instantánea de un sistema defectuoso en otro hardware
2. Clonación e implementación de sistemas operativos, independientemente del hardware
3. Migración de equipo físico a físico, físico a virtual y virtual a físico.

#### Principios de Universal Restore

1. Selección de la HAL automática y controladores de almacenamiento masivos.

   Universal Restore busca los controladores en el carpetas de la red que especifique, en dispositivos de arranque y en las carpetas de almacenamiento de controladores predeterminados del sistema que se recupera. Universal Restore analiza el nivel de compatibilidad de todos los discos encontrados e instala los controladores que mejor se adaptan de HAL y almacenamiento masivo en el hardware de destino. También se puede buscar y pasar los controladores para adaptadores de red al sistema operativo que los instala automáticamente cuando se inicia por primera vez.

   *La carpeta de almacenamiento de controladores predeterminada de Windows está determinada en el valor de registro **DevicePath** que se puede encontrar en la clave de registro **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. Esta carpeta de almacenamiento generalmente es WINDOWS/inf.*

2. Selección manual del controlador del dispositivo de almacenamiento masivo.

   El hardware de destino posee un controlador de almacenamiento masivo específico (como por ejemplo, un SCSI, RAID o un adaptador de canal de fibra) para el disco duro. Puede instalar el controlador correspondiente de manera manual y omitir el procedimiento de búsqueda automática e instalación del controlador.

3. Instalación de controladores para dispositivos Plug and Play.

   Universal Restore se basa en el proceso integrado de búsqueda y configuración de Plug and Play y en un proceso de configuración para manejar las diferencias del hardware en dispositivos que no son imprescindibles para el inicio del sistema, como vídeo, audio y USB. Windows controla este proceso durante la fase de inicio de sesión y si no se detecta ningún componente del nuevo hardware, tendrá la oportunidad de instalar manualmente los controladores correspondientes más tarde.

#### Universal Restore y Sysprep de Microsoft

Universal Restore no es una herramienta de preparación del sistema. Puede aplicarla a cualquier imagen de Windows creada con los productos Acronis, incluyendo las imágenes de sistemas preparadas con la herramienta de preparación del sistema de Microsoft (Sysprep). A continuación se muestra un ejemplo del uso de ambas herramientas en el mismo sistema.

Universal Restore no elimina el identificador de seguridad (SID) ni las configuraciones del perfil del usuario para poder ejecutar el sistema inmediatamente después de la recuperación sin volver a unirse al dominio o asignar nuevamente los perfiles de los usuarios de la red. Si desea cambiar las configuraciones anteriores en el sistema recuperado, puede preparar el sistema con la herramienta Sysprep y, si es necesario, crear una imagen y restaurarlo con Universal Restore.

#### Limitaciones

Universal Restore no está disponible.

- Cuando se inicia un equipo con Acronis Startup Recovery Manager (pulse F11) o
- la imagen de copia de seguridad se encuentra en Acronis Secure Zone o
- Cuando utilice Acronis Active Restore,

debido a que estas funciones fueron especialmente diseñadas para la recuperación instantánea de datos en el mismo equipo.

Universal Restore no está disponible cuando se recupera Linux.

#### Obtención de Universal Restore

Universal Restore viene de manera gratuita con Acronis Backup & Recovery 10 Advanced Server SBS Edition y Acronis Backup & Recovery 10 Advanced Server Virtual Edition.

Se puede comprar Universal Restore para las otras versiones del producto, tiene su propia licencia y se instala como característica separada desde el archivo de configuración. Necesita recrear los dispositivos de arranque para que el nuevo complemento instalado sea funcional en el entorno de inicio.

### 2.11.4 Acronis Active Restore

Active Restore es la tecnología propia de Acronis que pone en línea al sistema inmediatamente después de que se inicie la recuperación del sistema.

Los clientes que están familiarizados con Acronis Recovery para Microsoft Exchange pueden darse cuenta de que utiliza Active Restore para conseguir la disponibilidad inmediata de un almacén de información Exchange después de iniciar la recuperación. Si bien están basados en la misma tecnología, la recuperación de Almacén de información procede de manera diferente que la recuperación del sistema operativo que se describe en esta sección.

### Sistemas operativos compatibles

Acronis Active Restore está disponible para la recuperación de Windows desde Windows 2000.

### Limitación

La única ubicación compatible del archivo es un disco local, o más precisamente, cualquier dispositivo disponible por medio del BIOS del equipo. Puede ser Acronis Secure Zone, un disco duro USB, una unidad de memoria flash o cualquier disco duro interno.

### Cómo funciona

Cuando configure una operación de recuperación, seleccione los discos o volúmenes a recuperar desde una copia de seguridad. Acronis Backup & Recovery 10 explora los discos o volúmenes seleccionados en la copia de seguridad. Si la exploración encuentra un sistema operativo compatible, la opción Acronis Active Restore pasa a estar disponible.

Si no habilita la opción, la recuperación del sistema procederá de la manera normal y el equipo estará funcional después de que se complete la recuperación.

Si se habilita la opción, la secuencia de las acciones serán las siguientes.

Una vez que se inició la recuperación del sistema, el sistema operativo inicia desde la copia de seguridad. El equipo se vuelve funcional y listo para proporcionar los servicios necesarios. Se recuperan los datos que se utilizarán para las solicitudes entrantes con la más alta prioridad; todo lo demás se recupera en segundo plano.

Porque las solicitudes de servicio se realizan simultáneamente con la recuperación, se puede retrasar el funcionamiento del sistema incluso si se estableció como **Baja** a la prioridad de recuperación en las opciones de recuperación. De esta manera, el tiempo de inactividad se reduce al mínimo al costo de una aminoración temporal del rendimiento.

### Escenarios de usos:

1. La actividad del sistema es uno de los criterios de eficiencia.

   Ejemplos: Servicios orientados a clientes, revendedores de Web, estaciones de sondeo.
2. La proporción de sistema/espacio de almacenamiento está predispuesto hacia el almacenamiento.

   Se usa algunos equipos como servicios de almacenamiento, en donde el sistema operativo sólo tiene un pequeño segmento y el resto del espacio se dedica a almacenamiento, por ejemplo de películas, sonidos u otros archivos multimedia. Algunos de estos volúmenes de almacenamiento pueden ser muy grandes comparado con el sistema y entonces la mayoría del tiempo se dedicará al recuperación de los archivos, que puede ser usado mucho después o algún momento en el futuro.

   Si opta por Acronis Active Restore, el sistema estará operativo en poco tiempo. Los usuarios podrán abrir los archivos necesarios desde el almacenamiento y usarlos mientras que se recuperan el resto de los archivos, que no son necesarios de manera inmediata, en segundo plano.

   Ejemplos: almacenamiento de colección de películas, colección de música, almacenamiento multimedia.

### Cómo utilizarlo

1. Realice la copia de seguridad del disco del sistema o el volumen a una ubicación accesible por medio del BIOS del equipo. Puede ser Acronis Secure Zone, una unidad de disco duro USB, una unidad de memoria flash o cualquier unidad de disco duro interno.

*Si su sistema operativo y su cargador residen en diferentes volúmenes, debe incluir siempre ambas particiones en la imagen. Los volúmenes debe recuperarse juntos, de otro modo existe el riesgo de que no inicie el sistema operativo.*

2. Creación de dispositivos de arranque.
3. Si se presenta un fallo en el sistema, inicie el equipo con los dispositivos de arranque. Inicie la consola y conecte el agente de inicio.
4. Configure el sistema de recuperación: seleccione el disco de sistema o volumen y seleccione la casilla de verificación **Utilizar Acronis Active Restore**.

   *Acronis Active Restore escogerá el primer sistema operativo que encuentre durante la copia de seguridad para el inicio y la recuperación posterior. No intente realizar recuperaciones con más de un sistema operativo con Active Restore si desea predecir el resultado. Cuando se recupera un sistema con múltiples inicios, escoja sólo un volumen de sistema y un volumen de inicio a la vez.*

5. Una vez que se inició la recuperación del sistema, el sistema operativo inicia desde la copia de seguridad. El icono de Acronis Active Restore aparece en la bandeja del sistema. El equipo se vuelve funcional y listo para proporcionar los servicios necesarios. El usuario inmediato observa el árbol de la unidad y los iconos, puede abrir los archivos o ejecutar aplicaciones , incluso si todavía no se las recuperó.

   Los controladores de Acronis Active Restore interceptan las solicitudes del sistema y establecen la prioridad inmediata para la recuperación de archivos que son necesarios para responder a las solicitudes entrantes. Mientras procede la recuperación "en el momento", el proceso de recuperación continúa en segundo plano.

   *No apague o reinicie el equipo hasta que haya completado la recuperación. Si apaga el equipo, se perderían todos los cambios realizados al sistema desde el último inicio. El sistema no se recuperará ni siquiera parcialmente. La única solución posible en este caso sería reiniciar el proceso de recuperación desde un dispositivo de inicio.*

6. La recuperación en segundo plano seguirá hasta que se recuperen todos los volúmenes seleccionados, se agrega una entrada al registro y desaparece el icono de Acronis Active Restore de la bandeja del sistema.

## 2.12 Comprensión de la gestión centralizada

Esta sección contiene las generalidades de la protección de datos centralizada con Acronis Backup & Recovery 10. Asegúrese de que comprende cómo se protegen los datos en un solo equipo (pág. 27) antes de leer esta sección.

### 2.12.1 Conceptos básicos

#### Aplicar políticas de copias de seguridad y rastrear su ejecución

Para proteger datos en un solo equipo, instala en su equipo uno o varios agentes (pág. 400) para los distintos tipos de datos que desea proteger. Conecta la consola al equipo y crea uno o varios planes de copias de seguridad (pág. 411).

¿Qué ocurre si gestiona cientos de equipos? Lleva un tiempo crear un plan de copias de seguridad en cada equipo, a pesar de que los planes serán bastante parecidos, es decir, necesitará copiar, por ejemplo, la unidad del sistema y los documentos del usuario. Rastrear la ejecución de los planes en cada equipo por separado consume también mucho tiempo.

Para poder propagar las operaciones de gestión a múltiples equipos, instale Acronis Backup & Recovery 10 Management Server (pág. 409) y registre (pág. 412) los equipos en el servidor. Después, puede crear grupos de equipos y, por lo tanto, gestionar múltiples equipos como un todo. Puede proteger todos o aquellos de su elección al configurar un plan de copias de seguridad común, que se denomina política de copias de seguridad (pág. 412).

Una vez que aplica su política a un grupo de equipos, el servidor de gestión difunde la política entre todos los equipos. En cada equipo los agentes encontrarán los elementos objeto de copia de seguridad y crearán planes de copias de seguridad centralizados (pág. 411). Podrá monitorizar los estados de las políticas en una sola pantalla y navegar, en caso de que sea necesario, por cada equipo, plan o tarea para consultar sus estados y entradas de registro. El servidor de gestión también le permite monitorizar y gestionar las actividades originadas localmente por el agente.

El proceso de gestión mediante el cual usted conecta la consola al servidor de gestión en vez de a cada equipo y lleva a cabo todas las operaciones de gestión a través de la unidad de gestión central se denomina gestión centralizada (pág. 406).

La gestión centralizada no realiza la gestión directa (pág. 406) de cada equipo. Puede conectar la consola a cada equipo y realizar cualquier operación de gestión directa. Sin embargo, los planes de copias de seguridad centralizados pueden gestionarse únicamente a través del servidor de gestión, ya que una política correctamente elaborada funciona automáticamente y rara vez necesita de intervención humana.

A través del servidor de gestión, puede crear uno o varios almacenamientos centralizados de archivos comprimidos (bóvedas centralizadas (pág. 402)) que podrá compartir entre los equipos registrados. Cualquier política de copias de seguridad, así como cualquier plan de copias de seguridad creado en los equipos registrados puede utilizar una bóveda centralizada a través de la gestión directa.

### Organizar un almacenamiento de archivo comprimido gestionado

¿Qué capacidad debería tener su bóveda? ¿Que ocurre si transferir copias de seguridad grandes a la bóveda genera el bloqueo de la red? ¿Realizar una copia de seguridad de un servidor de producción en línea afecta el rendimiento del servidor? Para estar seguro de que la copia de seguridad centralizada no ralentizará los procesos comerciales de su empresa y para disminuir el consumo de recursos necesarios para la protección de datos, instale Acronis Backup & Recovery 10 Storage Node (pág. 410) y configúrelo para la gestión de una o varias bóvedas centralizadas. Esas bóvedas se denominan bóvedas gestionadas (pág. 402).

El nodo de almacenamiento ayuda al agente a deduplicar (pág. 404) las copias de seguridad antes de transferirlas a las bóvedas gestionadas y deduplica las copias de seguridad almacenadas en las bóvedas. La desduplicación tiene como resultado la reducción del tráfico de copias de seguridad y el ahorro de espacio de almacenamiento. El nodo de almacenamiento también lleva a cabo operaciones con archivos comprimidos (tales como la validación y la limpieza), que normalmente realiza el agente y, por lo tanto, libera a los equipos registrados de una carga de procesamiento innecesaria. Por último, pero no por ello menos importante, Acronis Backup & Recovery 10 Storage Node permite la utilización de una biblioteca de cintas como bóveda centralizada para el almacenamiento de copias de seguridad de archivos comprimidos.

Varios nodos de almacenamiento, gestionando un número de bóvedas cada uno, pueden configurarse y controlarse centralizadamente desde Acronis Backup & Recovery 10 Management Server.

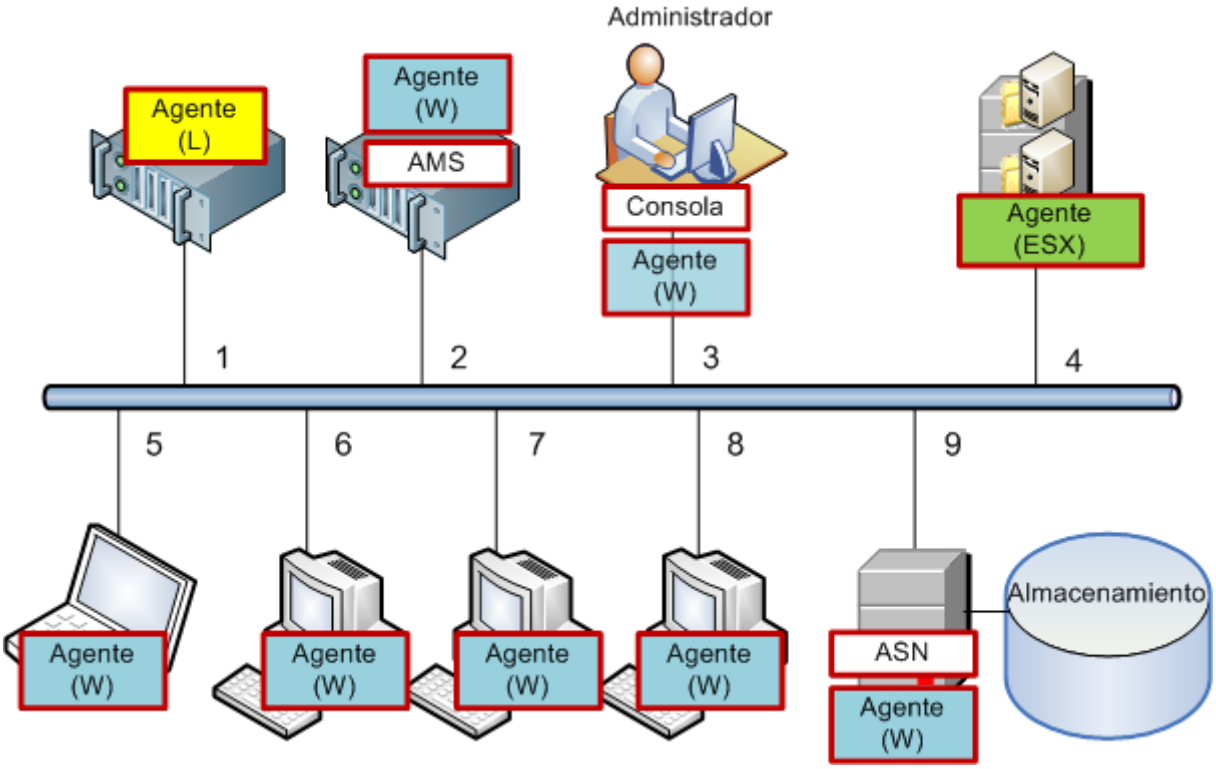
Para obtener más información sobre los nodos de almacenamiento, consulte Acronis Backup & Recovery 10 Storage Node (pág. 20).

## 2.12.2 Configurar la protección de datos centralizada en una red heterogénea

Supongamos que la infraestructura de la red incluye a los servidores (1, 2, 9) y a las estaciones de trabajo (3, 5-8) ejecutándose con Windows y Linux. También tiene un servidor VMware ESX (4) que alberga dos sistemas anfitriones.

Debe proteger cada servidor en conjunto, los datos de los usuarios en las estaciones de trabajo y los equipos virtuales. Si desea poder rastrear la salud de la protección de datos, entonces asegúrese de que los archivos comprimidos de la copia de seguridad no almacenen información duplicada y de que las copias de seguridad obsoletas se eliminen del almacenamiento rápidamente. Estos objetivos pueden lograrse realizando copias de seguridad regulares de los elementos de datos solicitados a una bóveda centralizada con desduplicación.




### Configurar la infraestructura de Acronis

1. Instale la Acronis Backup & Recovery 10 Management Console **[Consola]** en el equipo en el cual prefiere operar **(3)**. La consola le permite acceder y gestionar otros componentes de Acronis a través de la Interfaz gráfica de usuario.
2. Instale el Acronis Backup & Recovery 10 Management Server **[AMS]** en uno de los servidores de Windows **(2)**. El servidor de gestión es su único punto de entrada a la infraestructura de Acronis.
3. Instale el Acronis Backup & Recovery 10 Agente en cada uno de los equipos para realizar una copia de seguridad de los discos, volúmenes o archivos.
   - **Agente (W)** - Agente para Windows
   - **Agente (L)** - Agente para Linux.

   Al instalar los agentes, registre cada uno de los equipos en el servidor de gestión. Para hacerlo, introduzca el nombre del servidor o la dirección IP y las credenciales del administrador del

servidor en la ventana adecuada del asistente para la instalación. O, como alternativa, agregue los equipos al servidor de gestión más tarde utilizando sus nombres o direcciones IP.

4. Instale el agente de Acronis Backup & Recovery 10 para ESX/ESXi **[Agente (ESX)]** en el servidor ESX **(4)** para realizar una copia de seguridad de las máquinas virtuales del servidor. El agente se entrega como dispositivos virtuales.
5. Instale el Acronis Backup & Recovery 10 Storage Node **[ASN]** en uno de los servidores de Windows **(9)**. El nodo de almacenamiento le permite organizar la infraestructura para almacenar la copia de seguridad de los archivos comprimidos y utilizar la funcionalidad de desduplicación. El nodo puede instalarse junto con el servidor de gestión si el servidor dispone de la capacidad suficiente.

   Al instalar el nodo de almacenamiento, regístrelo en el servidor de gestión de la misma manera en la que registra los agentes.

**Consejos de instalación**

- Tanto AMS como ASN pueden instalarse también en el sistema operativo de una estación de trabajo.
- Pueden haber múltiples nodos de almacenamiento en la red. Cada nodo puede gestionar hasta 20 bóvedas locales o remotas.
- Pueden instalarse múltiples componentes de Acronis Backup & Recovery 10 en un equipo con un único procedimiento de instalación.
- En un dominio Active Directory, puede implementar los componentes utilizando la Política de grupo.

### Configurar el nodo de almacenamiento

Antes de utilizar el nodo de almacenamiento, asegúrese de que todos los usuarios que realizarán una copia de seguridad en las bóvedas del nodo dispongan de cuentas de Windows en el nodo.

- Si el nodo está incluido en un dominio Active Directory, todos los usuarios de dominio podrán realizar copias de seguridad en el nodo; y todos los administradores del dominio se convertirán en administradores del nodo.
- En un grupo de trabajo, cree una cuenta de usuario local para cada usuario que realizará una copia de seguridad en el nodo. Los miembros del grupo de Administradores se convierten en los administradores del nodo. Puede agregar más cuentas según se necesite más adelante.

1. Ejecute la consola, conéctese al servidor de gestión.
2. Cree una bóveda gestionada como se describe en Operaciones con bóvedas centralizadas (pág. 133). Permita la desduplicación al crear una bóveda gestionada.

### Configurar grupos y políticas

La explicación detallada de cuándo y por qué necesita organizar los grupos de los equipos puede encontrarse en la sección Agrupar los equipos registrados (pág. 60). Aquí hay algunas situaciones hipotéticas compatibles con la implementación de Acronis Backup & Recovery 10 anteriormente mencionada.

## Proteger los servidores

Lo más probable será que cree planes de copia de seguridad individuales en cada servidor dependiendo de sus roles. Pero es necesario realizar una copia de seguridad completa del servidor completo al menos una vez. Puede que desee realizar una copia de seguridad del servidor durante una ventana de mantenimiento o una ventana de copia de seguridad, después de instalar o actualizar el software, antes de la reubicación, etc. En nuestro ejemplo, no es necesario realizar copias de

seguridad de servidores completos de manera regular. Puede eliminar manualmente viejas copias de seguridad ya que no son numerosas.

1. Cree una política que realice una copia de seguridad de [**Todos los volúmenes**] en la bóveda gestionada en el nodo de almacenamiento. Elija **Realizar copia de seguridad más tarde,** inicio manual y tipo de copia de seguridad **Completa**.
2. Cree un grupo estático llamado, por ejemplo, S_1. Agregue todos los servidores a este grupo. (Puede agregarse un nodo de almacenamiento en caso de que la bóveda gestionada no esté en los discos del nodo local. De lo contrario, el almacenamiento del archivo comprimido realizará una copia de seguridad en si mismo).
3. Aplique la política al grupo S_1. Asegúrese que la política se haya implementado correctamente en cada uno de los servidores. El estado de implementación de políticas debe cambiar de **Implementando** a **Implementado** y su estatus debe ser **OK**. Para ver los planes de copias de seguridad resultantes en cada uno de los servidores:
   a. navegue hasta el grupo **Todos los equipos** o hasta el grupo S_1
   b. seleccione el servidor
   c. seleccione la pestaña **Tareas y planes de copias de seguridad** en el panel **Información**.

Cuando lo necesite y tenga la oportunidad de realizar una copia de seguridad de cada uno de los servidores, navegue hasta el plan de copias de seguridad como se describe arriba, seleccione el plan y ejecútelo.

## Protección de las estaciones de trabajo

Cómo configurar la programación más popular: copia de seguridad completa semanal y copia de seguridad incremental diaria de las carpetas predeterminadas de documentos de los usuarios. Además, retendremos las copias de seguridad solo durante 7 días.

1. Cree una política que realice una copia de seguridad de [**Todas las carpetas del perfil**] en la bóveda gestionada en el nodo de almacenamiento. Esto realizará una copia de seguridad de la carpeta donde están ubicados los perfiles de usuarios (por ejemplo, C:\Documents and Settings en Windows XP). Elija el esquema de copia de seguridad **Personalizado**.
   a. Programe la copia de seguridad completa de la siguiente manera: **Semanalmente**, cada 1 semana(s) los: domingos, ejecute la tarea una vez a las 12:00:00. Configuraciones avanzadas: Wake-on-LAN: Activado. También querrá distribuir la hora de inicio de la copia de seguridad dentro de la ventana de tiempo para optimizar la utilización de la red y la carga del CPU del nodo de almacenamiento.
   b. Programe la copia de seguridad incremental de la siguiente manera: **Semanalmente**, cada 1 semana(s) los: domingos, ejecute la tarea una vez a las 08:00:00 p.m. Establezca también las configuraciones avanzadas según sus necesidades.
   c. Configure las reglas de retención de la siguiente manera: **Eliminar las copias de seguridad anteriores a**: 7 días. **Cuando se elimine una copia de seguridad que tiene dependencias:** Consolidar las copias de seguridad. No cambie las configuraciones predeterminadas del resto de las reglas de retención. En **Aplicar reglas de retención**, establezca **Después de la copia de seguridad**.
2. Cree un grupo dinámico llamado, digamos, W_1. Especifique **%Windows%XP%** y **%Windows%Vista%** como criterios. De esta manera, cualquier estación de trabajo que se registre en el servidor de gestión más tarde se añadirá a este grupo y estará protegida por la misma política.
3. Aplique la política al grupo W_1. Asegúrese que la política se haya implementado correctamente en cada una de las estaciones de trabajo. El estado de implementación de políticas debe cambiar

de **Implementando** a **Implementado** y su estatus debe ser **OK**. Para ver los planes de copias de seguridad resultantes en cada uno de las estaciones de trabajo:

a. navegue hasta el grupo **Todos los equipos** o hasta el grupo W_1
b. seleccione la estación de trabajo
c. seleccione la pestaña **Tareas y planes de copia de seguridad** en el panel de **Información**.

También puede ver las tareas resultantes, creadas en las estaciones de trabajo, en la vista **Tareas**.

4. Utilice la vista **Tablero de control** o **Tareas** para rastrear las actividades diarias relacionadas con la política. Una vez que se asegure de que todas las tareas se ejecuten como se especifica, solo puede verificar el estado de la política en la vista **Políticas de copia de seguridad**.

Para proteger los datos diariamente, también puede utilizar los esquemas de copia de seguridad GFS o Torres de Hanói.

### Proteger los equipos virtuales

El agente de Acronis Backup & Recovery 10 para ESX/ESXi proporciona la flexibilidad para proteger las máquinas virtuales de muchas formas:

- Conecte la consola a la aplicación virtual (agente para ESX/ESXi) y cree un plan de copias de seguridad que realizará una copia de seguridad de algunos o todos los equipos virtuales.
- Conecte la consola a la aplicación virtual (agente para ESX/ESXi) y cree un plan de copias de seguridad individual para cada equipo. El plan realizará una copia de seguridad de los volúmenes que especifique.
- Registre la aplicación virtual (agente para ESX/ESXi) en el servidor de gestión. Todas las máquinas virtuales, excepto la aplicación virtual, aparecerán en el grupo **Todas las máquinas virtuales**. Puede agrupar estos equipos y aplicar cualquier política que realice una copia de seguridad de discos o volúmenes a ellos.
- Instale Agent para Windows o Agent para Linux en cada máquina virtual. Registre los equipos en el servidor de gestión. Los equipos se considerarán equipos físicos. Puede aplicar una política de copias de seguridad a estos equipos o crear un plan de copias de seguridad en cada equipo de manera separada. Si alguno de los equipos cumple con los criterios de membresía establecidos para un grupo dinámico de equipos físicos, el equipo estará protegido por la política aplicada a este grupo.

Las ediciones avanzadas de los productos que no sean la Edición virtual (Acronis Backup & Recovery 10 Advanced Server, Advanced Server SBS Edition y Advanced Workstation) permiten la utilización de solo el último de los métodos anteriores.

## 2.12.3 Agrupar los equipos registrados

En el momento en el que su equipo se encuentre registrado (pág. 412) en el servidor de gestión, el equipo aparece en el **grupo incorporado** Todos los equipos (pág. 408). Al aplicar una política de copias de seguridad a este grupo, protegerá todos los equipos. El caso es que un sola política puede no satisfacer todas la necesidades, dado que los equipos tienen diferentes roles. Los datos de la copia de seguridad son específicos para cada departamento; las copias de seguridad de algunos datos deben realizarse frecuentemente, otras, sin embargo, dos veces al año; por lo tanto, podría necesitar crear varias políticas para los diferentes grupos de equipos. En este caso, considere la creación de grupos personalizados.

## 2.12.4 Políticas sobre equipos y grupos

Esta sección le ayudará a comprender las políticas de revocación e implementación automática realizadas por el servidor de gestión cuando se aplica una política o varias políticas a equipos y grupos de equipos anidados en varias combinaciones, cuando se revoca una política de equipos o grupos, cuando se mueve un equipo o grupo de un grupo a otro.

Las operaciones con grupos a los cuales se aplican las políticas de copia de seguridad provocarán un cambio en las políticas de los equipos miembros. Siempre que se efectúa un cambio de jerarquía, es decir, cada vez que se mueven, eliminan o crean grupos, se agregan equipos a grupos estáticos o cuando los equipos ingresan a un grupo basado en criterios dinámicos, pueden ocurrir una cantidad enorme de cambios por herencia. Familiarícese con esta sección para asegurarse de que sus acciones alcancen los resultados deseados y para comprender el resultado de las operaciones automáticas de Acronis Backup & Recovery 10 Management Server.

### ¿Qué es aplicar, implementar y revocar?

**Aplicar** una política permite establecer una correspondencia entre la política y uno o más equipos. Este proceso se lleva a cabo dentro de la base de datos del servidor de gestión y no demora mucho tiempo.

**Implementar** una política permite transferir la correspondencia establecida a esos equipos. Físicamente, se crea un paquete de tareas en cada equipo, de acuerdo con la configuración proporcionada por la política.

**Revocar** una política es la acción inversa a la aplicación y la implementación en conjunto. Al revocar, se elimina la correspondencia entre la política y uno o más equipos, y luego se eliminan las tareas de los equipos.

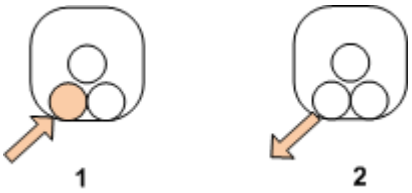
Si un equipo no está disponible o al alcance en un momento determinado, el cambio se propagará en el equipo una vez que este se encuentre disponible. Esto significa que implementar una política en múltiples equipos no es una acción inmediata. Lo mismo sucede al revocar. Estos dos procesos pueden demorar un tiempo, por lo que el servidor de gestión realiza el rastreo y muestra los estados individuales de cada equipo con el que trabaja, al igual que el estado acumulado de la política.

### Una política en un equipo o grupo

En los siguientes diagramas, cada esquema numerado ilustra el resultado de la acción numerada correspondiente.

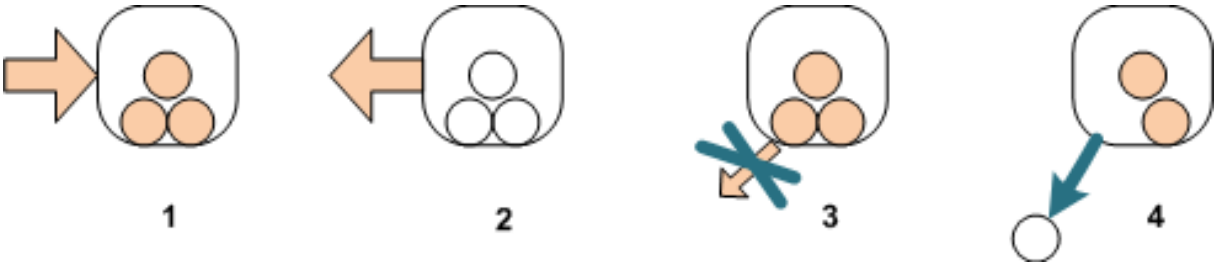
El contenedor representa un grupo, el círculo de color representa un equipo al que se le ha aplicado una política, el círculo negro representa un equipo al que no se le ha aplicado la misma política, el círculo blanco representa un equipo al que no se le ha aplicado ninguna política.

#### Una política en un equipo



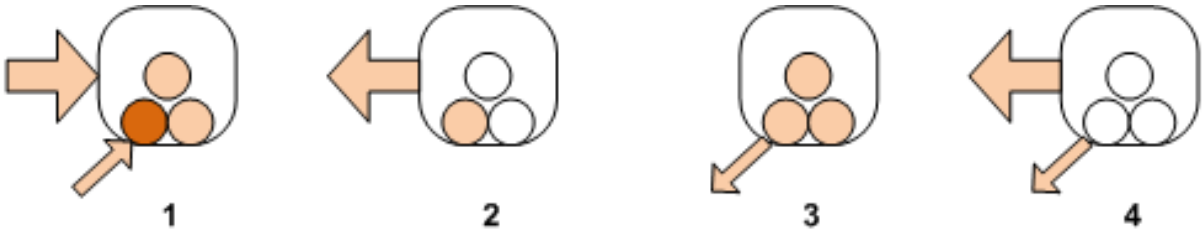

1. Se puede aplicar una política a un equipo.
2. Se puede revocar una política de un equipo.

**Una política en un grupo**




1. Se puede aplicar una política a un grupo.
2. Se puede revocar una política de un grupo.
3. No se puede revocar de un equipo una política que se ha aplicado a un grupo.
4. Para revocar una política de un equipo, elimine el equipo del grupo.

**La misma política en un grupo y en un equipo**




1. Se puede aplicar la misma política a un grupo y a un equipo. No cambia nada en el equipo al aplicar una misma política por segunda vez, pero el servidor recuerda que la política se ha aplicado dos veces.
2. Cuando se revoca una política del grupo, la misma permanece en el equipo.
3. Cuando se revoca una política del equipo, la misma permanece en el grupo y, por lo tanto, en el equipo.
4. Para revocar por completo la política del equipo, revóquela tanto del equipo como del grupo.

## Operaciones con un equipo

Esta sección es una ilustración simplificada de lo que sucede con las políticas en un equipo cuando el mismo se mueve, copia o elimina de un grupo.

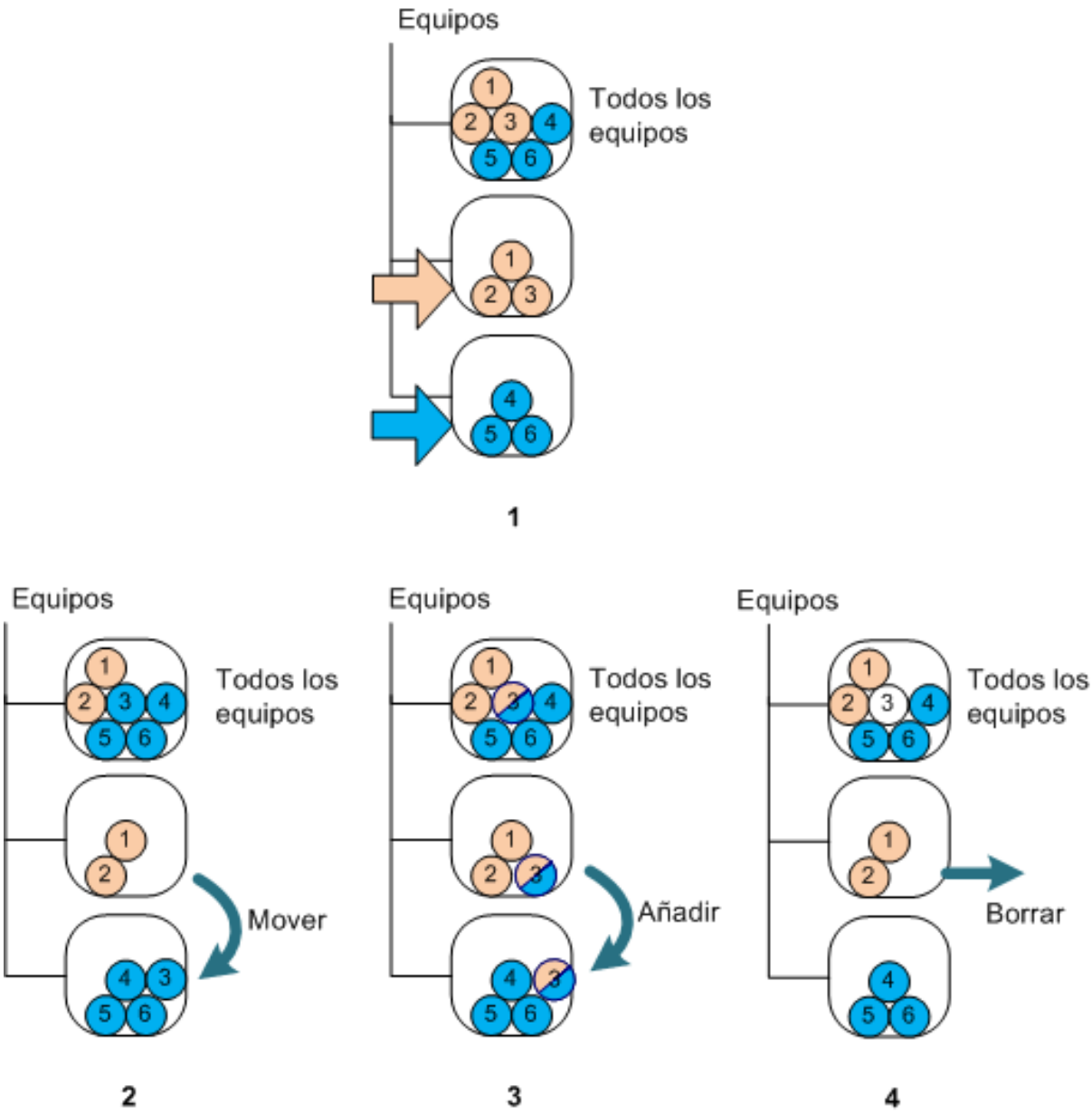
En el siguiente diagrama, el contenedor representa un grupo; el círculo de un color representa un equipo al que se le ha aplicado una política, el círculo de dos colores representa un equipo al que se le han aplicado dos políticas, el círculo blanco representa un equipo al que no se le ha aplicado ninguna política.

1. Este es el estado inicial: dos grupos personalizados contienen equipos diferentes. Se aplica una política a un grupo y otra política a otro grupo. Los siguientes esquemas ilustran los resultados de las acciones especificadas.

2. **Mover a otro grupo:** Se mueve el equipo n.º 3 de un grupo a otro. Se revoca la política "naranja", se aplica la política "azul" al equipo.

3. **Añadir a otro grupo**: Se agrega el equipo n.º 3 a otro grupo. Ahora, es miembro de ambos grupos. Se aplica la política "azul" pero la "naranja" permanece en el equipo.

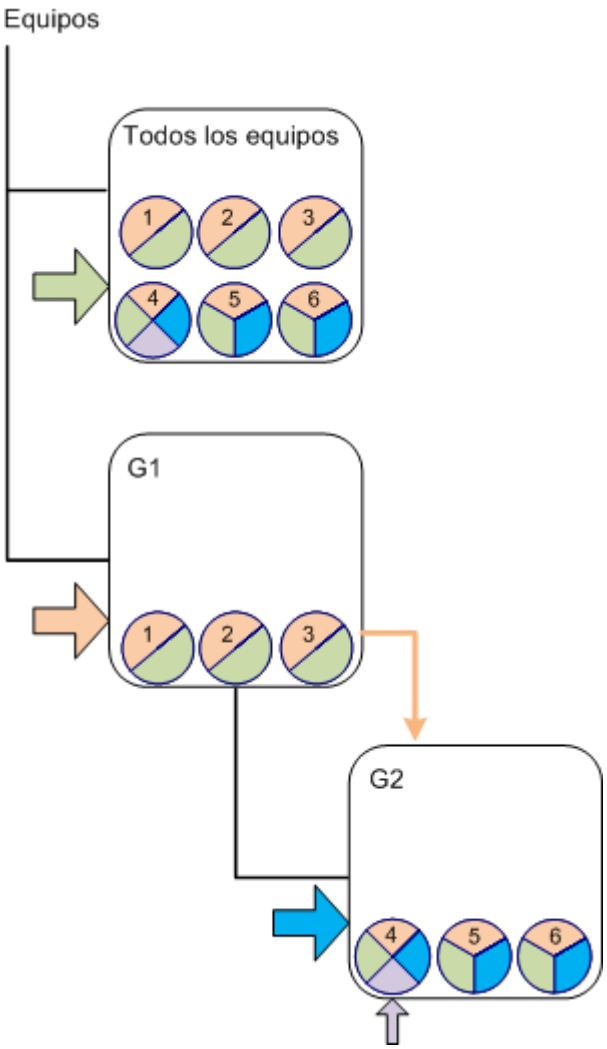
4. **Eliminar del grupo**: Se elimina el equipo n.º 3 del grupo. Se revoca la política "naranja" del equipo. El equipo permanece en el grupo **Todos los equipos**.




## Herencia de políticas.

La herencia de políticas se puede comprender fácilmente si asumimos que el equipo puede ser miembro únicamente de un grupo además del grupo **Todos los equipos**. Empecemos basándonos en este enfoque simplificado.

En el siguiente diagrama, el contenedor representa un grupo, el círculo de dos colores representa un equipo al que se le han aplicado dos políticas, el círculo de tres colores representa un equipo al que se le han aplicado tres políticas, y así sucesivamente.




Además del grupo **Todos los equipos**, está el grupo personalizado G1 en la raíz y el grupo personalizado G2, que es secundario de G1.

Todos los equipos heredan la política "verde" que se le ha aplicado al grupo **Todos los equipos**.

Los miembros de G1 y todos sus grupos secundarios, ya sean inmediatos o indirectos, heredan la política "naranja" que se le ha aplicado a G1.

Únicamente los miembros de G2 heredan la política "azul" que se le ha aplicado a G2, ya que el mismo no tiene grupos secundarios.

Se aplica la política "violeta" directamente al equipo n.º 4. La misma existirá en el equipo n.º 4 independientemente si este equipo es miembro de algún grupo o no.

Supongamos que creamos el grupo G3 en la raíz. Si no se aplica ninguna política al grupo, se supone que todos sus miembros son "verdes". Pero si añadimos, por ejemplo, el equipo n.º 1 a G3, el mismo tendrá tanto la política "naranja" como la "verde", independientemente de que G3 no tenga nada que ver con la política "naranja".

Por eso es tan difícil rastrear la herencia de las políticas desde la cima de la jerarquía cuando el equipo forma parte de múltiples grupos.

En la práctica, es mucho más sencillo ver la herencia desde el lado de los equipos. Para eso, navegue en cualquier grupo que contenga el equipo, seleccione el equipo y luego la pestaña **Políticas de copia de seguridad** en el panel **Información**. La columna **Herencia** muestra si una política ha sido heredada o si se le ha aplicado directamente al equipo. Haga clic en **Explorar herencia** para ver el orden de herencia de la política. En nuestro ejemplo, los nombres de las políticas, la columna **Herencia** y el orden de herencia serán los siguientes:

| Para el equipo | Nombre de la política | Herencia | Orden de la herencia |
|---|---|---|---|
| n.º 1 o n.º 2 o n.º 3 | "verde" | Heredada | Todos los equipos -> n.º 1 o n.º 2 o n.º 3 |
| | "naranja" | Heredada | G1 -> n.º 1 o n.º 2 o n.º 3 |

| | | | |
|---|---|---|---|
| n.º 4 | "verde" | Heredada | Todos los equipos -> n.º 4 |
| | "naranja" | Heredada | G1-> G2-> n.º 4 |
| | "azul" | Heredada | G2 -> n.º 4 |
| | "violeta" | Aplicada directamente | |
| n.º 5 o n.º 6 | "verde" | Heredada | Todos los equipos -> n.º 5 o n.º 6 |
| | "naranja" | Heredada | G1 -> G2-> n.º 5 o n.º 6 |
| | "azul" | Heredada | G2 -> n.º 5 o n.º 6 |

### 2.12.5 Estado y estatus de la política de copias de seguridad

La gestión centralizada implica que el administrador pueda monitorizar el centro de la infraestructura del producto completo utilizando unos poco parámetros fáciles de entender. El estado y el estatus de una política de copias de seguridad se incluyen en esos parámetros. Si se produce algún problema, surgirá de la parte más interna de la estructura (tareas en los equipos gestionados) hasta afectar al estatus de políticas acumuladas. El administrador comprueba el estatus rápidamente. Si el estatus no es OK, el administrador puede navegar hasta los detalles del problema a través de unos pocos clics.

Esta sección le ayuda a entender los estados y estatus de las políticas que muestra el servidor de gestión.

#### Estado de implementación de políticas en un equipo

Para ver este parámetro, seleccione cualquier grupo que contenga el equipo del árbol, después seleccione el equipo y, a continuación, seleccione la pestaña **Políticas de copia de seguridad** en el panel **Información**.

Una vez que aplique la política a un equipo o a un grupo de equipos, el servidor implementa la política a los equipos. En cada uno de los equipos, el agente crea un plan de copias de seguridad. Mientras la política se transfiere al equipo y se está creando el plan de copias de seguridad, el estado de implementación de la política del equipo está en **Implementando**.

Una vez que se crea correctamente el plan de copias de seguridad, el estado de la política en el equipo se convierte en **Implementado**.

Puede que sea necesario modificar la política por alguna razón. Una vez que confirme los cambios, el servidor de gestión actualiza la política en todos los equipos en los que se haya implementado la política. Mientras se transfieren los cambios al equipo y el agente actualiza el plan de copias de seguridad, el estado de la política del equipo será **Actualizando**. Una vez que se actualiza la política, su estado se convierte nuevamente en **Implementado**. Este estado significa que la política está funcionando y actualmente no se está realizando ningún cambio.

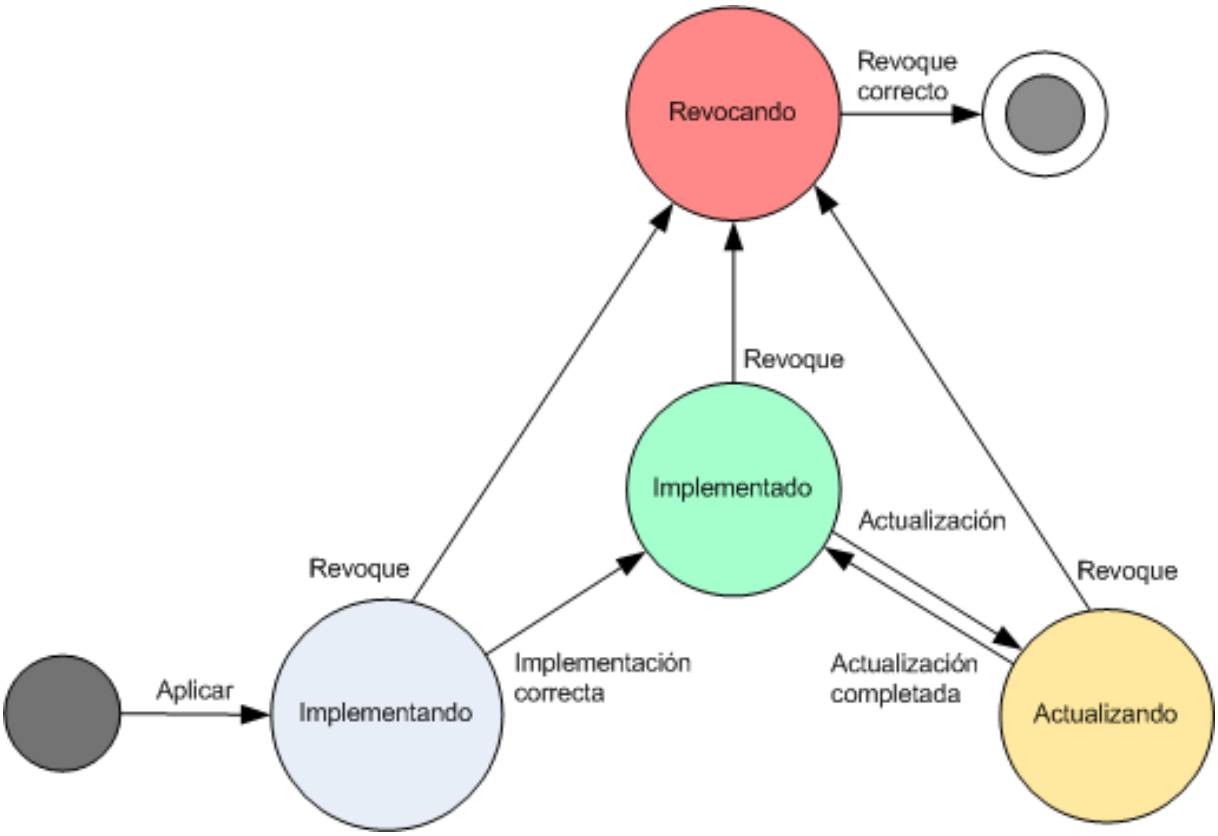
Una política que se ha modificado mientras se ha estado implementando permanece en el estado **Implementado**. El servidor de gestión comienza a implementar la política modificada desde el comienzo.

Puede que sea necesario revocar la política del equipo o del grupo en el que está incluido el equipo. Una vez que confirme los cambios, el servidor de gestión revoca la política del equipo. Mientras se

transfieren los cambios al equipo y el agente elimina el plan de copias de seguridad, el estado de la política del equipo será **Revocando**.

Puede cambiar las condiciones de agrupación o el equipo puede cambiar sus propiedades para que el equipo deje un grupo y se incluya en otro. Esto puede hacer que se revoque una política e implemente otra. En este caso, el estado de la primera política en el equipo será **Revocando** y el estado de la segunda política será **Implementando**. Las políticas pueden aparecer en la GUI simultáneamente o una tras otra.

Diagrama del estado de la política de copias de seguridad




## Estado de una política en un equipo

Para ver este parámetro, seleccione cualquier grupo de equipos en el árbol, después seleccione el equipo y, a continuación, seleccione la pestaña de **Políticas de copia de seguridad** en el panel de **Información**.

En cada uno de los estados, la política de copia de seguridad puede tener uno de los siguientes estatus: **Error**; **Advertencia**; **OK**. Mientras la política está en el estado **Implementado**, su estatus refleja si la política se ejecuta correctamente. Mientras la política está en otro estado, su estatus refleja si la política se está modificando.

**Estado de la política cuando no se encuentran en el equipo los datos de los que se debe realizar la copia de seguridad**

Se puede aplicar una política de copias de seguridad a un equipo que no tenga datos que cumplan con las reglas de selección (p. 413). No se registrará ningún error ni advertencia durante la implementación de la política ya que se asume que los datos pueden aparecer en el futuro. Se crea un plan de copias de seguridad como de costumbre y se cambia el estado de la política a **Implementada**.

Si no se encuentran datos para realizar la copia de seguridad cuando comienza la tarea de copia de seguridad, la tarea fallará y el estado de la política se cambiará a **Error**. Si se encuentra al menos un elemento de los datos, la tarea de copia de seguridad se completará con una advertencia. El estado de la política cambiará según corresponda.

Las tareas de copia de seguridad comenzarán según lo previsto como lo especifica la política y generarán un resultado similar hasta que todos los elementos de los datos aparezcan en el equipo o la política esté editada para que excluya los elementos de los datos no existentes.

**Ejemplos**

Supongamos que la regla de selección establece que la política debe realizar una copia de seguridad de los volúmenes D: y F:. La política se aplica a los equipos con Linux y Windows. Una vez que comienza la primera copia de seguridad, la política obtiene el estado de **Error** en los equipos con Linux y en los equipos con Windows que no tengan dichos volúmenes. La política obtiene el estado de **Advertencia** en los equipos con Windows que tengan volúmenes D: o F: a menos que ocurra un evento que ocasione un error.

La política que debe realizar una copia de seguridad del [Sistema] y de los volúmenes /dev/sda1, obtendrá un estado de **Advertencia** en los equipos con Windows (ya que /dev/sda no se encuentra) y en los equipos con Linux que tengan el volumen /dev/sda1 (ya que no se encuentra el volumen [Sistema]). La política obtendrá el estado de **Error** en los equipos con Linux que no tengan un dispositivo SCSI.

La siguiente tabla proporciona detalles.

| Estado | Estado | Descripción |
|---|---|---|
| **Implementando** | **Error** | El registro de implementación tiene errores, por ejemplo, no tiene espacio de disco suficiente |
| | **Advertencia** | El registro de implementación contiene advertencias: el equipo se ha desconectado durante la implementación; no se puede conectar durante N días… |
| | **OK** | El registro de implementación no tiene errores ni advertencias |
| **Implementado** | **Error** | El estatus del plan de copia de seguridad correspondiente es **Error** |
| | **Advertencia** | El estatus del plan de copia de seguridad correspondiente es **Advertencia** |
| | **OK** | El estatus del plan de copia de seguridad correspondiente es **OK** |
| **Actualizando** | **Error** | El registro de actualización contiene errores: no se puede eliminar la tarea bloqueada, el servicio de Acronis se ha detenido… |
| | **Advertencia** | El registro de actualización contiene advertencias |
| | **OK** | El registro de actualización no tiene errores ni advertencias |
| **Revocando** | **Error** | El registro de revocación contiene errores |
| | **Advertencia** | El registro de revocación contiene advertencias |
| | **OK** | El registro de revocación no contiene errores ni advertencias |

Además del estado y estatus de implementación relacionados con un equipo específico, la política de copia de seguridad tiene el estado y estatus de implementación en un grupo de equipos y el estado y estatus de implementación acumulativo de la política.

## Estado de implementación de políticas en un grupo

Para ver este parámetro, seleccione cualquier grupo en el árbol **Equipos**, después seleccione el grupo y, a continuación, seleccione la pestaña **Políticas de copia de seguridad** en el panel **Información**.

Este estado está definido como una combinación de estados de implementación de la política en los equipos incluidos en el grupo y en sus grupos secundarios.

Por ejemplo, ha aplicado la política al grupo que consiste de los equipos A y B. Mientras se lleva a cabo la implementación en ambos equipos, el estado de la política en el grupo será "Implementando". Si la implementación se completa en uno de los equipos mientras continúa en el otro, el estado será "Implementando, Implementado". Cuando la implementación se completa en ambos equipos, el estado será "Implementado".

## Estado de una política en un grupo

Para ver este parámetro, seleccione cualquier grupo en el árbol **Equipos**, después seleccione el grupo y, a continuación, seleccione la pestaña **Políticas de copia de seguridad** en el panel **Información**.

Esta estatus está definido como el estado más grave de la política en los equipos incluidos en el grupo y sus grupos secundarios. Si actualmente no se aplica la política a ningún equipo, su estatus es "OK".

## Estado y estatus acumulativo de una política

Además del estado y estatus de implementación relacionados a un equipo o grupo específico, la política de copias de seguridad tiene un estado de implementación acumulativo y un estatus acumulativo.

### El estado acumulativo de una política de copias de seguridad

Para ver este parámetro, seleccione **Políticas de copia de seguridad** en el árbol. La columna del **Estado de implementación** muestra el estado de implementación acumulativo de cada política.

Este estado está definido como la combinación de estados de implementación de la política en todos los equipos en los que se ha aplicado la política (directamente o a través de herencia). Si actualmente no se aplica la política a ningún equipo, esta no tienen ningún estado de implementación y la columna muestra "No aplicada".

Por ejemplo, ha aplicado la política al equipo A. La política se ha implementado correctamente. A continuación, modifica la política e inmediatamente la aplica al grupo que incluye los equipos B y C. La política debe actualizarse en A e implementarse en B y C. Mientras se lleven a cabo los procesos, el estado acumulativo de la política puede aparecer como "Actualizando, Implementando" y después cambiar a "Actualizando, Implementado" o "Implementado, Implementando" y normalmente terminará en "Implementado".

### El estatus acumulativo de una política de copias de seguridad

Para ver este parámetro, seleccione **Políticas de copia de seguridad** en el árbol. La columna de **Estatus** muestra el estatus acumulativo de cada política.

Esta estatus está definido como el estatus más grave de la política en todos los equipos a los que se ha aplicado la política. Si no se aplica la política a ningún equipo, su estatus es "OK".

## 2.12.6 Deduplicación

Esta sección describe la deduplicación, un mecanismo diseñado para eliminar la repetición de datos al almacenar los datos idénticos solo una vez en los archivos comprimidos.

### Generalidades

La desduplicación es el proceso de minimizar el espacio de almacenamiento que ocupan los datos por medio de la detección de la repetición de los datos y el almacenamiento de los datos idénticos una sola vez.

Por ejemplo, si una bóveda gestionada en la que la desduplicación está activa contiene dos copias del mismo archivo, tanto en el mismo archivo comprimido como en archivos comprimidos diferentes, el archivo se almacena una sola vez y se almacena un enlace en lugar del segundo archivo.

La desduplicación reduciría también la carga de la red: si, durante una copia de seguridad, se encuentran archivos o bloques del disco que son duplicados de archivos o bloques ya almacenados, su contenido no se transfiere a la red.

La desduplicación se lleva a cabo en bloques de disco (desduplicación a nivel de bloque) y en archivos (desduplicación a nivel de archivos) para las copias de seguridad a nivel de disco y a nivel de archivo, respectivamente.

En Acronis Backup & Recovery 10, la desduplicación incluye dos pasos:

**Deduplicación en el origen**

Realizada por un equipo gestionado durante la copia de seguridad. Acronis Backup & Recovery 10 Agente utiliza el nodo de almacenamiento para determinar qué datos pueden deduplicarse y no transfiere los datos cuyos duplicados ya están presentes en la bóveda.

**Deduplicación en el destino**

Realizada en la bóveda cuando se ha completado una copia de seguridad. El nodo de almacenamiento analiza los archivos comprimidos y deduplica los datos en la bóveda.

Cuando se crea un plan de copias de seguridad, es posible desactivar la desduplicación en el origen para ese plan. En este caso, las copias de seguridad serán más rápidas pero se generará una mayor carga en la red y en el nodo de almacenamiento.

**Bóveda de deduplicación**

Una bóveda centralizada gestionada en la que la deduplicación está activa se denomina *bóveda de deduplicación*. Cuando se crea una bóveda centralizada, es posible especificar si activar o no la deduplicación. No se puede crear una bóveda de deduplicación en un dispositivo de cinta.

#### Base de datos de deduplicación

Acronis Backup & Recovery 10 Storage Node gestiona una bóveda de desduplicación, conserva la base de datos de desduplicación, la cual contiene los valores hash de todos los elementos almacenados en la bóveda, excepto de aquellos que no se pueden deduplicar, como los archivos cifrados.

Al crear una bóveda, la base de datos de desduplicación se almacena en la carpeta especificada en **Ruta de la base de datos** en la vista **Crear bóveda centralizada**. La base de datos de desduplicación solo puede crearse en una carpeta local.

El tamaño de la base de datos de desduplicación constituye aproximadamente un uno por ciento del tamaño total de los archivos comprimidos de la bóveda. En otras palabras, por cada terabyte de nuevos datos (no duplicados) añadidos, se añaden 10 GB a la base de datos.

En caso de que se dañe la base de datos o se pierda el nodo de almacenamiento, mientras la bóveda conserva los archivos comprimidos y la carpeta de servicio que contiene los metadatos, el nodo de almacenamiento nuevo vuelve a explorar la bóveda y crea de nuevo la base de datos.

## Cómo funciona la deduplicación

### Deduplicación en el origen

Al realizar una copia de seguridad de una bóveda de deduplicación, el Acronis Backup & Recovery 10 Agent lee los elementos que se están copiando, bloques de disco para la copia de seguridad de los discos o archivos para la copia de seguridad de archivos, y calcula una impresión digital de cada bloque. Dicha impresión digital, generalmente llamada un *valor hash,* representa únicamente el contenido del elemento dentro de la bóveda.

Antes de enviar el elemento a la bóveda, el agente le pide a la base de datos de deduplicación que determine si el valor hash del elemento es el mismo que el de algún elemento ya almacenado.

Si es así, el agente solo envía el valor hash del elemento; de lo contrario, envía el elemento.

Algunos elementos, como archivos cifrados o bloques de discos de un tamaño no estándar, no pueden deduplicarse y el agente siempre transfiere dichos elementos a la bóveda sin calcular sus valores hash. Para obtener más información acerca de las restricciones de deduplicación a nivel de archivos y a nivel de discos, consulte Restricciones de deduplicación (pág. 72).

### Deduplicación en el destino

Una vez se completa la copia de seguridad de una bóveda de deduplicación, el nodo de almacenamiento ejecuta **tarea de indexación** para deduplicar los datos en la bóveda como se explica a continuación.

1. Mueve los elementos (bloques del disco o archivos) desde los archivos comprimidos a una carpeta especial dentro de la bóveda, almacenando allí los elementos duplicados sólo una vez. Esta carpeta se denomina **almacenamiento de datos de deduplicación**. Si ambas copias de seguridad, del nivel del disco y del nivel del archivo están en la bóveda, habrá para ellas dos almacenamientos de datos separados. Los elementos que no pueden deduplicarse permanecen en los archivos comprimidos.
2. En los archivos comprimidos, reemplaza los elementos movidos por las referencias correspondientes que conducen a los mismos.

Como resultado, la bóveda contiene una cantidad de elementos deduplicados y únicos, cada uno con una o más referencias desde los archivos comprimidos de la bóveda.

Es posible que la tarea de indexación necesite un tiempo considerable para completarse. Puede ver el estado de esta tarea en la vista **Tareas** del management server.

### Compactando

Después de que se borren una o más copias de seguridad o archivos comprimidos de la bóveda, ya sea manualmente o durante la limpieza, la bóveda puede contener elementos que ya no tienen referencia desde ningún archivo comprimido. Dichos elementos serán eliminados por la **tarea de compactación,** la cual es una tarea programada llevada a cabo por el nodo de almacenamiento.

De manera predeterminada, la tarea de compactación se ejecuta cada sábado por la noche a las 03:00am.Puede reprogramar la tarea como se describe en Acciones en nodos de almacenamiento (pág. 344), bajo "Cambiar la programación de la tarea compactada". También puede iniciar o detener la tarea manualmente desde la vista **Tareas**.

Debido a que la eliminación de elementos no utilizados consume recursos, la tarea de compactación la realiza únicamente cuando se ha acumulado una cantidad de datos suficiente para eliminar. El umbral viene determinado por el parámetro de configuración **Umbral de inicio de compactación** (pág. 361).

## En qué momentos es más eficaz la deduplicación

Los siguientes son los casos en los que la deduplicación genera los efectos máximos:

- Cuando se realizan copias de seguridad de datos similares de diferentes fuentes en el **modo de copia de seguridad completa**. Este es el caso cuando se hacen copias de seguridad de sistemas operativos y aplicaciones implementadas de una única fuente en la red.
- Cuando se hacen **copias de seguridad incrementales** de datos similares de fuentes diferentes, siempre y cuando los **cambios que se hacen a los datos también sean similares**. Este es el caso cuando se implementan actualizaciones de estos sistemas y se aplican las copias de seguridad incrementales.
- Cuando se hacen **copias de seguridad incrementales** de datos que no cambian en su contenido, pero **cambian su ubicación**. Este es el caso cuando circulan múltiples partes de datos en la red o dentro de un sistema. Cada vez que se mueve una parte de datos, este mismo se incluye en la copia de seguridad incremental, que se convierte en un tamaño grande aunque no contenga datos nuevos. La deduplicación ayuda a resolver el problema: cada vez que aparece un elemento en un lugar nuevo, se guarda una referencia hacia el mismo, en lugar del propio elemento.

### Deduplicación y copias de seguridad incrementales

En caso de realizar cambios aleatorios en los datos, la deduplicación y las copias de seguridad incrementales no surtirán demasiado efecto porque:

- Los elementos deduplicados que no se han cambiado no se incluyen en las copias de seguridad incrementales.
- Los elementos deduplicados que se han cambiado ya no son idénticos y por lo tanto no se deduplicarán.

## Mejores prácticas de deduplicación

Siga estas recomendaciones al utilizar la deduplicación:

- Al crear una bóveda de deduplicación, **ubique la bóveda y la base de datos de su deduplicación en discos diferentes.** Esto acelerará la deduplicación, ya que la deduplicación provoca un uso simultáneo extensivo de la bóveda y de la base de datos.
- La indexación de copias de seguridad requiere que la bóveda tenga **espacio libre con un tamaño mínimo de 1,1 multiplicado por el tamaño del archivo comprimido al cual pertenece la copia de seguridad**. Si no hay espacio libre suficiente en la bóveda, la tarea de indexación fallará y comenzará nuevamente después de 5–10 minutos, en base a la asimilación de que se ha liberado un poco de espacio como resultado de la limpieza o las tareas de indexación. Mientras más espacio libre haya en la bóveda, más rápido se reducirán los archivos comprimidos al tamaño mínimo posible.
- Al realizar copias de seguridad de múltiples sistemas con contenido similar, **primero realice la copia de seguridad de uno de los sistemas similares,** para que Acronis Backup & Recovery 10 Storage Node indexe todos los archivos del sistema como elementos de deduplicación

potenciales. Esto hará que los procesos de generación de copias de seguridad sean más rápidos y reducirá el tráfico de la red (gracias a una deduplicación eficaz en la fuente), independientemente de si se realizan las copias de seguridad de forma simultánea o no.

Antes de comenzar a realizar copias de seguridad subsiguientes, asegúrese de que la **tarea de indexado haya finalizado** la deduplicación de la primera copia de seguridad y que se encuentra inactiva. Puede consultar el estado de la tarea de indexación en la lista de tareas en el Acronis Backup & Recovery 10 Management Server.

## Proporción de deduplicación

La proporción de la deduplicación muestra el tamaño de los archivos comprimidos de una bóveda de deduplicación en relación con el tamaño que ocuparían en una bóveda que no es de deduplicación.

Por ejemplo, suponga que está realizando una copia de seguridad de dos archivos con contenido idénticos desde dos equipos. Si el tamaño de cada archivo es un gigabyte, entonces el tamaño de las copias de seguridad en una bóveda que no es de deduplicación será de 2 GB aproximadamente, pero de alrededor de 1 GB en una bóveda de deduplicación. Esto da como resultado una proporción de deduplicación de 2:1 o del 50%.

En cambio, si ambos archivos tuvieran un contenido diferente, los tamaños de la copia de seguridad en una bóveda de deduplicación y en una que no lo es sería el mismo (2 GB) y la proporción de deduplicación sería de 1:1 o del 100%.

### Qué proporción podemos esperar

Si bien, en algunas circunstancias, la proporción de la deduplicación puede ser muy alta (en el ejemplo anterior, si se incrementara la cantidad de equipos, se obtendrían proporciones de 3:1, 4:1, etc.), una expectativa razonable para un entorno típico es una proporción de entre 1.2:1 y 1.6:1.

Con un ejemplo más realista, suponga que está realizando una copia de seguridad de dos equipos de discos similares a nivel de archivos o del disco. En cada equipo, los archivos que todos los equipos tienen en común ocupan el 50% del espacio del disco (digamos, 1 GB) y los archivos que son específicos de cada equipo ocupan el otro 50% (1 GB más).

En este caso, en una bóveda de deduplicación, el tamaño de la copia de seguridad del primer equipo será de 2 GB, y el del segundo equipo será de 1 GB. En una bóveda que no es de deduplicación, las copias de seguridad ocuparían 4 GB en total. Como resultado, la proporción de deduplicación es de 4:3 o alrededor de 1.33:1.

De manera similar, con tres equipos, la proporción daría 1.5:1 y con cuatro equipos, 1.6:1. Se acerca a 2:1 ya que las copias de seguridad de dichos equipos se guardan en la misma bóveda. Esto significa que puede comprar, por ejemplo, un dispositivo de almacenamiento de 10 TB en vez de uno de 20 TB.

La cantidad real de reducción de capacidad está influenciada por muchos factores como el tipo de datos del cual se está realizando una copia de seguridad, la frecuencia de la copia de seguridad y el periodo de retención de las copias de seguridad.

## Restricciones de desduplicación

### Restricciones de desduplicación a nivel de bloque

Durante una copia de seguridad de un disco en un archivo comprimido en una bóveda de desduplicación, la desduplicación de un archivo no se realiza en los siguientes casos:

- Si se trata de un volumen comprimido

- Si el tamaño de la unidad de asignación de volumen, también llamado tamaño del clúster o tamaño del bloque, no es divisible entre 4 KB

  ***Consejo:*** *El tamaño de la unidad de asignación en la mayoría de los volúmenes NTFS y ext3 es de 4 KB y por lo tanto la desduplicación a nivel de bloque es posible. Otros ejemplos de tamaños de unidades de asignación que permiten la desduplicación a nivel de bloque serían 8 KB, 16 KB y 64 KB.*

- Si ha protegido el archivo comprimido con una contraseña

  ***Consejo:*** *Si desea proteger los datos en el archivo comprimido y al mismo tiempo permitir la desduplicación, prescinda de la protección con contraseña en el archivo comprimido y cifre la propia bóveda de desduplicación con una contraseña, lo cual puede hacerse al crear la bóveda.*

Los bloques de disco que se deduplicaron se almacenan en el archivo comprimido como si estuvieran en una bóveda sin desduplicación.

#### Restricciones de desduplicación a nivel de archivos

Durante una copia de seguridad de un archivo a un archivo comprimido en una bóveda de desduplicación, la desduplicación de un archivo no se realiza en los siguientes casos:

- Si el archivo se encuentra cifrado y en las opciones de copia de seguridad la casilla de verificación **En los archivos comprimidos, almacenar sin cifrar los archivos cifrados** está desactivada (se encuentra desactivada de manera predeterminada)
- Si el tamaño del archivo es menor que 4 KB
- Si ha protegido el archivo comprimido con una contraseña

Los archivos que no se deduplicaron se almacenan en el archivo comprimido como si estuvieran en una bóveda sin desduplicación.

##### La desduplicación y los flujos de datos de NTFS

En un sistema de archivo NTFS, un archivo puede poseer uno o más conjuntos de datos adicionales asociados llamados normalmente *flujos de datos alternativos*.

Cuando se realiza una copia de seguridad de esos archivos, se hace lo mismo con sus flujos de datos alternativos. Sin embargo, estos flujos nunca se deduplican, incluso aunque se deduplique el propio archivo.

## 2.12.7 Privilegios para la gestión centralizada

Esta sección describe los privilegios del usuario que se necesitan para gestionar un equipo de forma local y remota, para gestionar un equipo registrado en Acronis Backup & Recovery 10 Management Server y para acceder y gestionar Acronis Backup & Recovery 10 Storage Node.

### Tipos de conexión a un equipo gestionado

Existen dos tipos de conexión a un equipo gestionado: conexión local y conexión remota.

#### Conexión local

La conexión local se establece entre Acronis Backup & Recovery 10 Management Console de un equipo y Acronis Backup & Recovery 10 Agent del mismo equipo.

***Para establecer una conexión local***

- En la barra de herramientas, haga clic en **Conectar**. Luego seleccione **Nueva conexión** y haga clic en **Este equipo**.

### Conexión remota

La conexión remota se establece entre Acronis Backup & Recovery 10 Management Console de un equipo y Acronis Backup & Recovery 10 Agent de otro equipo.

Es posible que necesite especificar las credenciales de inicio de sesión para establecer una conexión remota.

***Para establecer una conexión remota***

1. En la barra de herramientas, haga clic en **Conectar,** luego señale **Nueva conexión** y haga clic en **Gestionar un equipo remoto**.
2. En **Equipo**, escriba o seleccione el nombre o la dirección IP del equipo remoto al que desea conectarse o haga clic en **Examinar** para seleccionar el equipo de la lista.
3. Para especificar las credenciales de conexión, haga clic en **Opciones** y luego escriba el nombre de usuario y la contraseña en las casillas **Nombre de usuario** y **Contraseña** respectivamente. En Windows, si deja la casilla **Nombre de usuario** vacía, se utilizarán las credenciales con las que se esté ejecutando la consola.
4. Para guardar la contraseña para el nombre de usuario especificado, seleccione la casilla de verificación **Guardar contraseña**. La contraseña se guardará en un almacenamiento seguro del equipo en el que la consola se esté ejecutando.

## Privilegios para la conexión local

Cualquier usuario que tenga el permiso de usuario "Iniciar sesión de forma local" de un equipo que ejecute Windows puede establecer una conexión local con ese equipo.

## Privilegios para la conexión remota en Windows

Para establecer una conexión remota con un equipo que se ejecuta con Windows, el usuario debe ser miembro del grupo de seguridad Usuarios de Acronis Remote de ese equipo.

Después de establecer una conexión remota, el usuario adquiere derechos de gestión sobre el equipo remoto, como se describe en Derechos del usuario en un equipo gestionado (pág. 33).

***Nota:*** *en un equipo remoto que se ejecuta con Windows Vista con el Control de Cuentas de Usuario (UAC) habilitado, y que no es parte de un dominio, únicamente el usuario Administrador incorporado puede realizar copias de seguridad de datos y realizar operaciones de gestión de discos. Para superar las restricciones, incluya el equipo en un dominio o deshabilite el UAC del equipo (el UAC está habilitado de manera predeterminada). Se aplica igualmente a los equipos que se ejecutan con Windows Server 2008 y Windows 7.*

Para obtener información sobre los grupos de seguridad de Acronis y sus miembros predeterminados, consulte grupos de seguridad de Acronis (pág. 74).

## Acronis security groups

En un equipo que se ejecuta con Windows, Acronis security groups determinan quién puede gestionar el equipo de forma remota y funcionar como administrador de Acronis Backup & Recovery 10 Management Server.

Estos grupos se crean en el momento que se instalan Acronis Backup & Recovery 10 Agents o Acronis Backup & Recovery 10 Management Server. Durante la instalación, puede especificar qué usuarios incluir en cada grupo.

### Acronis Backup & Recovery 10 Agents

Cuando Acronis Backup & Recovery 10 Agent para Windows se instala en un equipo, se crea (o actualiza) el grupo **Acronis Remote Users**.

Si un usuario es miembro de este grupo, puede gestionar el equipo de forma remota utilizando Acronis Backup & Recovery 10 Management Console, de acuerdo con los permisos de gestión que se describen en Privilegios del usuario en un equipo gestionado (pág. 33).

De manera predeterminada, este grupo incluye a todos los miembros del grupo de Administradores.

### Acronis Backup & Recovery 10 Management Server

En el momento que se instala Acronis Backup & Recovery 10 Management Server en un equipo, se crean (o actualizan) dos grupos:

**Acronis Centralized Admins**

Un usuario que es miembro de este grupo es un administrador del servidor de gestión. Los administradores del servidor de gestión se pueden conectar al servidor de gestión utilizando Acronis Backup & Recovery 10 Management Console, tienen los mismos permisos de gestión en los equipos registrados que los usuarios con privilegios administrativos en los mismos equipos, independientemente del contenido de Acronis security groups que allí se encuentren.

Para poder conectarse al servidor de gestión *de forma remota*, un administrador del servidor de gestión también debe ser miembro del grupo Acronis Remote Users.

Ningún usuario, ni siquiera un miembro del grupo de Administradores, puede ser administrador del servidor de gestión si no es miembro del grupo Acronis Centralized Admins.

De manera predeterminada, este grupo incluye a todos los miembros del grupo de Administradores.

**Acronis Remote Users**

Si un usuario es miembro de este grupo se puede conectar al servidor de gestión de forma remota, utilizando Acronis Backup & Recovery 10 Management Console, siempre y cuando también sea miembro del grupo Acronis Centralized Admins.

De manera predeterminada, este grupo incluye a todos los miembros del grupo de Administradores.

### En un controlador de dominio

Si un equipo es controlador de dominio en un dominio Active Directory, los nombres y el contenido predeterminados de Acronis security groups son diferentes:

- En lugar de **Acronis Remote Users** y **Acronis Centralized Admins**, los grupos se llaman *DCNAME* **$ Acronis Remote Users** y *DCNAME* **$ Acronis Centralized Admins** respectivamente. *DCNAME* representa el nombre NetBIOS del controlador de dominio. Hay un único espacio antes y después de cada uno de los símbolos de dólar.
- En lugar de incluir los nombres de todos los miembros del grupo de Administradores explícitamente, se incluye el propio grupo de Administradores.

***Consejo:*** *Para garantizar que los nombres de los grupos son los adecuados, debe instalar los componentes de Acronis en un controlador de dominio después de configurar el propio controlador de dominio. Si los componentes se instalan antes de configurar el controlador de dominio, cree los grupos* DCNAME ***$ Acronis Remote Users*** *y* DCNAME ***$ Acronis Centralized Admins*** *manualmente y luego incluya los miembros de los grupos Acronis Remote Users y Acronis Centralized Admins que acaba de crear.*

## Privilegios de usuario en un nodo de almacenamiento

EL alcance de los privilegios de un usuario en Acronis Backup & Recovery 10 Storage Node depende de los permisos del usuario sobre el equipo donde se está instalado el nodo de almacenamiento.

Un usuario común, como un miembro del grupo de Usuarios en el nodo de almacenamiento, puede:

- Crear archivos comprimidos en cualquier bóveda centralizada gestionada por el nodo de almacenamiento
- Ver y gestionar archivos comprimidos que son propiedad del usuario

Un usuario que es miembro del grupo de Administradores en el nodo de almacenamiento puede además:

- Ver y gestionar cualquier archivo comprimido en cualquier bóveda centralizada gestionada por el nodo de almacenamiento
- Crear bóvedas centralizadas que serán gestionadas por el nodo de almacenamiento, siempre y cuando el usuario sea también un administrador de Acronis Backup & Recovery 10 Management Server
- Reorganizar la tarea de compactación, como se describe en Operaciones con nodos de almacenamiento (pág. 344), bajo "Cambiar la programación de la tarea de compactación"

Los usuarios con estos privilegios adicionales también se llaman administradores del nodo de almacenamiento.

### Recomendaciones sobre las cuentas de usuario

Para permitir que los usuarios accedan a las bóvedas centralizadas gestionadas por el nodo de almacenamiento, debe asegurarse de que esos usuarios tengan el permiso para acceder al nodo de almacenamiento desde la red.

Si tanto los equipos de los usuarios como el equipo con el nodo de almacenamiento están en un dominio Active Directory, probablemente no necesite realizar ningún otro paso: todos los usuarios son miembros generalmente del grupo Usuarios de dominio y por lo tanto pueden acceder al nodo de almacenamiento.

De lo contrario, necesitará crear cuentas de usuarios en el equipo donde está instalado el nodo de almacenamiento. Recomendamos crear una cuenta de usuario separada para cada usuario que accederá al nodo de almacenamiento, para que los usuarios puedan acceder solo a los archivos comprimidos que les pertenecen.

Al crear las cuentas, siga estas pautas:

- Para usuarios que usted desea que funcionen como administradores del nodo de almacenamiento, agregue sus cuentas al grupo de **Administradores**.
- Para otros usuarios, agregue sus cuentas de usuario al grupo **Usuarios**.

### Permiso adicional de los administradores del equipo

Un usuario que es miembro del grupo de Administradores en un equipo puede ver y gestionar cualquier archivo comprimido creado *desde ese equipo* en una bóveda gestionada, sin importar el tipo de esa cuenta de usuario en el nodo de almacenamiento.

**Ejemplo**

Supongamos que dos usuarios en un equipo, UsuarioA y UsuarioB, realizan copias de seguridad desde este equipo a una bóveda centralizada gestionada por un nodo de almacenamiento. En el nodo de almacenamiento, permítale a estos usuarios tener cuentas (no administrativas) regulares UsuarioA_SN y UsuarioB_SN, respectivamente.

Normalmente, el UsuarioA puede acceder solo a los archivos comprimidos creados por el UsuarioA (y que pertenecen a UsuarioA_SN) y el UsuarioB puede acceder solamente a los archivos comprimidos creados por el UsuarioB (y que pertenecen a UsuarioB_SN).

Sin embargo, su el UsuarioA es miembro del grupo de Administradores en el equipo, este usuario puede acceder además a los archivos comprimidos creados desde este equipo por el UsuarioB, a pesar de que la cuenta del UsuarioA en el nodo de almacenamiento es una cuenta regular.

## Permisos de administrador del servidor de gestión

Por lo general, el administrador de Acronis Backup & Recovery 10 Management Server opera en un equipo registrado en nombre de Acronis Managed Machine Service (también conocido como el servicio de Acronis) de dicho equipo y dispone de los mismos privilegios que el servicio.

O bien, al crear una política de copias de seguridad, el administrador del servidor de gestión puede optar por especificar explícitamente una cuenta de usuario con la que se ejecutarán los planes de copias de seguridad centralizados en los equipos registrados. En este caso, la cuenta de usuario debe existir en todos los equipos en los que se implementará la política centralizada. Esto no siempre es eficaz.

Para ser un administrador del servidor de gestión, el usuario debe ser miembro del grupo Acronis Centralized Admins del equipo en el que se instala el servidor de gestión.

## Derechos de los servicios de Acronis

Los componentes de Acronis Backup & Recovery 10 Agent para Windows, Acronis Backup & Recovery 10 Management Server y Acronis Backup & Recovery 10 Storage Node se ejecutan como servicios. Al instalar cualquiera de estos componentes, debe especificar la cuenta en la cual el servicio del componente se ejecutará.

Para cada servicio, puede crear una cuenta de usuario dedicada (recomendado en la mayoría de los casos) o especificar una cuenta existente en un usuario local o del dominio, por ejemplo: .**UsuarioLocal** o **NombreDominio\UsuarioDominio**.

Si escoge crear cuentas de usuario dedicadas para los servicios, el programa de instalación creará las siguientes cuentas de usuario:

- Para el servicio de Acronis Backup & Recovery 10 Agent para Windows, **Acronis Agent User**
- Para el servicio de Acronis Backup & Recovery 10 Management Server, **AMS User**
- Para el servicio de Acronis Backup & Recovery 10 Storage Node, **ASN User**

A las cuentas creadas recientemente se les otorgan los siguientes privilegios:

- A las tres cuentas se les asigna el derecho de usuario de **Iniciar sesión como un derecho de usuario del servicio**.
- A la cuenta de usuario de Acronis Agent User se le asignan los derechos de usuario **Ajustar cantidades máximas de memoria para un proceso** y **Reemplazar símbolo de nivel de un proceso**.

- Las cuentas de Acronis Agent User y ASN User se incluyen en el grupo **Operadores de copia de seguridad**.
- La cuenta de usuario del usuario AMS está incluida en el grupo **Acronis Centralized Admins**.

El programa de instalación asignará los derechos de usuario que se enumeran arriba a todas las cuentas existentes que se especifiquen para el correspondiente servicio.

Si escoge especificar una cuenta de usuario existente para el servicio de agente o el servicio de nodo de almacenamiento, asegúrese de que esta cuenta sea miembro del grupo **Operadores de cuenta de seguridad**, antes de proceder con la instalación.

Si elije especificar una cuenta de usuario existente para el servicio de servidor de gestión, está cuenta se añadirá al grupo de **Acronis Centralized Admins** de forma automática.

Si el equipo es parte de un dominio de Active Directory, asegúrese de que las políticas de seguridad del dominio no impidan que las cuentas descritas en esta sección (ya sea que existan o hayan sido creadas como nuevas) tengan los derechos de usuarios que se enumeran arriba.

***Importante:*** *Después de la instalación, no especifique una cuenta de usuario diferente para el servicio de un componente. De otra manera, el componente puede dejar de funcionar.*

A las cuentas de usuario creadas recientemente también se les permite el acceso a la clave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Acronis (denominada clave de registro Acronis) con los siguientes derechos: **Consultar valor**, **Establecer valor**, **Crear clave secundaria**, **Enumerar claves secundarias**, **Notificar**, **Eliminar** y **Leer el control**.

Además, existen dos servicios de Acronis que se ejecutan bajo una cuenta de sistema:

- El **servicio de Acronis Scheduler2** proporciona programación de las tareas de los componentes de Acronis. Se ejecuta bajo una cuenta de Sistema local no puede ejecutarse bajo una cuenta diferente.
- El **servicio de Acronis Remote Agent** proporciona conectividad entre los componentes de Acronis. Se ejecuta bajo una cuenta de Servicio para redes y no puede ejecutarse bajo una cuenta diferente.

## 2.12.8 Comunicación entre los componentes de Acronis Backup & Recovery 10

Esta sección describe cómo los componentes de Acronis Backup & Recovery 10 se comunican entre ellos a través de una autenticación segura y de un sistema de cifrado.

Esta sección también contiene información sobre cómo configurar los ajustes de comunicación, seleccionando un puerto de red para la comunicación y gestionando certificados de seguridad.

### Comunicación segura

Acronis Backup & Recovery 10 proporciona la capacidad de asegurar los datos transferidos entre sus componentes en el interior de una red de área local y a través de una red de perímetro (también denominada zona delimitada, DMZ).

Existen dos mecanismos que aseguran una comunicación segura entre los componentes de Acronis Backup & Recovery 10:

- **Autenticación segura** proporciona una transferencia segura de los certificados necesarios para establecer una conexión, utilizando el protocolo de Capa de conexión segura (SSL).

- **Comunicación cifradaproporciona una transferencia segura de información entre dos componentes, como, por ejemplo, entre** Acronis Backup & Recovery 10 Agente y Acronis Backup & Recovery 10 Storage Node, a través del cifrado de los datos transferidos.

Para obtener instrucciones acerca de cómo configurar los ajustes de autenticación segura y cifrado de datos, consulte Configurar opciones de comunicación (pág. 79).

Para obtener instrucciones acerca de cómo gestionar certificados SSL utilizados para una autenticación segura, consulte certificados SSL (pág. 83).

***Nota:*** *Los componentes de versiones anteriores de productos de Acronis, incluyendo aquellos de la familia Acronis True Image Echo Family, no se pueden conectar a los componentes de Acronis Backup & Recovery 10, independientemente de los ajustes de autenticación segura y cifrado de datos.*

## Aplicaciones servidor y cliente

Existen dos protagonistas en el proceso de comunicación segura:

- **Aplicación cliente** o cliente, es la aplicación que intenta establecer la conexión.
- **Aplicación servidor** o servidor, es la aplicación a la que el cliente intenta conectarse.

Por ejemplo, si Acronis Backup & Recovery 10 Management Console está estableciendo conexión con Acronis Backup & Recovery 10 Agente en un equipo remoto, el primero sería el cliente y el segundo el servidor.

Un componente de Acronis puede actuar como una aplicación cliente, una aplicación servidor, o como ambas, tal y como se muestra en la siguiente tabla.

| Nombre del componente | Puede ser cliente | Puede ser servidor |
|---|---|---|
| Acronis Backup & Recovery 10 Management Console | Sí | No |
| Acronis Backup & Recovery 10 Agent | Sí | Sí |
| Acronis Backup & Recovery 10 Management Server | Sí | Sí |
| Acronis Backup & Recovery 10 Storage Node | Sí | Sí |
| Acronis PXE Server | No | Sí |
| Acronis Backup & Recovery 10 Bootable Agent | Sí | Sí |

## Configurar los ajustes de comunicación

Puede configurar los ajustes de comunicación tales como el posible cifrado de los datos transferidos entre los componentes de Acronis Backup & Recovery 10 instalados en uno o varios equipos, a través de Acronis Administrative Template. Para obtener más información sobre cómo cargar las plantillas administrativas, consulte Cómo cargar Acronis Administrative Template (pág. 360).

Cuando se aplican a un solo equipo, las plantillas administrativas definen los ajustes de comunicación para todos los componentes del equipo; cuando se aplica a un dominio o a una unidad organizacional, definen los ajustes de comunicación para todos los componentes en los equipos de ese dominio o unidad organizacional.

### *Para configurar ajustes de comunicación*

1. Haga clic en **Inicio**, luego haga clic en **Ejecutar** y luego escriba **gpedit.msc**:
2. En la consola de **Política de grupo**, expanda **Configuración del equipo** y **Plantilla administrativas**, y después haga clic en Acronis.
3. En el panel derecho de Acronis, haga doble clic en la opción de comunicación que desea configurar. La plantilla administrativa contiene las siguientes opciones (cada opción se detalla en este tema):
   - **Puertos de agente remoto**
   - **Opciones de cifrado del cliente**
   - **Opciones de cifrado del servidor**
4. Para que los nuevos ajustes de comunicación tengan efecto, reinicie todo los componentes de Acronis que se estén ejecutando, preferiblemente reiniciando Windows. Si no es posible reiniciar, asegúrese de hacer lo siguiente:
   - Si se está ejecutando Acronis Backup & Recovery 10 Management Console, ciérrela y ábrala de nuevo.
   - Si se están ejecutando otros componentes de Acronis, tales como Acronis Backup & Recovery 10 Agent para Windows o Acronis Backup & Recovery 10 Management Server, reinicie sus servicios correspondientes desde el complemento **Servicios** en Windows.

## Puertos de agente remoto

Especifique el puerto que utilizará el componente para la comunicación entrante y saliente con otro componentes de Acronis.

Seleccione una de las siguientes opciones:

**No configurado**

El componente utilizará el número de puerto predeterminado TCP 9876.

**Habilitado**

El componente utilizará el puerto especificado; escriba el número de puerto en el cuadro de diálogo **Puerto TCP del servidor**.

**Deshabilitado**

Igual que **No configurado**.

Para obtener más información sobre el puerto de red, así como instrucciones sobre cómo especificarlo en Linux y en un entorno de inicio, consulte Configuración del puerto de red (pág. 82).

## Opciones de cifrado del cliente

Especifique si desea cifrar los datos transferidos cuando el componente actúa como aplicación cliente y si desea confiar en los certificados SSL autofirmados.

Seleccione una de las siguientes opciones:

**No configurado**

El componente utilizará los ajustes predeterminados, que se basan en la utilización del cifrado siempre que sea posible y en la confianza en los certificados SSL autofirmados (consulte la siguiente opción).

**Habilitado**

El cifrado está habilitado. En **Cifrado**, seleccione una de las siguientes opciones:

**Habilitado**

La transferencia de datos estará cifrada si el cifrado se encuentra habilitado en la aplicación servidor, de otra manera, no se cifrará.

**Deshabilitado**

El cifrado está deshabilitado; no se establecerá ninguna conexión con una aplicación servidor que requiera cifrado.

**Obligatorio**

La transferencia de datos se llevará a cabo únicamente si el cifrado se encuentra habilitado en la aplicación servidor (consulte "Opciones de cifrado del servidor"); se cifrará.

*Parámetros de autenticación*

Activar la casilla de verificación **Confiar en certificados autofirmados** permite al cliente conectarse a las aplicaciones servidor que utilizan certificados SSL autofirmados tales como aquellos creados durante la instalación de los componentes de Acronis Backup & Recovery 10; consulte Certificados SSL (pág. 83).

Esta casilla de verificación deberá permanecer activada, a menos que disponga de una Infraestructura de clave pública (PKI) en su entorno.

En **Utilizar autenticación de certificado del agente**, seleccione una de las siguientes opciones:

**No utilizar**

La utilización de certificados SSL está deshabilitada. No se establecerá la conexión con ninguna aplicación servidor que requiera la utilización de certificados SSL.

**Utilizar si es posible**

La utilización de certificados SSL está habilitada. El cliente solo utilizará certificados SSL si su utilización está habilitada en la aplicación servidor.

**Siempre utilizar**

La utilización de certificados SSL está habilitada. La conexión se establecerá únicamente si la utilización de certificados SSL está habilitada en la aplicación servidor.

**Deshabilitado**

Igual que **No configurado**.

## Opciones de cifrado del servidor

Especifica si desea cifrar los datos transferidos cuando el componente actúa como aplicación servidor.

Seleccione una de las siguientes opciones:

**No configurado**

El componente utilizará el ajuste predeterminado, que se basa en la utilización de cifrado siempre que sea posible (consulte la siguiente opción).

**Habilitado**

El cifrado está habilitado. En **Cifrado**, seleccione una de las siguientes opciones:

**Habilitado**

La transferencia de datos estará cifrada solo si el cifrado se encuentra habilitado en la aplicación cliente.

**Deshabilitado**

El cifrado está deshabilitado; no se establecerá ninguna conexión con una aplicación cliente que requiera cifrado.

**Obligatorio**

La transferencia de datos se llevará a cabo solo si el cifrado está habilitado en la aplicación del cliente (consulte "Opciones de cifrado del cliente"); se cifrará.

*Parámetros de autenticación*

En **Utilizar autenticación de certificado del agente**, seleccione una de las siguientes opciones:

**No utilizar**

La utilización de certificados SSL está deshabilitada. No se establecerá ninguna conexión a la aplicación del cliente que requiera la utilización de certificados SSL.

**Utilizar si es posible**

La utilización de certificados SSL está habilitada. El servidor utilizará certificados SSL si su utilización está habilitada en la aplicación del cliente y de lo contrario, no los utilizará.

**Utilizar siempre**

La utilización de certificados SSL está habilitada. Se establecerá la conexión solo si la utilización de certificados SSL está habilitada en la aplicación del cliente.

**Deshabilitado**

Igual que **No configurado**.

## Configuración del puerto de red

Los componentes de Acronis Backup & Recovery 10 utilizan como puerto de red de comunicación predeterminado 9876/TCP. El servidor utilizará este puerto para detectar las conexiones entrantes. El cliente de Acronis también utiliza este puerto como predeterminado. Durante la instalación de los componentes, es posible que se le solicite la confirmación de la apertura del puerto o la realización de su apertura manual, en el caso de utilizar un cortafuegos distinto al de Windows.

Tras la instalación, puede cambiar los puertos en cualquier momento para establecer los valores que prefiera o por razones de seguridad. Esta operación requiere el reinicio del servicio de Acronis Remote Agent (en Windows) o Acronis_agent (en Linux).

Cuando cambie el puerto en el servidor, conéctese al servidor utilizando la dirección URL <Server-IP>:<port> o <Server-hostname>:<port>.

***Nota:*** *Si utiliza traducción de dirección de red (NAT), también puede configurar el puerto realizando su asignación.*

### Configurar el puerto en el sistema operativo

**Windows**

Para cambiar los números de puerto, cargue y configure la Plantilla administrativa de Acronis, tal y como se detalla en Configurar los ajustes de comunicación (pág. 79), en "Puertos de agente remoto".

**Linux**

Especifique el puerto en el archivo /etc/Acronis/Policies/Agent.config. Reinicie Acronis_agent daemon.

### Configurar el puerto en un entorno de inicio

Al crear un dispositivo de inicio de Acronis, puede preconfigurar el puerto de red que utilizará un Acronis Backup & Recovery 10 Bootable Agent. Puede elegir entre:

- El puerto predefinido (9876)
- El puerto utilizado actualmente
- Un nuevo puerto (escriba el número de puerto)

Si no se ha preconfigurado un puerto, el agente utiliza el número de puerto predeterminado.

## Certificados SSL

Los componentes de Acronis Backup & Recovery 10 utilizan certificados de Capa de conexión segura (SSL) para una autenticación segura.

Los certificados SSL para los componentes pueden ser de uno de los siguientes tipos:

- **Certificados autofirmados**, como los certificados generados automáticamente durante la instalación de un componente de Acronis.
- **Certificados no autofirmados**, como los certificados emitidos por una Entidad de certificación (CA) tercera; por ejemplo, por una CA pública como VeriSign® o Thawte™, o por la CA de su organización.

### Ruta del certificado

Todos los componentes de Acronis instalados en un equipo, cuando funcionan como una aplicación de servidor, utilizan un certificado SSL llamado el certificado del usuario.

En Windows, la ruta del certificado y el nombre del archivo del certificado del servidor están especificados en la clave de registro `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Encryption\Server`. La ruta predeterminada es %SystemDrive%\Archivos de programa\Archivos comunes\Acronis\Agent.

Para certificados autofirmados, se utiliza la impresión digital del certificado (también conocida como huella dactilar o hash) para la identificación de futuros servidores: Si un cliente se ha conectado previamente a un servidor utilizando un certificado autofirmado e intenta establecer conexión nuevamente, el servidor verifica si la impresión digital del certificado es la misma que las utilizadas anteriormente.

### Certificados autofirmados

En los equipos que se ejecutan con Windows, si la ubicación del certificado no contiene un certificado de servidor, se genera e instala automáticamente un certificado de servidor autofirmado durante la instalación de cualquier componente de Acronis a excepción de Acronis Backup & Recovery 10 Management Console.

Si se cambia el nombre del equipo después de que se ha generado el certificado autofirmado, el certificado no puede utilizarse y necesitará generar uno nuevo.

#### *Para generar un certificado autofirmado nuevo*

1. Inicie la sesión como miembro del grupo de Administradores.
2. En el menú **Inicio**, haga clic en **Ejecutar** y luego escriba: **cmd**
3. Ejecute el siguiente comando (tenga en cuenta las comillas):
   ```
   "%CommonProgramFiles%\Acronis\Utils\acroniscert" --reinstall
   ```
4. Reinicie Windows o reinicie los servicios de Acronis que se están ejecutando.

### Certificados no autofirmados

Tiene la posibilidad de utilizar certificados de terceros o certificados creados por la CA de su organización como una alternativa para los certificados autofirmados, al utilizar una Utilidad de línea de comandos del certificado de Acronis.

#### *Para instalar un certificado de terceros*

1. Haga clic en **Inicio**, luego haga clic en **Ejecutar** y luego escriba: **certmgr.msc**
2. En la consola de **Certificados**, haga doble clic en el nombre del certificado que desea instalar.
3. En la pestaña **Detalles**, en la lista de campos, haga clic en **Impresión digital**.
4. Seleccione y copie el valor del campo, llamado una impresión digital de certificado; una cadena como **20 99 00 b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85**
5. En el menú **Inicio**, haga clic **Ejecutar** y luego escriba lo siguiente en el cuadro **Abrir**:

   ```
   "%CommonProgramFiles%\Acronis\Utils\acroniscert.exe" --install
   "20 99 00 b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85"
   ```

   (Tenga en cuenta las comillas; sustituya la impresión digital representativa que se muestra aquí con la de su certificado.)

# 3 Opciones

Esta sección cubre las opciones de Acronis Backup & Recovery 10 que se puede configurar utilizando la interfaz gráfica de usuario (GUI). El contenido de esta sección es aplicable a las ediciones avanzadas y autónomas de Acronis Backup & Recovery 10.

## 3.1 Opciones de Consola

Las opciones de consola definen la manera en la que se representa la información en la Interfaz Gráfica de Usuario de Acronis Backup & Recovery 10.

Para acceder a las opciones de la Consola, seleccione **Opciones> Consola** desde el menú superior.

### 3.1.1 Página de inicio

Esta opción define si se desea mostrar la ventana de **Bienvenida** o el **Tablero** después de que la consola se conecte al equipo gestionado o Management server.

El valor predeterminado: La ventana de **Bienvenida**.

Para realizar una selección, marque o desmarque la casilla de verificación para **mostrar el Tablero después de que la consola se conecte al equipo**.

Esta opción también se puede establecer en la ventana de **Bienvenida**. Si selecciona la casilla de verificación **Al inicio, se verá el Tablero en vez de la vista actual** en la ventana de **Bienvenida,** dicha configuración se actualizará según corresponda.

### 3.1.2 Mensajes emergentes

#### Sobre las tareas que necesitan interacción

Esta opción es eficaz cuando la consola está conectada a un equipo gestionado o Management server.

La opción define si se debe mostrar la ventana emergente cuando hay una o más tareas que requieran de la interacción del usuario. Esta ventana le permite especificar su decisión para confirmar el reinicio o para volver a intentarlo después de liberar espacio de disco, o en todas las tareas en el mismo lugar. Hasta que una tarea necesite de interacción, puede abrir esta ventana en cualquier momento desde el **Tablero** del equipo gestionado. También podría revisar los estados de ejecución de tareas en la vista de**Tareas** y especificar su decisión sobre cada tarea en el panel de **Información**.

El valor predeterminado: **Habilitado.**

Para realizar una selección, seleccione o anule su selección en la casilla de verificación en la **ventana emergente "Tareas que necesitan Interacción"**.

#### Sobre los resultados de la ejecución de tareas

La opción sólo es eficaz cuando la consola está conectada a un equipo gestionado.

La opción define si se muestran los mensajes emergentes sobre los resultados de la ejecución de tareas: finalización exitosa, falla o éxito con advertencias. Cuando se deshabilita la visualización de mensajes emergentes, puede revisar los estados de ejecución de tareas y los resultados en la vista de **Tareas**.

El valor predeterminado: **Habilitado** para todos los resultados.

Para una realizar una configuración por cada resultado individualmente (finalización exitosa, falla o éxito con advertencias) selecciones o anule su selección en la casilla de verificación respectiva.

### 3.1.3 Alertas según el momento

#### Última copia de seguridad

Esta opción es eficaz cuando la consola está conectada a un equipo gestionado (pág. 405) o Management server (pág. 409).

La opción define si se informa en caso de que no se realice la copia de seguridad en algún equipo durante cierto tiempo. Puede ingresar el período de tiempo que cree es importante para su empresa.

El valor predeterminado: Informa si se completó la última copia de seguridad en un equipo con hasta **5 días** de anterioridad.

Se muestra la alerta en la sección **Alertas** del **Tablero**. Cuando la consola se conecta al Management server, la configuración también controlará el esquema de colores de los valores de la columna de la **Última Copia de seguridad** para cada equipo. .

#### Última conexión

Esta opción es eficaz cuando la consola se conecta al Management server o al equipo registrado (pág. 405).

Esta opción define si se informa si no se establece la conexión entre el equipo registrado y el Management server durante un período de tiempo, y así indica que es posible que el equipo no pueda ser gestionado centralmente (por ejemplo: en el caso de fallas de la conexión de red para ese equipo). Puede establecer el período de tiempo que crea importante.

El valor predeterminado: Informa si la última conexión del equipo al Management server se realizó con más de **5 días** de anterioridad.

Se muestra la alerta en la sección **Alertas** del **Tablero**. Cuando la consola se conecta al Management server, la configuración también controlará el esquema de colores de los valores de la columna de la **Última conexión** para cada equipo. .

### 3.1.4 Cantidad de tareas

La opción sólo es eficaz cuando la consola está conectada al Management server.

La opción define la cantidad de tareas que se mostrará a la vez en la vista de **Tareas**. También puede usar los filtros disponibles en la vista de **Tareas** para limitar el número de tareas mostradas.

El valor predeterminado: **400**. Los valores de ajuste son: **20 a 500**.

Para realizar una selección, elija el valor deseado desde el **Número de tareas** en el menú desplegable.

### 3.1.5 Fuentes

Esta opción es eficaz cuando la consola está conectada a un equipo gestionado o Management server.

La opción define las fuentes que se usarán en la Interfaz Gráfica de Usuario de Acronis Backup & Recovery 10. Las configuraciones de **Menú** afectan a los menús desplegables y contextuales. La configuración de **Aplicación** afecta a los otros elementos de la GUI.

El valor predeterminado: La **fuente por defecto** del sistema para los menús y los elementos de la interfaz de la aplicación.

Para realizar una selección, elija la fuente en el cuadro combinado respectivo y establezca las propiedades de la fuente. Puede obtener una vista previa de la fuente al hacer clic en el botón de la derecha.

## 3.2 Opciones de Management Server

Las opciones de Management Server le permiten que ajuste el comportamiento de Acronis Backup & Recovery 10 Management server.

Para tener acceso a las opciones de Management server, conecte la consola de Management server y después seleccione **Opciones > Opciones de Management Server** desde el menú superior.

### 3.2.1 Nivel de registro

Esta opción define si el Management server debe recopilar los sucesos del registro de los equipos registrados en el registro centralizado que se guarda en base de datos y está disponible en la vista de **Registros**. Puede establecer para la opción de todos los sucesos a la vez o seleccionar los tipos de sucesos a recopilar. Si deshabilita la recopilación de los sucesos del registro por completo, el registro centralizado sólo tendrá los registros del management server.

El valor predeterminado: **Recopilar** los registros de **todos los sucesos**.

Use el cuadro de combinaciones con los **Tipos de sucesos a guardar en el registro** para especificar los tipos de sucesos a recopilar:

- **Todos los sucesos**: todos los sucesos (información, advertencias y errores) en todos los equipos registrados en el Management server, serán guardados en el registro centralizado.
- **Errores y advertencias**: se guardarán las advertencias y los errores en el registro centralizado.
- **Sólo Errores**: sólo se guardarán los errores en el registro centralizado.

Para deshabilitar la recopilación de sucesos del registro, anule la selección de la casilla de verificación **Recopilación de registros**.

### 3.2.2 Reglas de limpieza de los registros

Esta opción especifica cómo limpiar el registro de sucesos centralizado almacenado en la base de datos de informes del management server.

Esta opción define el tamaño máximo de la base de datos de los informes.

El valor predeterminado: **Tamaño de registro máximo: 1 GB**. **Durante la limpieza, mantenga el 95% del tamaño de registro máximo**.

Cundo la opción está habilitada, el programa compara el tamaño de registro actual con el tamaño máximo cada 100 entradas del registro. Una vez exedido el tamaño de registro máximo, el programa elimina las entradas de registro más antiguas. Puede seleccionar las entradas del registro a retener. La configuración predeterminada de 95% conservará la mayoría del registro. Con la configuración mínima de 1%, el registro se borrará casi por completo.

*Incluso si borra el límite de tamaño de registro, el registro de sucesos de una base de datos SQL Server Express se detendrá después de que el tamaño del registro alcance los 4 GB, ya que SQL Express Edition tiene un límite de 4 GB por base de datos. Establezca el tamaño de registro máximo en aproximadamente 3.8 GB si desea utilizar la capacidad máxima de la base de datos de SQL Express.*

Este parámetro también puede establecerse utilizando Acronis Administrative Template (pág. 363).

## 3.2.3 Seguimiento de sucesos

Puede configurar Management server para registrar los sucesos en el Registro de sucesos de aplicación de Windows además del propio registro de management server.

Puede configurar Management server para enviar objetos de Simple Network Management Protocol (SNMP) al gestor SNMP especificado.

### Registro de sucesos de Windows

Esta opción define si management server debe registrar sus propios sucesos de registro en el Registro de sucesos de aplicación de Windows (para ver este registro, ejecute **eventvwr.exe** o seleccione **Panel de Control > Herramientas administrativas > Visor de sucesos**). Puede filtrar los sucesos a ser registrados.

El valor predeterminado es: **Deshabilitado**.

Para habilitar esta opción, active la casilla de verificación **Registrar eventos**.

Utilice la casilla de verificación **Tipos de eventos para registrar** para filtrar los eventos que vayan a registrarse en el Registro de sucesos de aplicación de Windows:

- **Todos los eventos**: todos los eventos (información, advertencias y errores)
- **Errores y advertencias**
- **Solo errores**.

Para deshabilitar esta opción, active la casilla de verificación **Registrar eventos**.

### Notificaciones SNMP

Esta opción define si Management server debe enviar sus propio registro de sucesos de gestores Simple Network Management Protocol (SNMP) específicos. Puede elegir los tipos de sucesos a enviar.

Para obtener información detallada acerca de cómo utilizar SNMP con Acronis Backup & Recovery 10, vaya a "Asistencia para SNMP (pág. 49)".

El valor predeterminado: **Deshabilitado**.

#### *Configurar el envío de mensajes SNMP*

1. Active la casilla de verificación **Enviar mensajes al servidor**.

2. Especifique las opciones apropiadas como se detalla a continuación:
   - **Tipos de eventos para enviar**: elija los tipos de eventos: **Todos los eventos**, **Errores y advertencias**, o **Sólo errores**.
   - **Nombre del servidor/IP:** introduzca el nombre o dirección IP del servidor en el que se ejecuta la aplicación de gestión SNMP y al que se enviarán los mensajes.
   - **Comunidad**: tipo de nombre de la comunidad SNMP a la que pertenecen tanto el servidor que ejecuta la aplicación de gestión SNMP como el equipo emisor. La comunidad típica es "pública".

   Haga clic en **Enviar mensaje de prueba** para verificar si la configuración es correcta.

Para deshabilitar el envío de mensajes SNMP, desactive la casilla de verificación **Enviar mensajes al servidor SNMP**.

Los mensajes se envían a través de UDP.

### 3.2.4 Credenciales de acceso al dominio

Esta opción determina el nombre de usuario y la contraseña que el servidor de gestión utilizará para acceder al dominio.

El valor predeterminado: Sin credenciales

El servidor de gestión necesita credenciales de acceso al dominio cuando trabaja con un grupo dinámico que está basado en el criterio (pág. 335) de **Unidad organizativa**. Cuando está creando dicho grupo y en esta opción no se proporcionan las credenciales, el programa le pedirá las credenciales y las guardará en esta opción.

Es suficiente especificar las credenciales de un usuario que es miembro del grupo de **Usuarios del dominio** en el dominio.

### 3.2.5 Acronis WOL Proxy

Esta opción también funciona combinada con la configuración avanzada de programación **Utilizar Wake-On-LAN** (pág. 181). Utilice esta opción si el management server debe activarse para realizar copias de seguridad de equipos ubicados en otra subred.

Cuando la operación programada está a punto de comenzar, el management server envía paquetes mágicos para activar los equipos adecuados. (un paquete mágico es un paquete que contiene 16 copias contiguas de la dirección MAC de la tarjeta NIC receptora). El Acronis WOL Proxy, instalado en otra subred, transfiere los paquetes a los equipos ubicados en esa subred.

El valor predeterminado: **Deshabilitado**.

***Para utilizar esta opción:***

1. Instale Acronis WOL Proxy en cualquier servidor de la subred donde se encuentren los equipos que se deben activar. El servidor debe proporcionar disponibilidad de servicios continuos. Con múltiples subredes, instale Acronis WOL Proxy en cada subred donde necesite utilizar la funcionalidad de Wake-On-LAN.
2. Habilite el **Acronis WOL Proxy** en las **Opciones de management server** de la siguiente manera:
   a. Seleccione la casilla de verificación **Utilizar los siguientes proxies**.
   b. Haga clic en **Añadir** y luego introduzca el nombre o la dirección IP del equipo donde el Acronis WOL Proxy está instalado. Proporcione las credenciales de acceso para el equipo.

c. Repita este paso si hay varios Acronis WOL Proxies.

3. Al programar una política de copias de seguridad, habilite la configuración **Utilizar Wake-On-LAN**.

También tiene la capacidad para eliminar proxys de la lista. Tenga en cuenta que cualquier cambio en esta opción afecta al management server completo. Si elimina un proxy de la lista, la funcionalidad Wake-On-LAN en la subred correspondiente se deshabilitará para todas las políticas, incluyendo las políticas ya aplicadas.

## 3.2.6 Opciones de protección de las máquinas virtuales

Estas opciones definen el comportamiento del servidor de gestión en relación con la copia de seguridad y recuperación de las máquinas virtuales alojadas en servidores de virtualización.

### Integración de VMware vCenter

Esta opción define si mostrar las máquinas virtuales gestionadas por un VMware vCenter Server en el servidor de gestión y mostrar el estado de la copia de seguridad de estos equipos en el vCenter.

La integración está disponible en todas las ediciones avanzadas de Acronis Backup & Recovery 10; no se necesita una licencia para Virtual Edition. No se necesita ninguna instalación de software en el vCenter Server.

#### Del lado del servidor de gestión

Cuando la integración está habilitada, la vista de inventario de **VM y plantillas** de vCenter aparece en la interfaz de usuario del servidor de gestión debajo de **Navegación** > **Máquinas virtuales**.

Desde el punto de vista del servidor de gestión, este es un grupo dinámico de máquinas virtuales. El nombre del grupo coincide con el nombre o la dirección IP del vCenter Server, según se haya especificado cuando se configuró la integración. El contenido del grupo se sincroniza con el vCenter Server y no se puede cambiar del lado del servidor de gestión. En caso de que exista una inconsistencia ocasional, haga clic con el botón derecho en el grupo y seleccione **Actualizar**.

Las máquinas virtuales gestionadas por el vCenter Server también aparecerán en el grupo **Todas las máquinas virtuales**. Puede ver las propiedades y el estado de alimentación de las máquinas virtuales; crear grupos de máquina virtual y añadir máquina virtual a los grupos existentes.

No es posible la copia de seguridad y recuperación de una máquina virtual, a menos que Acronis Backup & Recovery 10 Agent para ESX/ESXi esté implementado (pág. 341) en el servidor de la máquina virtual. Dichos equipos aparecen como no gestionables (deshabilitados).

Una vez que el agente esté implementado en un servidor ESX/ESXi (esto necesita una licencia para Acronis Backup & Recovery 10 Advanced Server Virtual Edition), las máquinas virtuales desde este servidor están listas para aplicar una política de copias de seguridad o una copia de seguridad individual. Dichos equipos aparecen como gestionables.

*Si Agent para Windows o Agent para Linux están instalados en un sistema invitado, pero no hay Agent para ESX/ESXi en su servidor, la máquina virtual aparece como no gestionable debajo de **Máquinas virtuales**. Dicho equipo deberá gestionarse como un equipo físico.*

#### Del lado de vCenter Server

Cuando la integración está habilitada, vCenter Server almacenará y mostrará la información sobre cuándo y cuán correctamente se realizó la copia de seguridad de la máquina virtual. La misma

información se muestra en las columnas **Estatus** y **Última copia de seguridad** en el servidor de gestión.

**Estatus de la copia de seguridad**: el estatus más grave de todos los planes de copias de seguridad y las políticas de copias de seguridad en el equipo. Para obtener más información, consulte "Estatus del plan de copias de seguridad (pág. 194)" y "Estado de una política en un equipo (pág. 66)".

**Última copia de seguridad**: tiempo transcurrido desde la última copia de seguridad realizada correctamente.

Puede ver esta información en el resumen de la máquina virtual (**Resumen** > **Anotaciones**) o en la pestaña **Máquinas virtuales** para cada servidor, centro de datos, carpeta o vCenter Server completo (por ejemplo, **Ver** > **Inventario** > **Servidores y sectores del disco** > seleccione el servidor> **Máquinas virtuales**).

### 3.2.7 Proxy de copia de seguridad en línea

Esta opción está vigente únicamente para conexiones con Acronis Online Backup Storage a través de Internet.

Esta opción define si el servidor de gestión se conectará a Internet a través de un servidor proxy.

***Nota:*** *Acronis Backup & Recovery 10 Online es compatible únicamente con servidores proxy http y https.*

Las configuraciones de proxy para el agente y el servidor de gestión se configuran de forma separada, incluso si están instaladas en el mismo equipo.

***Para configurar los servidores proxy***

1. Seleccione la casilla de verificación **Utilizar un servidor proxy**.
2. En **Dirección**, especifique el nombre de la red o la dirección IP del servidor proxy; por ejemplo: **proxy.ejemplo.com** o **192.168.0.1**
3. En **Puerto**, especifique el número de puerto del servidor proxy; por ejemplo: **80**
4. Si el servidor proxy requiere autenticación, especifique las credenciales en **Nombre de usuario** y **Contraseña**.
5. Para probar la configuración del servidor proxy, haga clic en **Probar conexión**.

## 3.3 Opciones del equipo

Las opciones del equipo definen el comportamiento general de las agentes de Acronis Backup & Recovery 10 que funcionan en el equipo gestionado, y así se consideran que las opciones son específicas del equipo.

Para acceder a las opciones del equipo, conéctese al equipo gestionado y selecciones **Opciones** > **Opciones del equipo** desde el menú superior.

### 3.3.1 Gestión del equipo

Esta opción define si el equipo debe ser gestionado centralmente por el Management server Acronis Backup & Recovery 10.

Para poder utilizar esta opción, debe iniciar sesión como miembro del grupo de **Administradores** del equipo.

Puede registrar el equipo en el Management server cuando instala un agente de Acronis Backup & Recovery 10. Si el equipo no está registrado, seleccione **Gestión centralizada** aquí y comenzará el Registro (pág. 412). O puede agregar el equipo al Management server desde el servidor. Para cualquiera de los tres métodos de registro necesita tener privilegios de administrador.

Cuando seleccione **Gestión autónoma** en un equipo registrado terminará la comunicación del equipo con el servidor. En el servidor de gestión, el equipo aparece como **Retirado**. El administrador del servidor de gestión puede eliminar el equipo del servidor o registrarlo nuevamente.

El valor predeterminado: **Gestión autónoma**.

***Para una gestión centralizada en el equipo:***

1. Seleccione **Gestión centralizada**.
2. Especifique el **Nombre o dirección IP del Management server**.
3. Especifique el nombre de usuario y contraseña del administrador del Management server cuando se lo solicite.
4. En la **Dirección de registro del equipo**, seleccione el equipo se registrará en el servidor de gestión: por su nombre (recomendado) o dirección IP
5. Haga clic en **Aceptar** y el equipo se registrará en el servidor de gestión.

Para desactivar la Gestión centralizada, seleccione **Gestión autónoma**.

### 3.3.2 Seguimiento de sucesos

Es posible duplicar los sucesos de registro generados por el agente que funcionan en el equipo gestionado, en el registro de sucesos de aplicación de Windows; o enviar los sucesos al gestor de SNMP especificado. Si no modifica las opciones de seguimiento de sucesos en todos lados menos aquí, su configuración será efectiva para cada plan de copia de seguridad local y cada tarea creada en el equipo.

Puede anular las configuraciones aquí, únicamente para los sucesos que ocurran durante la copia de seguridad o recuperación (Consulte las opciones de copia de seguridad predeterminada y recuperación (pág. 96)) En este caso, las configuraciones serán eficaces para las funciones que no estén relacionadas con la copia de seguridad y la recuperación, como limpieza y validación de archivos comprimidos.

Además podrá anular las configuraciones establecidas en las opciones de copia de seguridad y recuperación, cuando se cree un plan de copia de seguridad predeterminada o tarea de recuperación. Las tareas que obtenga es este caso serán específicas del plan o de la tarea.

#### Registro de sucesos de Windows

Esta opción sólo funciona en los sistemas operativos de Windows.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción define si el agente operativo en el equipo gestionado tiene que recopilar los sucesos en el registro de sucesos de aplicación de Windows (para ver este registro, ejecute **eventvwr.exe** o seleccione **Panel de Control > Herramientas administrativas > Visor de sucesos**). Puede filtrar los sucesos a ser recopilados.

Puede anular las configuraciones aquí, únicamente para los sucesos que ocurran durante la copia de seguridad o recuperación, en las opciones de recuperación y copia de seguridad predeterminada (pág. 96). En este caso, las configuraciones serán eficaces para las funciones que no estén

relacionadas con la copia de seguridad y la recuperación, como limpieza y validación de archivos comprimidos.

Además podrá anular las configuraciones establecidas en las opciones de copia de seguridad predeterminada y recuperación, cuando se cree un plan de copia de seguridad o tarea de recuperación. Las tareas que obtenga es este caso serán específicas del plan o de la tarea.

El valor predeterminado es: **Deshabilitado**.

Para habilitar esta opción, active la casilla de verificación **Registrar eventos**.

Utilice la casilla de verificación **Tipos de eventos para registrar** para filtrar los eventos que vayan a registrarse en el Registro de sucesos de aplicación de Windows:

- **Todos los eventos**: todos los eventos (información, advertencias y errores)
- **Errores y advertencias**
- **Solo errores**.

Para deshabilitar esta opción, active la casilla de verificación **Registrar eventos**.

## Notificaciones SNMP

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción define si el agente operativo en el equipo gestionado debe enviar los sucesos de registro a los gestores de Simple Network Management Protocol (SNMP). Puede elegir los tipos de sucesos a enviar.

Puede anular las configuraciones aquí, únicamente para los sucesos que ocurran durante la copia de seguridad o recuperación, en las opciones de recuperación y copia de seguridad predeterminada (pág. 96). En este caso, las configuraciones serán eficaces para las funciones que no estén relacionadas con la copia de seguridad y la recuperación, como limpieza y validación de archivos comprimidos.

Además podrá anular las configuraciones establecidas en las opciones de copia de seguridad predeterminada y recuperación, cuando se cree un plan de copia de seguridad o tarea de recuperación. Las tareas que obtenga es este caso serán específicas del plan o de la tarea.

Para obtener información detallada acerca de cómo utilizar SNMP con Acronis Backup & Recovery 10, vaya a "Asistencia para SNMP (pág. 49)".

El valor predeterminado: **Deshabilitado**.

### *Configurar el envío de mensajes SNMP*

1. Active la casilla de verificación **Enviar mensajes al servidor**.
2. Especifique las opciones apropiadas como se detalla a continuación:
   - **Tipos de eventos para enviar**: elija los tipos de eventos: **Todos los eventos**, **Errores y advertencias**, o **Sólo errores**.
   - **Nombre del servidor/IP:** introduzca el nombre o dirección IP del servidor en el que se ejecuta la aplicación de gestión SNMP y al que se enviarán los mensajes.
   - **Comunidad**: tipo de nombre de la comunidad SNMP a la que pertenecen tanto el servidor que ejecuta la aplicación de gestión SNMP como el equipo emisor. La comunidad típica es "pública".

   Haga clic en **Enviar mensaje de prueba** para verificar si la configuración es correcta.

Para deshabilitar el envío de mensajes SNMP, desactive la casilla de verificación **Enviar mensajes al servidor SNMP**.

Los mensajes se envían a través de UDP.

La siguiente sección tiene información adicional sobre la configuración de los servicios SNMP en el equipo receptor (pág. 94).

### La configuración de los servicios SNMP en el equipo receptor.

#### Windows

Para instalar los servicio SNMP en una máquina en la que se ejecuta Windows:

1. **Inicio > Panel de control > Agregar o quitar programas > Agregar o quitar componentes de Windows.**
2. Seleccione las **Herramientas de Gestión y Supervisión**.
3. Haga clic en **Detalles.**
4. Seleccione la casilla de verificación **Protocolo Simple Network Management** .
5. Haga clic en **Aceptar**.

Es posible que se le pida lmmib2.dll, que se encuentra en el disco de instalación de su sistema operativo.

#### Linux

Para recibir mensajes SNMP en un equipo en el que se ejecuta Linux, se deberán instalar los paquetes net-snmp (para RHEL y SUSE) o snmpd (para Debian).

A SNMP se lo puede configurar con el comando **snmpconf**. El archivo de configuración predeterminado está ubicado en el directorio: /etc/snmp:

- /etc/snmp/snmpd.conf - archivo de configuración para el agente Net-SNMP SNMP.
- /etc/snmp/snmptrapd.conf - archivo de configuración para el daemon Net-SNMP.

## 3.3.3 Reglas de limpieza de los registros

Esta opción especifica cómo limpiar el registro del agenteAcronis Backup & Recovery 10.

Esta opción define el tamaño máximo de la carpeta de registro del agente (en un servidor Windows XP/2003, %ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\MMS\LogEvents).

El valor predeterminado: **Tamaño de registro máximo: 1 GB**. **Durante la limpieza, mantenga el 95% del tamaño de registro máximo**.

Cuando la opción está habilitada, el programa compara el tamaño de registro actual con el tamaño máximo cada 100 entradas del registro. Una vez que se excede el tamaño de registro máximo, el programa elimina las entradas de registro más antiguas. Puede seleccionar las entradas del registro a retener. La configuración predeterminada de 95% conservará la mayoría del registro. Con la configuración mínima de 1%, el registro se borrará casi por completo.

Este parámetro también puede establecerse utilizando Acronis Administrative Template (pág. 368).

### 3.3.4 Proxy de copia de seguridad en línea

Esta opción es eficaz sólo para realizar copias de seguridad en Acronis Online Backup Storage y recuperar desde él a través de Internet.

Esta opción si el agente de Acronis se conectará a Internet a través de un servidor proxy.

***Nota:*** *Acronis Backup & Recovery 10 Online es compatible únicamente con servidores proxy http y https.*

***Para configurar los servidores proxy***

1. Seleccione la casilla de verificación **Utilizar un servidor proxy**.
2. En **Dirección**, especifique el nombre de la red o la dirección IP del servidor proxy; por ejemplo: **proxy.ejemplo.com** o **192.168.0.1**
3. En **Puerto**, especifique el número de puerto del servidor proxy; por ejemplo: **80**
4. Si el servidor proxy requiere autenticación, especifique las credenciales en **Nombre de usuario** y **Contraseña**.
5. Para probar la configuración del servidor proxy, haga clic en **Probar conexión**.

Si no conoce la configuración de su servidor proxy, póngase en contacto con su administrador de red o proveedor de servicio de Internet para recibir asistencia.

Como alternativa, puede probar esta configuración desde la configuración de su navegador. A continuación le mostramos cómo encontrarla en tres conocidos exploradores.

- **Microsoft Internet Explorer** En el menú **Herramientas**, haga clic en **Opciones de Internet**. En la pestaña **Conexiones**, haga clic en **Configuración de LAN**.
- **Mozilla Firefox.** En el menú **Herramientas**, haga clic en **Opciones** y después en **Avanzado**. Haga clic en la pestaña **Red** y, en el apartado **Conexión**, haga clic en **Configuración**.
- **Google Chrome.** En **Opciones**, haga clic en **Avanzadas**. En el apartado **Red**, haga clic en **Cambiar la configuración del proxy**.

### 3.3.5 Programa de Experiencia del Cliente

Esta opción define si el equipo participará en el Programa de Experiencia del Cliente de Acronis (PECA).

Si escoge **Sí, deseo participar en el PECA**, la información sobre la configuración de hardware, las funciones que más y menos se utilizan, y cualquier tipo de problema se recopilarán automáticamente del equipo y se enviarán a Acronis regularmente. Los resultados finales tienen como objetivo suministrar mejoras en el software y mayores funcionalidades para satisfacer mejor las necesidades de los clientes de Acronis.

Acronis no recopila ningún dato personal. Para obtener más información acerca del PECA, lea los términos de participación en la página web de Acronis o en la interfaz gráfica de usuario del producto.

Inicialmente, la opción se configura durante la instalación de Acronis Backup & Recovery 10 Agent. Estos ajustes se pueden cambiar en cualquier momento a través de la interfaz gráfica de usuario (**Opciones** > **Opciones del equipo** > **Programa de Experiencia del Cliente**). La opción también se puede configurar a través de la Infraestructura de la política de grupo (pág. 372). Un ajuste definido con una política de grupo no puede modificarse a través de la interfaz gráfica de usuario del producto a menos que la política de grupo se deshabilite en el equipo.

## 3.4 Opciones predeterminadas de copia de seguridad y recuperación

### 3.4.1 Opciones de copia de seguridad predeterminadas

Cada agente de Acronis tiene sus propias opciones predeterminadas de copia de seguridad. Una vez instalado el agente, las opciones predeterminadas tienen valores predefinidos, que se consideran **preajustes** en la documentación. Cuando crea un plan de copia de seguridad, puede utilizar una opción predeterminada o anular la opción predeterminada mediante el valor personalizado que se especificará únicamente para este plan.

También puede personalizar una opción predeterminada al cambiar su valor a otro diferente al predefinido. El nuevo valor se utilizará de manera predeterminada para todos los planes de copias de seguridad que cree en su equipo en adelante.

Para ver o cambiar las opciones de copia de seguridad predeterminadas, conecte la consola al equipo gestionado y después seleccione **Opciones > Opciones predeterminadas de copia de seguridad y recuperación > Opciones predeterminadas de copia de seguridad** en el menú superior.

#### Disponibilidad de las opciones de copia de seguridad

El conjunto de opciones de copia de seguridad disponible depende de:

- El entorno en el que opera el agente (Windows, dispositivo de arranque)
- El tipo de datos que se está copiando (disco, archivo)
- El destino de la copia de seguridad (ubicación en redes o disco local)
- El esquema de copia de seguridad (realizar copia de seguridad ahora o utilizando el programador)

La siguiente table resume la disponibilidad de las opciones de copia de seguridad.

| | **Agente de Windows** | | **Medio de inicio (Basado en Linux o basado en PE)** | |
|---|---|---|---|---|
| | **Copia de seguridad del disco** | **Copia de seguridad del archivo** | **Copia de seguridad del disco** | **Copia de seguridad del archivo** |
| Protección del archivo comprimido (pág. 98) (contraseña + cifrado) | + | + | + | + |
| Exclusión de archivos de origen (pág. 99) | + | + | + | + |
| Comandos previos o posteriores a la copia de seguridad (pág. 100) | + | + | sólo PE | sólo PE |
| Comandos previos o posteriores a la captura de datos (pág. 102) | + | + | - | - |
| Instantánea multivolumen (pág. 105) | + | + | - | - |

| | | | | |
|---|---|---|---|---|
| Instantánea de la copia de seguridad a nivel de archivo (pág. 104) | - | + | - | - |
| Utilizar VSS (pág. 105) | + | + | - | - |
| Nivel de compresión (pág. 106) | + | + | + | + |
| Rendimiento de la copia de seguridad: | | | | |
| Prioridad de la copia de seguridad (pág. 107) | + | + | - | - |
| Velocidad de escritura del HDD (pág. 107) | Destino: HDD | Destino: HDD | Destino: HDD | Destino: HDD |
| Velocidad de la conexión de red (pág. 108) | Destino: red compartida | Destino: red compartida | Destino: red compartida | Destino: red compartida |
| Copias de seguridad incrementales/diferenciales rápidas (pág. 111) | + | - | + | - |
| División de copias de seguridad (pág. 112) | + | + | + | + |
| Seguridad a nivel de archivo (pág. 112): | | | | |
| Preservar el ajuste de seguridad de los archivos comprimidos en las copias de seguridad | - | + | - | - |
| En un archivo comprimido, almacenar sin cifrar los archivos cifrados | - | + | - | - |
| Componentes de medios | Destino: medio extraíble | Destino: medio extraíble | - | - |
| Manejo de errores (pág. 114): | | | | |
| No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso) | + | + | + | + |
| Reintentar si se produce un error | + | + | + | + |
| Ignorar los sectores defectuosos | + | + | + | + |
| Doble destino (pág. 114) | Destino: local | Destino: local | - | - |
| Condiciones de inicio de la tarea (pág. 115) | + | + | - | - |
| Manejo de fallos de la tarea (pág. 116) | + | + | - | - |
| Soporte de cintas (pág. 117) | Destino: bóveda gestionada en biblioteca de cintas | Destino: bóveda gestionada en biblioteca de cintas | Destino: bóveda gestionada en biblioteca de cintas | Destino: bóveda gestionada en biblioteca de cintas |
| Ajustes adicionales (pág. 119): | | | | |

| | | | | |
|---|---|---|---|---|
| Sobrescribir los datos en una cinta sin solicitar la confirmación del usuario | Destino: Cinta | Destino: Cinta | Destino: Cinta | Destino: Cinta |
| Desmontar dispositivos después de que la copia de seguridad haya finalizado | Destino: medio extraíble | Destino: medio extraíble | Destino: medio extraíble | Destino: medio extraíble |
| Solicitar el primer medio al realizar la copia de seguridad en un medio extraíble. | Destino: medio extraíble | Destino: medio extraíble | Destino: medio extraíble | Destino: medio extraíble |
| Restablecer el bit del archivo comprimido | - | + | - | + |
| Reiniciar el equipo automáticamente después de que finalice la copia de seguridad | - | - | + | + |
| Deduplicar la copia de seguridad sólo después de transferirla a la bóveda | Destino: deduplicación de bóveda | Destino: deduplicación de bóveda | Destino: deduplicación de bóveda | Destino: deduplicación de bóveda |
| Utilizar FTP en modo activo | Destino: Servidor FTP | Destino: Servidor FTP | Destino: Servidor FTP | Destino: Servidor FTP |
| Notificaciones: | | | | |
| Correo electrónico (pág. 108) | + | + | - | - |
| Win Pop-up (pág. 109) | + | + | - | - |
| Rastreo de eventos: | | | | |
| Registro de eventos de Windows (pág. 110) | + | + | - | - |
| SNMP (pág. 111) | + | + | - | - |

## Protección del archivo comprimido

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio..

Esta opción es eficaz tanto para la copia de seguridad a nivel de disco como a nivel de archivo.

El valor predeterminado: **Deshabilitado.**

***Para proteger el archivo comprimido de accesos no autorizados***

1. Seleccione la casilla de verificación **Establecer la contraseña para el archivo comprimido**.
2. En el campo **Introducir contraseña,** escriba la contraseña.
3. En el campo **Confirmar contraseña**, vuelva a escribir la contraseña.
4. Seleccione una de las siguientes opciones:
   - **No cifrar**: el archivo comprimido estará protegido sólo con la contraseña
   - **AES 128:** se cifrará el archivo comprimido por medio del algoritmo estándar avanzado de cifrado (AES) con una clave de 128 bits
   - **AES 192:** se cifrará el archivo comprimido por medio del algoritmo AES con una clave de 192-bits
   - **AES 256:** se cifrará el archivo comprimido por medio del algoritmo AES con una clave de 256-bits

5. Haga clic en **Aceptar**.

El algoritmo de cifrado AES funciona en el modo Cipher-block chaining (CBC) y utiliza una clave generada de manera aleatoria con un tamaño definido por el usuario de 128, 192 ó 256 bits. Cuanto más grande sea el tamaño de clave, más tiempo se tardará en cifrar el archivo comprimido y más seguros estarán los datos.

Luego, la clave de cifrado se cifra con AES-256 usando un hash SHA-256 de la contraseña como clave. La contraseña no se guarda en ninguna parte del disco o del archivo de copia de seguridad; el hash de la contraseña se usa como para verificación. Con esta seguridad con dos niveles, los datos de copia de seguridad están protegidos contra el acceso no autorizado.

## Exclusión de archivos de origen

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio..

Esta opción es eficaz solo para copias de seguridad a nivel de disco de sistemas de archivos NTFS y FAT. Esta opción es eficaz para copias de seguridad a nivel de archivos de todos los sistemas de archivos compatibles.

La opción define qué archivos y carpetas omitir durante el proceso de copia de seguridad y que, por lo tanto, quedan excluidos de la lista de datos que se incluirán en la copia de seguridad.

El valor predeterminado es: **Excluir los archivos que coincidan con los siguientes criterios *.tmp, *.~, *.bak.**

***Para especificar los archivos y carpetas que desea excluir:***

Configure alguno de los siguientes parámetros:

- **Excluir todos los archivos y carpetas ocultos**

  Esta opción está vigente sólo para sistemas de archivos compatibles con Windows. Seleccione esta casilla de verificación para omitir archivos y carpetas con el atributo **Oculto**. Si una carpeta está **Oculta**, se excluirán todos sus contenidos, incluso los archivos que no se encuentran **Ocultos**.
- **Excluir todos los archivos y carpetas del sistema**

  Esta opción está vigente sólo para sistemas de archivos compatibles con Windows. Seleccione esta casilla de verificación para omitir archivos y carpetas con el atributo **Sistema**. Si una carpeta tiene el atributo **Sistema**, se excluirán todos sus contenidos, incluso los archivos que no tengan el atributo **Sistema**.

*Puede ver los atributos del archivo o de la carpeta en las propiedades del archivo/carpeta o mediante el comando **atrib**. Para obtener más información, consulte el Centro de Servicio Técnico y Ayuda de Windows.*

- **Excluir los archivos que coincidan con los siguientes criterios**

  Seleccione esta casilla de verificación para omitir los archivos y las carpetas cuyos nombres en la lista coincidan con alguno de los criterios, llamados máscaras del archivo; utilice los botones **Agregar**, **Editar**, **Eliminar** y **Eliminar todos** para crear la lista de máscaras del archivo.

  Puede utilizar uno o más caracteres comodín * y ? en una máscara de archivo:

  El asterisco (*) sustituye de cero a más caracteres del nombre del archivo; por ejemplo, la máscara de archivo Doc*.txt genera archivos Doc.txt y Document.txt

  El signo de interrogación (?) substituye a un único carácter; por ejemplo, la máscara de archivo Doc?.txt genera archivos Doc1.txt y Docs.txt, pero, por el contrario, no general archivos Doc.txt o Doc11.txt

Para excluir una carpeta especificada por una ruta que contiene la letra de unidad, agregue una barra invertida (\) al nombre de carpeta en el criterio; por ejemplo: C:\Finance\

**Ejemplos de exclusión**

| Criterio | Ejemplo | Descripción |
|---|---|---|
| **Windows y Linux** | | |
| Por nombre | F.log<br>F | Excluye todos los archivos denominados "F.log"<br>Excluye todas las carpetas denominadas "F" |
| Por máscara (*) | *.log<br>F* | Excluye todos los archivos con la extensión .log<br>Excluye todos los archivos y carpetas cuyos nombres comiencen con "F" (como carpetas F, F1 y archivos F.log, F1.log) |
| Por máscara (?) | F???.log | Excluye todos los archivos .log cuyos nombres contengan cuatro símbolos y comiencen con "F" |
| **Windows** | | |
| Por ruta de archivo | C:\Finance\F.log | Excluye el archivo denominado "F.log" ubicado en la carpeta C:\Finance |
| Por ruta de carpeta | C:\Finance\F\ | Excluye la carpeta C:\Finance\F (asegúrese de especificar la ruta completa, comenzando por la letra de unidad) |
| **Linux** | | |
| Por ruta de archivo | /home/user/Finance/F.log | Excluye el archivo denominado "F.log", ubicado en la carpeta /home/user/Finance |
| Por ruta de carpeta | /home/user/Finance/ | Excluye la carpeta /home/user/Finance |

*Los ajustes anteriores no afectan a los archivos o carpetas seleccionados expresamente para la copia de seguridad. Por ejemplo, supongamos que seleccionó la carpeta MiCarpeta y el archivo MiArchivo.tmp fuera de esa carpeta, y seleccionó la opción de omitir todos los archivos .tmp. En este caso, todos los archivos .tmp de la carpeta MiCarpeta serán omitidos durante el proceso de copia de seguridad, pero no se omitirá el archivo MiArchivo.tmp.*

## Comandos pre / post

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio basados en PE..

Esta opción le permite definir los comandos a ejecutar automáticamente antes y después del proceso de copia de seguridad.

El siguiente esquema describe cuando se ejecutan los comandos pre/post.

| Comando de pre-Copia de seguridad | Copia de seguridad | Comando de post-copia de seguridad |
|---|---|---|

Ejemplos de como se pueden usar los comandos pre/post:

- eliminación de archivos temporales antes de comenzar la copia de seguridad
- configuración de un producto antivirus de terceros antes de comenzar la copia de seguridad
- copia de un archivo comprimido a otra ubicación después de que termine la copia de seguridad.

El programa no admite comandos interactivos, es decir, comandos que requieran la intervención del usuario (por ejemplo, “pause”).

***Para especificar comandos pre/post***

1. Puede habilitar la ejecución de comandos pre/post al marcar las siguientes opciones:
   - **Ejecutar antes de la copia de seguridad**
   - **Ejecutar después de la copia de seguridad**
2. Realice uno de los siguientes:
   - Haga clic en **Editar** para especificar un nuevo comando o un archivo por lotes
   - Seleccione el comando existente o el archivo por lotes de la lista desplegable
3. Haga clic en **Aceptar**.

## Comando de pre-copia de seguridad

***Para especificar un comando o archivo por lotes para que se ejecute antes de que comience el proceso de copia de seguridad***

1. En el campo **Comando**, introduzca un comando o examine hasta encontrar un archivo por lotes. El programa no admite comandos interactivos, es decir, comandos que exijan la intervención del usuario (por ejemplo, “pause”).
2. En el campo **Directorio de trabajo**, especifique la ruta mediante la que se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
5. Haga clic en **Probar comando** para verificar si el comando es correcto.

| **Casilla de verificación** | **Selección** | | | |
|---|---|---|---|---|
| **Hacer que la tarea falle si falla la ejecución del comando** | Seleccionado | Borrado | Seleccionado | Borrado |
| **No realizar la copia de seguridad hasta que finalice la ejecución de comandos** | Seleccionado | Seleccionado | Borrado | Borrado |
| **Resultado** | | | | |
| | **Valor predeterminado**<br>Realizar la copia de seguridad solo después de que se ejecute el comando correctamente. Hacer que la tarea falle si | Realizar la copia de seguridad después de que se ejecute el comando a pesar del éxito o fallo de la ejecución | N/A | Realizar la copia de seguridad al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando. |

| | | | | |
|---|---|---|---|---|
| | falla la ejecución del comando | | | |

## Comando de post-copia de seguridad

***Para especificar un comando o archivo que se ejecute después de completar la copia de seguridad***

1. En el campo **Comando**, ingrese un comando o examinar hasta encontrar un archivo por lotes.
2. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Si es crítico que la ejecución del comando sea satisfactoria para su estrategia de copia de seguridad, marque la casilla de verificación **para suspender la tarea si falla la ejecución del comando**. Si la ejecución del comando falla, el programa eliminará el archivo TIB y los archivos temporales resultantes, si fuera posible, y la tarea fallará.

   Cuando no se marca la casilla de verificación, los resultados de la ejecución de comando no afectarán el éxito o fallo cuando se ejecute la tarea. Se puede seguir los resultados de la ejecución de comandos al explorar el registro de errores y advertencias que se muestran en el **Tablero**.
5. Haga clic en **Probar comando** para verificar el archivo si el comando es correcto.

## Comandos previos o posteriores a la captura de datos

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux..

La opción le permite definir los comandos que se ejecutarán automáticamente antes y después de la captura de datos (es decir, tomar la instantánea de los datos). La captura de datos la realiza Acronis Backup & Recovery 10 al comienzo del procedimiento de copia de seguridad.

El siguiente esquema describe cuando se ejecutan los comandos pre/post de la captura de datos.

| | <---------- Copia de seguridad ----------> | | | | |
|---|---|---|---|---|---|
| Comando de precopia de seguridad | Comandos antes de la captura de datos | Captura de datos | Comandos Post de la captura de datos | | Comando de Post-copia de seguridad |

Si la opción Servicio de instantáneas de volumen (pág. 105) está habilitada, la ejecución de los comandos y las acciones de Microsoft VSS se sucederán tal y como se indica a continuación:

Comandos "Antes de la captura de datos" -> Suspensión de VSS -> Captura de datos -> Reanudación de VSS -> Comandos "Después de la captura de datos".

El uso de comandos Pre/Post de la captura de datos, puede suspender y reanudar la base de datos o la aplicación que no sea compatible con VSS. A diferencia de los Comandos pre/post (pág. 100), los comandos antes/después de la captura de datos se ejecutarán antes y después del proceso de captura de datos. Esto demora segundos. El proceso completo de copia de seguridad puede demorar más tiempo, según la cantidad de datos que se incluirá en la copia de seguridad. Por lo tanto, el tiempo de inactividad de la base de datos o aplicación será mínimo.

***Para especificar los comandos Pre/Post de la captura de datos***

1. Puede habilitar la ejecución de comandos de captura de datos Pre/Post al marcar las siguientes opciones:
   - **Ejecutar antes de la captura de datos**

- **Ejecutar después de la captura de datos**

2. Realice uno de los siguientes pasos:
   - Haga clic en **Editar** para especificar un nuevo comando o un archivo por lotes
   - Seleccione el comando existente o el archivo por lotes de la lista desplegable.
3. Haga clic en **Aceptar**.

## Comandos antes de la captura de datos

***Para especificar un comando o archivo por lotes para que se ejecute antes de la captura de datos***

1. En el campo **Comando**, introduzca un comando o examine hasta encontrar un archivo por lotes. El programa no admite comandos interactivos, es decir, comandos que exijan la intervención del usuario (por ejemplo, “pause”).
2. En el campo **Directorio de trabajo**, especifique la ruta mediante la que se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
5. Haga clic en **Probar comando** para verificar si el comando es correcto.

| **Casilla de verificación** | **Selección** | | | |
|---|---|---|---|---|
| **Hacer que la tarea de copia de seguridad falle si falla la ejecución del comando** | Seleccionado | Borrado | Seleccionado | Borrado |
| **No realizar la captura de datos hasta que finalice la ejecución de comandos** | Seleccionado | Seleccionado | Borrado | Borrado |
| **Resultado** | | | | |
| | **Valor predeterminado**<br>Realizar la captura de datos solo después de que se ejecute el comando correctamente. Hacer que la tarea falle si falla la ejecución del comando | Realizar la captura de datos después de que se ejecute el comando a pesar del éxito o fallo de la ejecución | N/A | Realizar la captura de datos al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando. |

## Comandos Post de la captura de datos

***Para especificar un comando o archivo por lotes para que se ejecute después de la captura de datos***

1. En el campo **Comando**, introduzca un comando o examine hasta encontrar un archivo por lotes. El programa no admite comandos interactivos, es decir, comandos que exijan la intervención del usuario (por ejemplo, “pause”).
2. En el campo **Directorio de trabajo**, especifique la ruta mediante la que se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
5. Haga clic en **Probar comando** para verificar si el comando es correcto.

| **Casilla de verificación** | **Selección** | | | |
|---|---|---|---|---|
| **Hacer que la tarea falle si falla la ejecución del comando** | Seleccionado | Borrado | Seleccionado | Borrado |
| **No realizar la copia de seguridad hasta que finalice la ejecución de comandos** | Seleccionado | Seleccionado | Borrado | Borrado |
| **Resultado** | | | | |
| | **Valor predeterminado**<br>Continúe la copia de seguridad solo después de que se ejecute el comando correctamente. Elimina el archivo tib y los archivos temporales y suspende la tarea si falla la ejecución del comando. | Continúe la copia de seguridad después de que se ejecute el comando a pesar del éxito o fallo de su ejecución. | N/A | Continuar la copia de seguridad al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando. |

## Instantánea de la copia de seguridad a nivel de archivo

Esta opción es eficaz sólo para la copia de seguridad a nivel de archivo. En sistemas operativos de Windows y Linux.

Esta opción define si se hace una copia de seguridad archivo por archivo o si se toma una instantánea de los datos.

***Nota:*** *A los archivos que no estén almacenados en redes compartidas se le realizará la copia de seguridad uno a uno.*

El valor predeterminado: **Crear instantáneas si es posible.**

Seleccione una de las siguientes opciones:

- **Siempre crear una instantánea**

  La instantánea permite la copia de seguridad de todos los archivos, inclusive los archivos abiertos para accesos exclusivos. Los archivos se incluirán en la copia de seguridad al mismo momento determinado. Seleccione esta configuración sólo si los factores son críticos, es decir: la copia de seguridad sin tomar una instantánea no tiene sentido. Para utilizar una instantánea, el plan de copia de seguridad se debe ejecutar con una cuenta que tenga los privilegios de Administrador o de Copia de seguridad. Si no se puede tomar una instantánea, la copia de seguridad fallará.
- **Crear instantáneas si es posible.**

  Realizar la copia de seguridad directamente si no es posible tomar una instantánea.
- **No crear una instantánea**

  Siempre realizar la copia de seguridad directamente. No son necesarios los privilegios de Administrador o de operador de copia de seguridad. El intento de copia de seguridad de archivos que están abiertos para acceso exclusivo generará un error de lectura. Los archivos en la copia de seguridad puede que no sean consistentes en el tiempo.

## Instantánea multivolumen

Esta opción es eficaz sólo en los sistemas operativos de Windows y Linux.

Esta opción se aplica a copia de seguridad de nivel del disco. Esta opción también se aplica a la copia de seguridad a nivel de archivo cuando se realiza una copia de seguridad a nivel de archivo al tomar una instantánea. (La opción de instantánea de la copia de seguridad a nivel de archivo (pág. 104) determina si se tomará una instantánea durante la copia de seguridad a nivel de archivo).

La opción determina si se tomarán instantáneas de varios volúmenes al mismo tiempo o uno a uno.

El valor predeterminado: **Habilitar.**

Cuando se establece la opción **Habilitar**, se creará las instantáneas simultáneamente de todos los volúmenes de los que se hace la copia de seguridad. Utilice esta opción para crear una copia de seguridad consistente en el tiempo de datos que están en varios volúmenes, por ejemplo para una base de datos Oracle.

Cuando se establece la opción **Deshabilitar**, se tomaran instantáneas de los volúmenes una después de la otra. Como resultado, si los datos están en varios volúmenes, la copia de seguridad que se obtiene no será consistente.

## Servicio de instantáneas de volumen

Esta opción es eficaz sólo en los sistemas operativos de Windows y Linux.

La opción define si un proveedor de Servicio de instantáneas de volumen (VSS), o un VSS de Acronis o VSS de Microsoft, tiene que notificar a las aplicaciones compatibles con VSS que la copia de seguridad está por iniciarse. Esto garantiza el estado consistente de todos los datos usados por las aplicaciones, en particular por la finalización de todas las transacciones de las bases de datos de Acronis Backup & Recovery 10. En cambio, la consistencia de los datos garantiza que la aplicación se recuperará en el estado correcto y será operativa inmediatamente después de la recuperación.

El valor predeterminado: **Crear instantáneas con VSS**

Acronis Backup & Recovery 10 seleccionará el proveedor de VSS automáticamente basado en el sistema operativo en ejecución en el equipo, siempre que el equipo sea miembro de un dominio de Active Directory.

**Crear instantáneas sin utilizar VSS**

Escoja esta opción si su base de datos es incompatible con VSS. Acronis Backup & Recovery 10 tomará automáticamente la instantánea de datos. El proceso de copia de datos es más rápido, pero no es posible garantizar la consistencia de datos de las aplicaciones cuyas transacciones no se completaron en el momento de la toma de la instantánea. Puede utilizar Comandos antes/después de la captura de datos (pág. 102) para indicar los comandos que se deberían ejecutarse antes y después de tomar la instantánea para garantizar que los datos que se incluyen en la copia de seguridad tienen un estado consistente. Por ejemplo, especifique los comandos de captura anterior a los datos que suspenderán la base de datos y vacía la memoria caché para garantizar que se completen todas las transacciones, y especificar los comandos Post de la captura de datos que reanudarán las operaciones después de tomar las instantáneas.

### Copiadoras de instantáneas de volumen

Antes de realizar una copia de seguridad de los datos de aplicaciones compatibles con VSS, asegúrese de que las copiadoras de instantáneas de volumen para esas aplicaciones estén activadas al examinar la lista de copiadoras que se encuentran en el sistema operativo. Para ver esta lista, ejecute el siguiente comando:

```
vssadmin list writers
```

***Nota:*** *En Microsoft Windows Small Business Server 2003, el escritor para Microsoft Exchange Server 2003 está desactivado de manera predeterminada. Para obtener instrucciones acerca de cómo activarlo, consulte el artículo del Servicio técnico y ayuda de Microsoft (http://support.microsoft.com/kb/838183/es) correspondiente.*

## Nivel de compresión

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

Esta opción define el nivel de compresión que se aplicará a los datos que se incluyen en la copia de seguridad.

El valor predeterminado: **Normal.**

El nivel de compresión de datos óptimo dependerá del tipo de datos que se incluyen en la copia de seguridad. Por ejemplo, ni siquiera la máxima compresión conseguirá reducir significativamente el tamaño del archivo comprimido si éste incluye archivos esencialmente comprimidos, como .jpg, .pdf o .mp3. Sin embargo, los formatos como .doc o .xls estarán bien comprimidos.

***Para especificar el nivel de compresión de los datos.***

Seleccione una de las siguientes:

- **Ninguno**: los datos se copiarán como se encuentra, sin ningún tipo de compresión. El tamaño de la copia de seguridad resultante será máximo.
- **Normal**: recomendado en la mayoría de los casos.
- **Alto:** El tamaño de la copia de seguridad resultante será menor al nivel típico **Normal**.

- **Máximo:** se comprimirá los datos tanto como sea posible. La duración de la copia de seguridad será máxima. Es posible que desee seleccionar compresión Máxima para los medios extraíbles y así reducir la cantidad de discos en blanco que necesite.

### Rendimiento de la copia de seguridad.

Utilice este grupo de opciones para especificar la cantidad de recursos de la red y del sistema que desea asignar para el proceso de copia de seguridad.

Las opciones de rendimiento de la copia de seguridad pueden tener un efecto más o menos perceptible en la velocidad del proceso de copia de seguridad. Esto depende del configuración general del sistema y las características físicas de los dispositivos desde o hacia los que se realiza la copia de seguridad.

## Prioridad de la copia de seguridad

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

La prioridad de un proceso que se ejecute en un sistema determina la cantidad de uso de la CPU y los recursos del sistema que se asignan a dicho proceso. La disminución de la prioridad de la copia de seguridad liberará más recursos para otras aplicaciones. El aumento de la prioridad podría acelerar el proceso de copia de seguridad al solicitar que el sistema operativo asigne más recursos como CPU a la aplicación de copia de seguridad. Sin embargo, el efecto resultante dependerá del uso total del CPU y otros factores como velocidad de salida o entrada del disco o el tráfico en la red.

El valor predeterminado: **Bajo.**

***Para especificar la prioridad del proceso de copia de seguridad***

Seleccione una de las siguientes:

- **Bajo**: para minimizar el uso de recursos por parte del proceso de copia de seguridad lo que dejará más recursos para otros procesos que se ejecuten en el equipo.
- **Normal**: ejecución del proceso de copia de seguridad con la velocidad normal, lo que permite asignar recursos al mismo nivel de otros procesos
- **Alto:** maximizará la velocidad del proceso de copia de seguridad al tomar recursos de otros procesos.

## Velocidad de escritura del HDD

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

Esta opción se encuentra disponible cuando se realiza la copia de seguridad de un disco duro interno (fijo) del equipo al que se eligió como destino de la copia de seguridad.

La copia de seguridad en un disco duro (por ejemplo en Acronis Secure Zone) puede disminuir el rendimiento del sistema operativo y las aplicaciones por la gran cantidad de datos que se deben escribir en el disco. Puede limitar el uso del disco duro mediante el proceso de copia de seguridad al nivel deseado.

El valor predeterminado: **Máximo.**

***Para establecer la velocidad de grabación del disco duro (HDD) para copia de seguridad***

Realice uno de los siguientes:

- Haga Clic en **Velocidad de grabación indicada como un porcentaje de la velocidad máxima del disco duro de destino**, y luego arrastre el deslizador o seleccione un porcentaje en la caja
- Haga Clic en **Velocidad de grabación expresada en kilobytes por segundo**, y después ingrese la velocidad de grabación del disco en kilobytes por segundo

## Velocidad de la conexión de red

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

Esta opción se encuentra disponible cuando se selecciona una ubicación en la red (Redes compartidas, bóveda gestionada o un servidor FTP/SFTP) como el destino de la copia de seguridad.

Esta opción define el ancho de banda asignado a la conexión de red para la transferencia de los datos de la copia de seguridad.

Se establece la velocidad máxima de manera predeterminada, es decir que el software utiliza todo el ancho de banda que puede obtener cuando se transfieran los datos de la copia de seguridad. Utilice esta opción para reservar una parte del ancho de banda de la red para otras actividades de la red.

El valor predeterminado: **Máximo.**

***Para establecer la velocidad de la conexión de red para la copia de seguridad.***

Realice uno de los siguientes:

- Haga Clic en **Velocidad de transferencia indicada como un porcentaje de la velocidad máxima de la conexión de red**, y luego arrastre el deslizador o tipo de porcentaje en la caja
- Haga Clic en **Velocidad de transferencia expresada en kilobytes por segundo**, y después ingrese el límite de ancho de banda para la transferencia de datos de la copia de seguridad en kilobytes por segundo

# Notificaciones

Acronis Backup & Recovery 10 proporciona la capacidad de informar a los usuarios sobre la finalización de una copia de seguridad por correo electrónico o servicio de mensajes.

## Correo electrónico

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

La opción le permite recibir notificaciones por correo electrónico sobre la finalización satisfactoria de la tarea de copia de seguridad, fallo o necesidad de interacción por todo el registro de la tarea.

El valor predeterminado: **Deshabilitado**.

***Configurar notificación por correo electrónico***

1. Active la casilla de verificación **Enviar notificaciones por correo electrónico** para activar las notificaciones.

2. En el campo **Direcciones de correo electrónico**, escriba la dirección de correo electrónico a la que se enviarán las notificaciones. Puede introducir varias direcciones separadas por punto y coma.
3. Debajo de **Enviar notificaciones**, seleccione las casillas de verificación adecuadas como se indica a continuación:
   - **Cuando la copia de seguridad finaliza correctamente**: enviar una notificación cuando la copia de seguridad haya finalizado correctamente.
   - **Cuando la copia de seguridad falla**: enviar una notificación cuando la copia de seguridad falle.

   La casilla de verificación **Cuando la interacción del usuario sea necesaria** está activada.
4. Para que el mensaje de correo electrónico incluya las entradas del registro relacionadas con la copia de seguridad, active la casilla de verificación **Agregar registro completo a la notificación**.
5. Haga clic en **Parámetros adicionales de correo electrónico** para configurar parámetros adicionales de correo electrónico como se detalla a continuación y después haga clic en **Aceptar**:
   - **De**: escriba la dirección de correo electrónico del usuario emisor del mensaje. Si no completa este campo, los mensajes se crearán como si se enviaran desde la dirección de destino.
   - **Utilizar cifrado**: puede optar por una conexión cifrada al servidor de correo. Los tipos de cifrado SSL y TLS se encuentran disponibles para su elección.
   - Algunos proveedores de servicios de Internet exigen la autenticación del servidor de correo entrante antes de permitir enviar cualquier información. Si ese es su caso, active la casilla de verificación **Inicio de la sesión en el servidor de correo entrante** para habilitar el servidor POP y configurar sus ajustes:
     - **Servidor de correo entrante (POP)**: escriba el nombre del servidor POP.
     - **Puerto**: configure el puerto del servidor POP. De manera predeterminada, el puerto está configurado en 110.
     - **Nombre de usuario**: introduzca el nombre de usuario
     - **Contraseña**: introduzca la contraseña.
   - Active la casilla de verificación **Utilizar el servidor de correo saliente especificado** para habilitar un servidor SMTP y configurar sus ajustes:
     - **Servidor de correo saliente (SMTP)**: escriba el nombre del servidor SMTP.
     - **Puerto:** configure el puerto del servidor SMTP. De manera predeterminada, el puerto se establece en 25.
     - **Nombre de usuario**: introduzca el nombre de usuario
     - **Contraseña**: introduzca la contraseña.
6. Haga clic en **Enviar mensaje de correo electrónico de prueba** para comprobar que los ajustes son correctos.

## Servicio de Messenger (WinPopup)

Esta opción es eficaz para los sistemas operativos Windows y Linux del equipo emisor y sólo para Windows en el equipo receptor.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

La opción le permite recibir notificaciones WinPopup sobre la finalización satisfactoria de la tarea de copia de seguridad, fallo o necesidad de interacción.

El valor predeterminado: **Deshabilitado.**
Antes de configurar las notificaciones de WinPopup, asegúrese de que el servicio Messenger se encuentra activo tanto en el equipo que ejecuta la tarea como en el que recibirá los mensajes.

El servicio Messenger no se activa de manera predeterminada en la familia Microsoft Windows Server 2003. Cambie el servicio de Modo de inicio a Automático e inícielo.

***Para configurar las notificaciones de WinPopup:***

1. Active la casilla de verificación **Enviar notificaciones de WinPopup**.
2. En el campo **Nombre del equipo**, escriba el nombre del equipo al que se enviarán las notificaciones. No es posible introducir varios nombres.

Debajo de **Enviar notificaciones**, seleccione las casillas de verificación adecuadas como se indica a continuación:

- **Cuando se realiza la copia de seguridad satisfactoriamente**: envía una notificación cuando se completa satisfactoriamente la operación de copia de seguridad.
- **Cuando la copia de seguridad falla**: envía una notificación cuando la copia de seguridad falla.

Casilla de verificación **Cuando se requiere interacción con el usuario**: envía una notificación durante la operación cuando se requiere de la interacción con el usuario, siempre seleccionada.

Haga clic en **Enviar mensaje de WinPopup de prueba** para verificar si la configuración es correcta.

### Seguimiento de sucesos

Es posible duplicar los sucesos de registro en la operación de copia de seguridad, realizada en el equipo gestionado, en el registro de sucesos de aplicación de Windows; o enviar los sucesos al gestor de SNMP especificado.

## Registro de sucesos de Windows

Esta opción sólo funciona en los sistemas operativos de Windows.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción define si el agente operativo en el equipo gestionado tiene que recopilar los sucesos de operaciones de copias de seguridad en el registro de sucesos de aplicación de Windows (para ver este registro, ejecute **eventvwr.exe** o seleccione **Panel de Control > Herramientas administrativas > Visor de sucesos**). Puede filtrar los sucesos a ser recopilados.

El valor predeterminado: **Use la configuración en las configuración del Equipo.**

***Seleccione si desea recopilar los sucesos de operaciones de copia de seguridad en el Registro de sucesos de aplicación de Windows:***

Elija una de las siguientes opciones:

- **Usar la configuración establecida en las opciones del Equipo:** use la configuración establecida para el equipo. Para obtener más información, consulte opciones de Equipo (pág. 91).
- **Registrar los siguientes tipos de eventos**: recopilación de sucesos de operaciones de copia de seguridad en Registro de sucesos de aplicación. Especifique los tipos de sucesos a recopilar:
  - **Todos los eventos**: recopilación de los sucesos (información, advertencias y errores)
  - **Errores y advertencias**
  - **Sólo errores**

- **No recopilar**: desactiva el registro de sucesos de operaciones de copia de seguridad en el Registro de sucesos de aplicación.

## Notificaciones SNMP

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción define si el agente operativo en el equipo gestionado debe enviar los sucesos de registro de las operaciones de copia de seguridad a los gestores especificados de Protocolo Simple Network Management (SNMP). Puede elegir los tipos de sucesos a enviar.

Para obtener información detallada acerca de cómo utilizar SNMP con Acronis Backup & Recovery 10, vaya a "Asistencia para SNMP (pág. 49)".

El valor predeterminado: **Use la configuración en las configuración del Equipo.**

***Opción de seleccionar si se envía los sucesos de operaciones de copia de seguridad a los gestores SNMP:***

Elija una de las siguientes opciones:

- **Usar la configuración establecida en las opciones del Equipo:** use la configuración establecida para el equipo. Para obtener más información, consulte opciones de Equipo (pág. 91).
- **Envío individual de notificaciones SNMP para sucesos de operación de copia de seguridad**:envía los sucesos de las operaciones de copia de seguridad al gestor SNMP especificado.
  - **Tipos de sucesos a enviar**: seleccione los tipos de sucesos a enviar. **Todos los sucesos, errores y advertencias**, o **sólo errores**.
  - **Nombre del servidor/IP:** ingrese el nombre o dirección IP del servidor en donde se ejecuta la aplicación de gestión de SNMP y a donde se enviarán los mensajes.
  - **Comunidad**: ingrese el nombre de la comunidad SNMP al que pertenece tanto el servidor que ejecuta la aplicación de gestión de SNMP y el equipo emisor. La comunidad típica es "pública".

  Haga clic en **Enviar mensaje de prueba** para verificar si la configuración es correcta.
- **No enviar notificaciones de SNMP:** deshabilita el envío de sucesos de registro de las operaciones de copia de seguridad de los gestores SNMP.

## Copias de seguridad incrementales / diferenciales rápidas

Esta opción es eficaz tanto para los sistemas operativos Windows y Linux y los medios de inicio.

Esta opción es eficaz para las copias de seguridad incrementales y diferenciales a nivel de disco.

Esta opción define si se detecta el cambio de archivos por medio del tamaño de archivo y sellos de tiempo o la comparación del contenido de los archivos con aquellos guardados en el archivo comprimido.

El valor predeterminado: **Habilitado.**

La copia de seguridad incremental o diferencial sólo captura los cambios en los datos. Para acelerar el proceso de copia de seguridad, el programa determina si un archivo ha cambiado por su tamaño y la fecha/hora en la que se guardó por última vez. Si desactiva esta característica, el programa comparará el contenido completo del archivo con el que esté guardado en el archivo comprimido.

## División de copias de seguridad

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

Esta opción define como se divide la copia de seguridad.

El valor predeterminado: **Automático**

Las siguientes configuraciones están disponibles:

### Automático

Con esta configuración, Acronis Backup & Recovery 10 actuará de la siguiente manera.

- **Cuando se realiza una copia de seguridad en el disco duro:**

  Se creará un sólo archivo de copia de seguridad si el sistema de archivos del disco de destino permite el tamaño de archivo estimado.

  La copia de seguridad se dividirá automáticamente en varios archivos si el sistema de archivos del disco de destino no permite el tamaño estimado. Éste puede ser el caso cuando la copia de seguridad se ubica en sistemas de archivos FAT16 y FAT32 que tienen un límite de tamaño de archivo de 4 GB.

  Si el disco de destino se queda sin espacio libre mientras crea la copia de seguridad, la tarea ingresa en el estado **Necesita interacción**. Tiene la posibilidad de liberar espacio y reintentar la operación. Si lo hace, la copia de seguridad resultante se dividirá en las partes creadas antes y después del intento.
- **Cuando se realiza una copia de seguridad en un medio extraíble** (CD, DVD o dispositivo de cinta incluido a nivel local al equipo gestionado):

  La tarea ingresará en el estado **Necesita interacción** y le pedirá un disco nuevo cuando el anterior esté completo.

### Tamaño fijo

Ingrese el tamaño de archivo deseado o selecciónelo de la lista desplegable. La copia de seguridad entonces se dividirá en múltiples archivos del tamaño especificado. Esto resulta conveniente cuando se crea una copia de seguridad que planea grabar en múltiples CD, DVD o DVD+R/RW más adelante. Es posible que también desee dividir la copia de seguridad destinada a un servidor FTP, ya que la recuperación de datos directamente desde un servidor FTP requiere que los archivos se dividan en archivos no mayores a los 2GB.

## Seguridad de nivel de archivo

Estas opciones son sólo eficaces para las copias de seguridad en los sistemas operativos de Windows.

### En archivos comprimidos, almacenar archivos cifrados sin cifrar

Esta opción define si se descifran los archivos antes de guardarlos en el archivo de copia de seguridad.

El valor predeterminado: **Deshabilitado**.

Simplemente ignore esta opción si no utiliza la función de cifrado. Habilite la opción si hay archivos cifrados en la copia de seguridad y desea que cualquier usuario pueda acceder a ellos después de la recuperación. De lo contrario, sólo el usuario que cifró los archivos o las carpetas podrá leerlos. El descifrado también puede ser útil si va a recuperar archivos cifrados en otro equipo.

*El cifrado de archivos está disponible en Windows que usan el sistema de archivos NTFS con el Sistema de cifrado de archivos (EFS). Para acceder a la configuración de cifrado de archivos o carpetas* ***Propiedades > General > Atributos avanzados > Cifrar contenido para proteger datos.***

### Protección de la configuración de seguridad de documentos en archivos comprimidos

Esta opción define si realiza copia de seguridad de permisos para archivos NTFS junto a los archivos.

El valor predeterminado: **Habilitado.**

Cuando se habilita la opción, los archivos y carpetas se guardan en el archivo comprimido con los permisos originales de lectura, escritura, o ejecución de archivos por cada usuario o grupo de usuarios. Si restaura un archivo o carpeta protegidos en un equipo sin la cuenta de usuario especificada en los permisos, es posible que no pueda leer ni modificar este archivo.

Para evitar este tipo de problemas, puede deshabilitar la protección de la configuración de seguridad de archivos en los archivos comprimidos. Los archivos y carpetas recuperados siempre heredarán los permisos de la carpeta de la que se recupera o desde el disco, si se recupera a la raíz.

O bien, puede desactivar la recuperación (pág. 124) de la configuración de seguridad, incluso se están disponibles en el archivo comprimido. El resultado será el mismo: los archivos heredarán los permisos de la carpeta principal.

*Para tener acceso a los permisos NTFS de los archivos o carpetas, seleccione* ***Propiedades*** *>* ***Seguridad****.*

## Componentes de medios

Esta opción es eficaz tanto para sistemas operativos de Windows como de Linux, cuando la copia de seguridad es un medio extraíble.

Cuando realice una copia de seguridad a una medio extraíble, puede hacer que ese medio funcione como cualquier medio de inicio (pág. 410) basado en Linux al escribirle componentes adicionales. Como resultado, no necesitará un disco de rescate por separado.

El valor predeterminado: **Ninguno seleccionado.**

Seleccione las casillas de verificación para los componentes que quiera guardar en el medio de inicio:

- **Restauracion con un solo clic** es un componente adicional mínimo para su copia de seguridad del disco almacenada en medio extraíble, lo que permite una recuperación fácil desde la copia de seguridad. Si arranca un equipo desde el dispositivo y hace clic en **Ejecutar Acronis One-click Restore,** todos los datos se recuperarán sin intervención a su ubicación inicial.

  ***Precaución: Debido a que el enfoque de un solo clic no incluye selecciones por parte del usuario, como seleccionar particiones para restaurar,*** *Acronis One-Click Restore siempre recupera el disco entero. Si su disco tiene varios volúmenes y planea usar Acronis One-Click Restore, incluya todos los volúmenes de la copia de seguridad. Cualquier volumen que falte en la copia de seguridad se perderá.*

- El **agente de arranque** es una utilidad de rescate de arranque (basado en el kernel de Linux) que incluye la mayoría de las funcionalidades del agente de Acronis Backup & Recovery 10. Guarde este componente en el medio si quiere una mayor funcionalidad durante la recuperación. Entonces podrá configurar la operación de recuperación de la misma manera que bajo un medio de inicio; utilice Active Restore o Universal Restore. Si el dispositivo se está creando en Windows, la función de gestión de disco también estará disponible.

## Manejo de errores

Estas opciones son eficaces tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

Estas opciones le permiten que establezca como se manejarán los errores que puedan suceder durante la copia de seguridad.

### No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso)

El valor predeterminado: **Deshabilitado**.

Cuando se habilite el modo silencioso, el programa manejará automáticamente las situaciones que requieran interacción del usuario (a excepción del manejo de sectores defectuosos que se definen con otra opción). Si una operación no puede continuar sin la acción del usuario, ésta fallará. Los detalles de la operación, incluyendo los errores, si los hubiera, pueden encontrarse en el registro de la operación.

### Reintentar si se produce un error.

El valor predeterminado: **Habilitado**. **Cantidad de intentos: 5. Intervalo entre intentos: 30 segundos.**

Cuando se produce un error recuperable, el programa vuelve a intentar para realizar la operación fallida. Puede establecer el intervalo temporal y el número de intentos. Se detendrán los intentos tan pronto como la operación sea exitosa o se realice el número de intentos especificados, lo que suceda primero.

Por ejemplo, si no se tiene acceso o no está disponible el destino de la copia de seguridad en la red, el programa intentará llegar al destino cada 30 segundos, pero sólo 5 veces. Se detendrán los intentos tan pronto como se reanude la operación o se realice el número de intentos especificados, lo que suceda primero.

### Ignorar los sectores defectuosos

El valor predeterminado: **Deshabilitado**.

Cuando la opción está deshabilitada, el programa mostrará una ventana emergente cada vez que se encuentre con un sector defectuoso y le solicitará al usuario que decida si desea continuar o detener el procedimiento de copia de seguridad. Para realizar una copia de seguridad de información válida en un disco que se está dañando rápidamente, habilite ignorar sectores defectuosos Se realizará una copia de seguridad del resto de los datos y podrá montar la copia de seguridad del disco resultante y extraer los archivos válidos a otro disco.

## Doble destino

La opción es eficaz para los sistemas operativos de Windows y Linux, cuando el destino primario de la copia de seguridad es una *carpeta local o Acronis Secure Zone* y el destino secundario es *otra carpeta local o red compartida*. Las bóvedas gestionadas y servidores FTP no son compatibles como destinos secundarios.

El valor predeterminado: **Deshabilitado.**

Cuando está habilitado el destino doble, el agente copiará automáticamente cada copia de seguridad creada localmente al segundo lugar de destino como una red compartida. Una vez que se complete la copia de seguridad al primer lugar de destino, el agente compara el contenido del primer archivo comprimido actualizado con el contenido del segundo archivo comprimido y copia todas las copias de seguridad que faltan al segundo lugar de destino junto a la nueva copia de seguridad.

Esta opción permite una copia de seguridad rápida por equipo a la unidad interna como un paso intermedio antes de guardar la copia de seguridad lista en la red. Esto es práctico en caso de que la red esté lenta u ocupada y cuando existen procedimientos de copia de seguridad que requieren mucho tiempo. La desconexión durante la transferencia de la copia no afectará el procedimiento de copia de seguridad, como sucede al realizar copias de seguridad directamente desde la ubicación remota.

Otras ventajas:

- La replicación mejoran la confiabilidad del archivo comprimido.
- Los usuarios itinerantes pueden realizar copias de seguridad de sus equipos portátiles en Acronis Secure Zone mientras están en circulación. Mientras el equipo portátil esté conectado a la red corporativa, se transferirán todos los cambios en el archivo comprimido a la copia estática después de la primera operación de copia de seguridad.

*Si selecciona Acronis Secure Zone protegido con contraseña como destino primario, tenga en cuenta que el archivo comprimido en el destino secundario no está protegido con contraseña.*

***Para utilizar destino doble:***

1. Seleccione la casilla de verificación **Utilizar destino doble**.
2. Examinar el segundo lugar de destino o ingrese la ruta completa de destino manualmente.
3. Haga clic en **Aceptar**.

Puede ser que deba proporcionar las credenciales de acceso para el segundo lugar de destino. Ingrese las credenciales cuando se lo pida.

## Condiciones de inicio de la tarea

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción determina el comportamiento del programa si hay una tarea de copia de seguridad que está por iniciarse (el momento programado u ocurra el suceso especificado en el programa) pero no se cumple con la condición (o cualquiera de las condiciones). Para obtener más información sobre las condiciones, consulte Programación (pág. 173) y Condiciones (pág. 185).

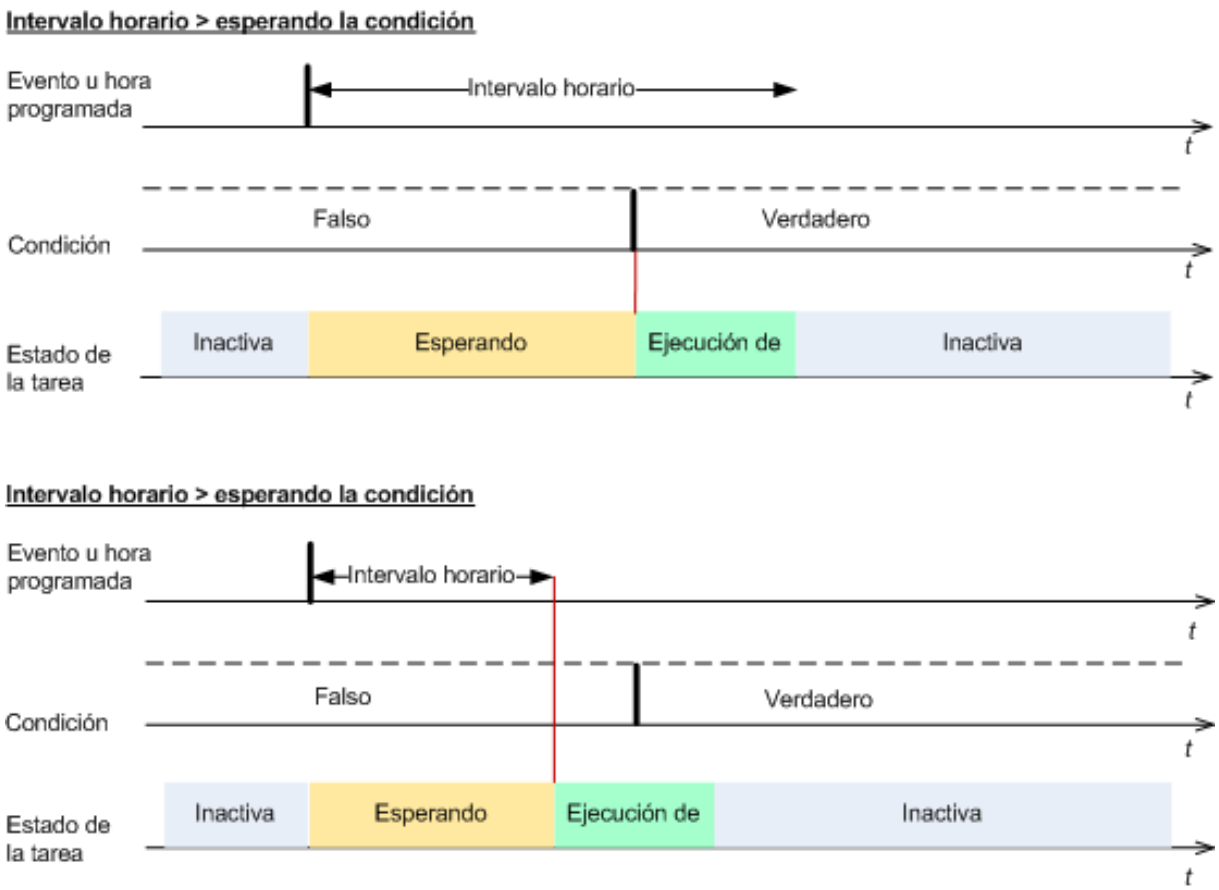
El valor predeterminado: **Esperar hasta que se cumplan las condiciones.**

### Esperar hasta que se cumplan las condiciones

Con esta configuración, el Programado comienza a supervisar las condiciones e inicia la tarea cuando se cumplen las condiciones. Si no se cumplen las condiciones, la tarea no comenzará nunca.

Para manejar la situación cuando no se cumplen con las condiciones por mucho tiempo y el retraso de la copia de seguridad se vuelve peligroso, puede definir el intervalo del cual la tarea se ejecutará independientemente de la condición. Seleccione la casilla de verificación **Ejecutar la tarea de todos modos después** y especifique el intervalo de tiempo. La tarea comenzará tan pronto como se cumpla con las condiciones o pase el período máximo de tiempo, lo que suceda primero.

**Diagrama temporal: Esperar hasta que se cumplan las condiciones**




### Omitir la ejecución de tarea

El retraso de una copia de seguridad puede ser inadmisible, por ejemplo, cuando necesite realizar una copia de seguridad estrictamente a la hora especificada. Entonces parece sensato omitir la copia de seguridad en vez de esperar a que se cumplan las condiciones, en especial si los sucesos son frecuentes.

## Manejo de fallos de la tarea

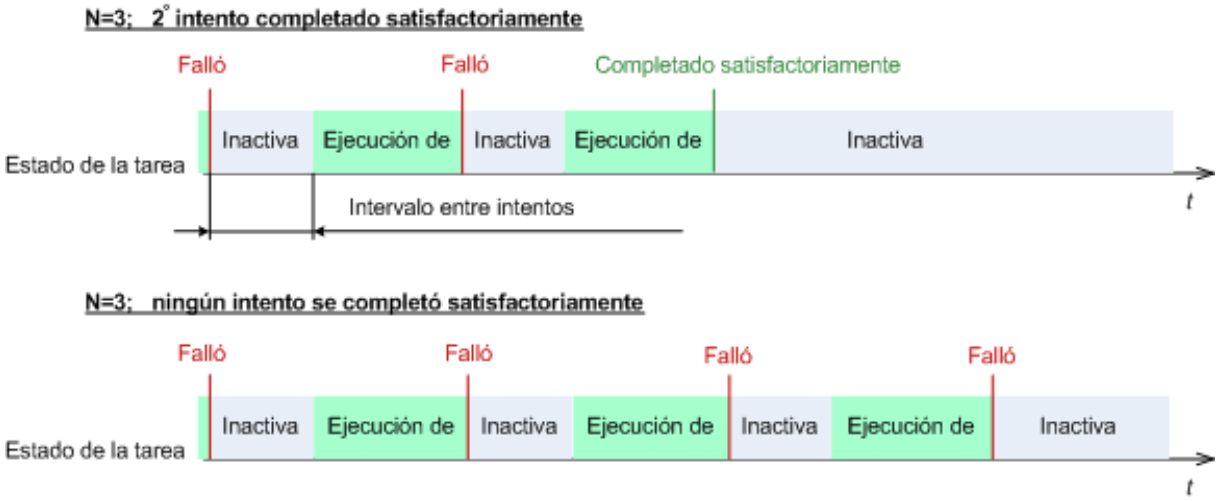
Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción determina el comportamiento del programa cuando fallan cualquiera de las tareas del plan de copia de seguridad.

El valor predeterminado es **no reiniciar una tarea que falló.**

Si selecciona la casilla de verificación **Reiniciar una tarea que falló** y especifica la cantidad de intentos y el intervalo de tiempo entre los mismos, el programa intentará ejecutar la tarea que falló nuevamente. El programa dejará de intentar tan pronto como un intento finalice correctamente o se haya realizado el número de intentos especificados, lo que suceda primero.




*Si falla la tarea por un error en el plan de copia de seguridad, puede editar el plan mientras la tarea esté inactiva. Mientras se ejecute la tarea, debe detenerla antes de editar el plan de copia de seguridad.*

## Soporte de cintas

Estas opciones son efectivas cuando el destino de la copia de seguridad es una bóveda gestionada ubicada en una biblioteca de cintas.

**Las opciones de Soporte para Cintas** le permiten especificar cómo las tareas de copias de seguridad distribuirán las copias de seguridad entre las cintas.

*Algunas combinaciones de las opciones de cintas pueden degradar la eficiencia en el uso de la biblioteca de cintas entera y de cada cinta. Si no se ve obligado a modificar estas opciones debido a necesidades específicas, no las cambie.*

Un archivo comprimido puede ocupar varias cintas. En tales casos se utiliza un llamado **conjunto de cintas** para conservar las copias de seguridad de datos.

Un **conjunto de cintas** es un grupo lógico de una o más cintas que contienen copias de seguridad de los datos específicos protegidos. Un conjunto de cintas también puede contener copias de seguridad de otros datos.

Un **conjunto de cintas separado** es un conjunto de cintas que contiene copias de seguridad de los datos específicos protegidos. Otras copias de seguridad no pueden escribirse en un conjunto de cintas separado.

### (Para la política o el plan de copias de seguridad a crear) Utilice un conjunto de cintas separado

El valor predeterminado: **Deshabilitado**.

Si no cambia esta opción, entonces las copias de seguridad, que pertenecen a la política o al plan que se está creando, pueden escribirse sobre cintas que contienen copias de seguridad escritos por diferentes políticas de copia de seguridad y que contienen datos de diferentes equipos. De la misma manera, las copias de seguridad de otras políticas pueden escribirse en cintas que contienen las

copias de seguridad de esta política. No tendrá problemas con dichas cintas, ya que el programa gestiona todas las cintas automáticamente.

Cuando está opción está habilitada, las copias de seguridad, que pertenecen a la política o al plan que se está creando, se ubicarán en un conjunto de cintas separado. Otras copias de seguridad no se escribirán en este conjunto de cintas.

### Si la consola está conectada al servidor de gestión

La opción **Utilizar un conjunto de cintas separado** tiene definiciones más precisas. Para crear una política de copias de seguridad puede utilizar un conjunto de cintas separado para todos los equipos o para cada equipo.

La opción **Un único conjunto de cintas para todos los equipos** está seleccionada de manera predeterminada. Generalmente, esta opción asegura un uso más eficiente de las cintas que la opción **Utilizar un conjunto de cintas separado para cada equipo**. Sin embargo, la segunda puede ser útil, por ejemplo, cuando existen requisitos especiales para almacenar las cintas con copias de seguridad desde un equipo específico externo.

Cuando la opción **Utilizar un conjunto de cintas separado** está habilitada, puede suceder que se tenga que escribir la copia de seguridad en una cinta que esté actualmente fuera del dispositivo de biblioteca de cintas. Qué hay que hacer en este caso.

- **Pedir la interacción del usuario**: la tarea de copia de seguridad entrará en el estado **Necesita interacción** y esperará a que se cargue la cinta, con la etiqueta requerida, al dispositivo de biblioteca de cintas.
- **Utilizar una cinta en blanco**: la copia de seguridad se escribirá en una cinta en blanco, por lo que la operación se detendrá sólo si no hay ninguna cinta en blanco en la biblioteca.

### Utilizar siempre una cinta en blanco

Si no cambia las opciones a continuación, entonces cada copia de seguridad se escribirá en una cinta especificada por la opción **Utilizar un conjunto de cintas separado**. Con algunas de las siguientes opciones habilitadas, el programa añadirá cintas nuevas al conjunto de cintas cada vez que se cree una copia de seguridad completa, incremental o diferencial.

- **Para cada copia de seguridad completa**

El valor predeterminado: **Deshabilitado**.

Cuando esta opción está habilitada, cada copia de seguridad completa se escribirá en una cinta en blanco. Se cargará la cinta a una unidad especialmente destinada para esta operación. Si la opción **Utilizar un conjunto de cintas separado** está habilitada, sólo las copias de seguridad incrementales y diferenciales de los datos se añadirán al final de la cinta.

- **Para cada copia de seguridad diferencial**

El valor predeterminado: **Deshabilitado**.

Cuando esta opción está habilitada, cada copia de seguridad diferencial se escribirá en una cinta en blanco. Esta opción está disponible sólo cuando se selecciona la opción de utilizar una cinta en blanco para cada copia de seguridad completa.

- **Para cada copia de seguridad incremental**

El valor predeterminado: **Deshabilitado**.

Cuando esta opción está habilitada, cada copia de seguridad incremental se escribirá en una cinta en blanco. Esta opción sólo está disponible cuando se selecciona la opción de utilizar una cinta en blanco para cada copia de seguridad completa y diferencial.

## Ajustes adicionales

Especifique los ajustes adicionales para la operación de copia de seguridad al seleccionar o desmarcar las siguientes casillas de verificación.

### Sobrescribir los datos en una cinta sin solicitar la confirmación del usuario

Esta opción es eficaz sólo cuando se realiza una copia de seguridad en un dispositivo de cinta.

El valor predeterminado: **Deshabilitado**.

Cuando se comienza una copia de seguridad a un dispositivo de cinta que no está vacía en un dispositivo de cinta incluido a nivel local, el programa alerta sobre que perderá los datos en la cinta. Para desactivar esta advertencia, marque la casilla de verificación.

### Desmontar dispositivos después de que la copia de seguridad haya finalizado

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción es eficaz cuando se realiza la copia de seguridad en un medio extraíble (CD, DVD, cinta o disquete.)

El valor predeterminado: **Deshabilitado.**

Se puede expulsar el CD/DVD de destino o se puede desmontar la cinta después de que se termine la copia de seguridad.

### Solicitar el primer medio al realizar la copia de seguridad en un medio extraíble.

Esta opción es eficaz sólo cuando se realiza una copia de seguridad en un medio extraíble.

La opción define si se muestra la solicitud de medio **Insertar el primer medio** cuando se realiza una copia de seguridad en un medio extraíble.

El valor predeterminado: **Habilitado**.

Cuando la opción está habilitada, quizá no se pueda realizar la copia de seguridad en un medio extraíble si el usuario no se encuentra en el equipo, ya que el programa esperará a que alguien pulse la opción Aceptar en el cuadro de aviso. Por lo tanto, debe deshabilitar el mensaje al programar una copia de seguridad en un medio extraíble. Por lo tanto, si el medio extraíble está disponible (por ejemplo, DVD introducido) la tarea puede ejecutarse sin supervisión.

### Restablecer el bit del archivo comprimido

Esta opción es eficaz solamente para copia de seguridad a nivel de archivo para sistemas operativos Windows y en medio de inicio.

El valor predeterminado: **Deshabilitado**.

En sistemas operativos Windows, cada archivo posee el atributo **Archivo listo para archivar** que está disponible al seleccionar **Archivo**->**Propiedades**- >**General**- >**Avanzado**- >**Atributos de archivos comprimidos e índices** El sistema operativo configura este atributo, también conocido como bit del archivo comprimido, cada vez que se modifica el archivo y puede restablecerse mediante las aplicaciones de copia de seguridad cada vez que se incluya un archivo en una copia de seguridad. Diversas aplicaciones utilizan el valor del bit del archivo comprimido, como por ejemplo, las bases de datos.

Cuando se selecciona la casilla de verificación **Reinicio del valor del bit del archivo comprimido,** Acronis Backup & Recovery 10 restablecerá los bits de archivos comprimidos de todos los archivos a los que se les realiza una copia de seguridad. Acronis Backup & Recovery 10 no usará el valor del bit de archivo comprimido. Cuando se realizan copias de seguridad incrementales o diferenciales, determina si se modificó el tamaño o la fecha y hora del archivo cuando se guardó por última vez.

### Reiniciar el equipo automáticamente después de que finalice la copia de seguridad

Esta opción sólo está disponible cuando se trabaja desde dispositivos de inicio.

El valor predeterminado: **Deshabilitado**.

Cuando la opción está habilitada, Acronis Backup & Recovery 10 reiniciará el equipo después de completar el proceso de copia de seguridad.

Por ejemplo, si el equipo inicia desde una unidad de disco duro predeterminada y puede seleccionar la casilla de verificación, el equipo se reiniciará y el sistema operativo comenzará tan pronto como el agente de inicio termine de crear la copia de seguridad.

### Deduplicar la copia de seguridad sólo después de transferirla a la bóveda (no deduplicar en el origen)

Esta opción está disponible solamente en las ediciones avanzadas de Acronis Backup & Recovery 10.

Esta opción es eficaz tanto para los sistemas operativos Windows como Linux y medios de inicio, cuando el destino de la copia de seguridad es una bóveda de desduplicación.

El valor predeterminado: **Deshabilitado**.

Al habilitar esta opción apaga la desduplicación de la copia de seguridad en el origen, lo que significa que Acronis Backup & Recovery 10 realizará la desduplicación de la copia. El Nodo de almacenamiento después de la copia de seguridad de la bóveda (se llama desduplicación en el destino).

La desactivación de la desduplicación en origen puede llevar a los procesos de copia de seguridad más rápidos pero mayor tráfico en la red y una carga más pesada del nodo de almacenamiento. El tamaño posible de la copia de seguridad en la bóveda es independiente de si está habilitada la desduplicación en el origen.

La desduplicación en el origen y en el destino se describen en Generalidades de Desduplicación (pág. 69).

### Guarde el RAID por software y los metadatos de la LVM junto con las copias de seguridad

Esta opción es eficaz sólo para las copias de seguridad a nivel de disco de equipos que ejecutan Linux.

El valor predeterminado: **Habilitado.**

Cuando esta opción esté habilitada, Acronis Backup & Recovery 10 guardará la información sobre la estructura de los volúmenes lógicos (conocidos como volúmenes LVM) y de los dispositivos RAID por software de Linux (conocidos como dispositivos MD), en el directorio **/etc/Acronis** antes de crear la copia de seguridad.

Al recuperar dispositivos MD y volúmenes LVM en el dispositivo de arranque, se puede utilizar esta información para recrear la estructura del volumen de forma automática. Para obtener instrucciones consulte Recuperación de dispositivos MD y volúmenes lógicos (pág. 288).

Cuando utilice esta opción, asegúrese de que el volumen que contiene el directorio **/etc/Acronis** esté entre los volúmenes de los que se va a realizar la copia de seguridad.

### Utilizar FTP en modo activo

El valor predeterminado: **Deshabilitado**.

Habilite esta opción si el servidor FTP es compatible con el modo activo y desea utilizar este modo en la transferencia de archivos.

## 3.4.2 Opciones predeterminadas de recuperación

Cada agente de Acronis tiene sus propias opciones predeterminadas de recuperación. Una vez instalado el agente, las opciones predeterminadas tienen valores predefinidos, que se consideran **preajustes** en la documentación. Cuando realiza una tarea de recuperación, puede utilizar una opción predeterminada o anular la opción predeterminada mediante el valor personalizado que se especificará únicamente para esta tarea.

También puede personalizar una opción predeterminada al cambiar su valor a otro diferente al predefinido. El nuevo valor se utilizará de manera predeterminada para todas las tareas de recuperación que realice en su equipo en adelante.

Para ver y cambiar las opciones de recuperación predeterminadas, conecte la consola al equipo gestionado y después seleccione **Opciones > Opciones predeterminadas de copia de seguridad y recuperación > Opciones predeterminadas de recuperación** en el menú superior.

### Disponibilidad de las opciones de recuperación

El conjunto de opciones de recuperación disponibles depende de:

- El entorno en el que opera el agente (Windows, dispositivo de inicio)
- El tipo de datos que se está copiando (disco, archivo)
- El sistema operativo que se está recuperando de la copia de seguridad del disco.

La siguiente tabla resume la disponibilidad de las opciones de recuperación.

| | **Agente para Windows** | | **Dispositivo de inicio (Basado en Linux o basado en PE)** | |
|---|---|---|---|---|
| | **Recuperación del disco** | **Recuperación de los archivos (también desde una copia de seguridad del disco)** | **Recuperación del disco** | **Recuperación de los archivos (también desde una copia de seguridad del disco)** |
| Comandos antes/después de la recuperación (pág. 122) | + | + | solo PE | solo PE |
| Prioridad de recuperación (pág. 124) | + | + | - | - |
| Seguridad a nivel de archivo (pág. 124)s: | | | | |
| Recuperar archivos con su configuración de seguridad | - | + | - | + |
| Manejo de errores (pág. 128): | | | | |

| | | | | |
|---|---|---|---|---|
| No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso) | + | + | + | + |
| Reintentar si se produce un error | + | + | + | + |
| Ajustes adicionales (pág. 128): | | | | |
| Configure la fecha y hora actual para los archivos recuperados | - | + | - | + |
| Validar el archivo comprimido de copia de seguridad antes de la recuperación | + | + | + | + |
| Verificar el sistema de archivos después de la recuperación | + | - | + | - |
| Reiniciar automáticamente el equipo si es necesario para la recuperación | + | + | - | - |
| Cambiar SID después de la recuperación | Recuperación de Windows | - | Recuperación de Windows | - |
| Notificaciones: | | | | |
| Correo electrónico (pág. 125) | + | + | - | - |
| Win Pop-up (pág. 126) | + | + | - | - |
| Rastreo de eventos: | | | | |
| Registro de eventos de Windows (pág. 126) | + | + | - | - |
| SNMP (pág. 127) | + | + | - | - |

## Comandos pre / post

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio basados en PE..

Esta opción le permite definir los comandos a ejecutar automáticamente antes y después del proceso de recuperación de datos.

Ejemplos de como se pueden usar los comandos pre/post:

- El uso del comando `Checkdisk` para encontrar y reparar los errores en el sistema de archivos en un volumen lógico, los errores físicos o sectores defectuosos se iniciará antes del comienzo de recuperación o después de la finalización de la recuperación.

El programa no admite comandos interactivos, es decir, comandos que requieran la intervención del usuario (por ejemplo, “pause”).

No se ejecutará un comando de recuperación posterior si la recuperación sucede como reinicio.

***Para especificar comandos pre/post***

1. Puede habilitar la ejecución de comandos pre/post al marcar las siguientes opciones:

- **Ejecutar antes de la recuperación**
- **Ejecutar después de la recuperación**

2. Realice uno de los siguientes:
   - Haga clic en **Editar** para especificar un nuevo comando o un archivo por lotes
   - Seleccione el comando existente o el archivo por lotes de la lista desplegable
3. Haga clic en **Aceptar**.

## Comandos antes de la recuperación

***Para especificar un comando o archivo por lotes para su ejecución antes de comenzar el proceso de copia de seguridad***

1. En el campo **Comando**, introduzca un comando o examine hasta encontrar un archivo por lotes. El programa no admite comandos interactivos, es decir, comandos que exijan la intervención del usuario (por ejemplo, “pause”).
2. En el campo **Directorio de trabajo**, especifique la ruta mediante la que se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
5. Haga clic en **Probar comando** para verificar si el comando es correcto.

| **Casilla de verificación** | **Selección** | | | |
|---|---|---|---|---|
| **Hacer que la tarea falle si falla la ejecución del comando** | Seleccionado | Borrado | Seleccionado | Borrado |
| **No recuperar hasta que finalice la ejecución de comandos** | Seleccionado | Seleccionado | Borrado | Borrado |
| **Resultado** | | | | |
| | **Valor predeterminado**<br>Realizar la recuperación solo después de que se ejecute el comando correctamente. Hacer que la tarea falle si falla la ejecución del comando | Realizar la recuperación después de que se ejecute el comando a pesar del éxito o fallo de la ejecución. | N/A | Realizar la recuperación al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando. |

## Comandos posteriores a la recuperación

***Para especificar un comando o archivo ejecutable después de completar la recuperación***

1. En el campo **Comando**, introduzca un comando o examine hasta encontrar un archivo por lotes.

2. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Si es crítico que la ejecución del comando sea satisfactoria para su estrategia de copia de seguridad, marque la casilla de verificación **Suspende la tarea si falla la ejecución del comando**. Si la ejecución del comando falla, el resultado de la ejecución de tarea será Error.

   Cuando no se marca la casilla de verificación, los resultados de la ejecución de comando no afectarán el éxito o fallo cuando se ejecute la tarea. Se puede seguir los resultados de la ejecución de comandos al explorar el registro de errores y advertencias que se muestran en el **Tablero**.
5. Haga clic en **Probar comando** para verificar si el comando es correcto.

*No se ejecutará un comando de recuperación posterior si la recuperación sucede como reinicio.*

## Prioridad de recuperación

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

La prioridad de un proceso que se ejecute en un sistema determina la cantidad de uso de la CPU y los recursos del sistema que se asignan a dicho proceso. La disminución de la prioridad de la recuperación liberará más recursos para otras aplicaciones. El aumento de la prioridad de la recuperación puede acelerar el proceso de recuperación al solicitar que el sistema operativo asigne más recursos por la aplicación que realizará la recuperación. Sin embargo, el efecto resultante dependerá del uso total del CPU y otros factores como velocidad de salida o entrada del disco o el tráfico en la red.

El valor predeterminado: **Normal.**

***Para especificar la prioridad del proceso de recuperación***

Seleccione una de las siguientes:

- **Bajo**: para minimizar el uso de recursos por parte del proceso de recuperación lo que dejará más recursos para otros procesos que se ejecuten en el equipo.
- **Normal**: ejecución del procesos de recuperación con la velocidad normal, lo que permite asignar recursos al mismo nivel de otros procesos.
- **Alto:** maximizará la velocidad del proceso de recuperación al tomar recursos de otros procesos.

## Seguridad de nivel de archivo

Esta opción sólo es eficaz para la recuperación desde archivos de Windows de copia de seguridad a nivel de archivo.

Esta opción define si realiza la recuperación de permisos para archivos NTFS junto a los archivos.

El valor predeterminado: **Recupera archivos con su configuración de seguridad**.

Si se preservan los permisos NTFS durante la copia de seguridad (pág. 112), puede elegir entre recuperar los permisos o permitir que los archivos hereden los permisos NTFS de la carpeta desde donde son recuperados.

## Notificaciones

Acronis Backup & Recovery 10 proporciona la capacidad de informar a los usuarios sobre la finalización de la recuperación por correo electrónico o servicio de mensajes.

### Correo electrónico

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

La opción le permite recibir notificaciones por correo electrónico sobre la finalización satisfactoria de la recuperación, fallo o necesidad de interacción con todo el registro de la tarea.

El valor predeterminado: **Deshabilitado**.

***Configurar notificación por correo electrónico***

1. Active la casilla de verificación **Enviar notificaciones por correo electrónico** para activar las notificaciones.
2. En el campo **Direcciones de correo electrónico**, escriba la dirección de correo electrónico a la que se enviarán las notificaciones. Puede introducir varias direcciones separadas por punto y coma.
3. Debajo de **Enviar notificaciones**, seleccione las casillas de verificación adecuadas como se indica a continuación:
   - **Cuando la copia de seguridad finaliza correctamente**: enviar una notificación cuando la copia de seguridad haya finalizado correctamente.
   - **Cuando la copia de seguridad falla**: enviar una notificación cuando la copia de seguridad falle.

   La casilla de verificación **Cuando la interacción del usuario sea necesaria** está activada.
4. Para que el mensaje de correo electrónico incluya las entradas del registro relacionadas con la copia de seguridad, active la casilla de verificación **Agregar registro completo a la notificación**.
5. Haga clic en **Parámetros adicionales de correo electrónico** para configurar parámetros adicionales de correo electrónico como se detalla a continuación y después haga clic en **Aceptar**:
   - **De**: escriba la dirección de correo electrónico del usuario emisor del mensaje. Si no completa este campo, los mensajes se crearán como si se enviaran desde la dirección de destino.
   - **Utilizar cifrado**: puede optar por una conexión cifrada al servidor de correo. Los tipos de cifrado SSL y TLS se encuentran disponibles para su elección.
   - Algunos proveedores de servicios de Internet exigen la autenticación del servidor de correo entrante antes de permitir enviar cualquier información. Si ese es su caso, active la casilla de verificación **Inicio de la sesión en el servidor de correo entrante** para habilitar el servidor POP y configurar sus ajustes:
     - **Servidor de correo entrante (POP)**: escriba el nombre del servidor POP.
     - **Puerto**: configure el puerto del servidor POP. De manera predeterminada, el puerto está configurado en 110.
     - **Nombre de usuario**: introduzca el nombre de usuario
     - **Contraseña**: introduzca la contraseña.
   - Active la casilla de verificación **Utilizar el servidor de correo saliente especificado** para habilitar un servidor SMTP y configurar sus ajustes:
     - **Servidor de correo saliente (SMTP)**: escriba el nombre del servidor SMTP.

- **Puerto:** configure el puerto del servidor SMTP. De manera predeterminada, el puerto se establece en 25.
- **Nombre de usuario**: introduzca el nombre de usuario
- **Contraseña**: introduzca la contraseña.

Haga clic en **Enviar mensaje de correo electrónico de prueba** para comprobar que los ajustes son correctos.

## Servicio de Messenger (WinPopup)

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

La opción le permite recibir notificaciones WinPopup sobre la finalización satisfactoria de la tarea de recuperación, fallo o necesidad de interacción.

El valor predeterminado: **Deshabilitado.**

Antes de configurar las notificaciones de WinPopup, asegúrese de que el servicio Messenger se encuentra activo tanto en el equipo que ejecuta la tarea como en el que recibirá los mensajes.

El servicio Messenger no se activa de manera predeterminada en la familia Microsoft Windows Server 2003. Cambie el servicio de Modo de inicio a Automático e inícielo.

***Para configurar las notificaciones de WinPopup:***

1. Active la casilla de verificación **Enviar notificaciones de WinPopup**.
2. En el campo **Nombre del equipo**, escriba el nombre del equipo al que se enviarán las notificaciones. No es posible introducir varios nombres.
3. Debajo de **Enviar notificaciones**, seleccione las casillas de verificación adecuadas como se indica a continuación:
   - **Cuando se realiza la recuperación satisfactoriamente**: envía una notificación cuando la tarea de recuperación se ha completado satisfactoriamente.
   - **Cuando falla la recuperación**: envía una notificación cuando no se realiza la tarea de recuperación.

   Casilla de verificación **Cuando se requiere interacción con el usuario**: envía una notificación durante la operación cuando se requiere de la interacción con el usuario, siempre seleccionada.
4. Haga clic en **Enviar mensaje de WinPopup de prueba** para verificar si la configuración es correcta.

### Seguimiento de sucesos

Es posible duplicar los sucesos de registro de operaciones de recuperación, realizada en el equipo gestionado, en el registro de sucesos de aplicación de Windows; o enviar los sucesos al gestor de SNMP especificado.

## Registro de sucesos de Windows

Esta opción sólo funciona en los sistemas operativos de Windows.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción define si el agente operativo en el equipo gestionado tiene que registrar los sucesos de operaciones de copias de seguridad en el registro en sucesos de aplicación de Windows (para ver

este registro, ejecute **eventvwr.exe** o seleccione **Panel de Control > Herramientas administrativas > Visor de sucesos**). Puede filtrar los sucesos a ser recopilados.

El valor predeterminado: **Use la configuración en las configuración del Equipo.**

***Seleccione si desea recopilar los sucesos de operaciones de recuperación en el Registro de sucesos de aplicación de Windows:***

Seleccione una de las siguientes:

- **Usar la configuración establecida en las opciones del Equipo:** use la configuración establecida para el equipo. Para obtener más información, consulte opciones de Equipo (pág. 91).
- **Registro de los siguientes tipos de eventos**: registro de sucesos de operaciones de recuperación en Registro de sucesos de aplicación. Especifique los tipos de sucesos a recopilar:
  - **Todos los eventos**: recopilación de los sucesos (información, advertencias y errores)
  - **Errores y advertencias**
  - **Sólo errores**
- **No recopilar**: desactiva el registro de sucesos de operaciones de copia de seguridad en el Registro de sucesos de aplicación.

## Notificaciones SNMP

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción define si el agente operativo en el equipo gestionado debe enviar los sucesos de registro de las operaciones de recuperación de seguridad a los gestores especificados de Protocolo Simple Network Management (SNMP). Puede elegir los tipos de sucesos a enviar.

Para obtener información detallada acerca de cómo utilizar SNMP con Acronis Backup & Recovery 10, vaya a "Asistencia para SNMP (pág. 49)".

El valor predeterminado: **Use la configuración en las configuración del Equipo.**

***Opción de seleccionar si se envía los sucesos de operaciones de recuperación a los gestores SNMP:***

Elija una de las siguientes opciones:

- **Usar la configuración establecida en las opciones del Equipo:** use la configuración establecida para el equipo. Para obtener más información, consulte opciones de Equipo (pág. 91).
- **Envío individual de notificaciones SNMP para sucesos de recuperación de copia de seguridad**:envía los sucesos de las operaciones de recuperación al gestor SNMP especificado.
  - **Tipos de sucesos a enviar**: seleccione los tipos de sucesos a enviar. **Todos los sucesos, errores y advertencias**, o **sólo errores**.
  - **Nombre del servidor/IP:** ingrese el nombre o dirección IP del servidor en donde se ejecuta la aplicación de gestión de SNMP y a donde se enviarán los mensajes.
  - **Comunidad**: ingrese el nombre de la comunidad SNMP al que pertenece tanto el servidor que ejecuta la aplicación de gestión de SNMP y el equipo emisor. La comunidad típica es "pública".

  Haga clic en **Enviar mensaje de prueba** para verificar si la configuración es correcta.

**No enviar notificaciones de SNMP:** deshabilita el envío de sucesos de registro de las operaciones de recuperación de los gestores SNMP.

## Manejo de errores

Estas opciones son eficaces tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

Estas opciones le permiten que establezca como se manejarán los errores que puedan suceder durante la recuperación.

### No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso)

El valor predeterminado: **Deshabilitado**.

Con el modo silencioso habilitado, el programa manejará automáticamente las situaciones que requieran de la interacción con el usuario cuando sea posible. Si una operación no puede continuar sin la acción del usuario, ésta fallará. Los detalles de la operación, incluyendo los errores, si los hubiera, pueden encontrarse en el registro de la operación.

### Reintentar si se produce un error.

El valor predeterminado: **Habilitado**. **Cantidad de intentos: 5. Intervalo entre intentos: 30 segundos.**

Cuando se produce un error recuperable, el programa vuelve a intentar para realizar la operación fallida. Puede establecer el intervalo temporal y el número de intentos. Se detendrán los intentos tan pronto como la operación sea exitosa o se realice el número de intentos especificados, lo que suceda primero.

Por ejemplo, si no se tiene acceso a la ubicación de la red o si no está disponible, el programa intentará llegar al destino cada 30 segundos, pero sólo 5 veces. Se detendrán los intentos tan pronto como se reanude la operación o se realice el número de intentos especificados, lo que suceda primero.

## Configuraciones adicionales

Especifique ajustes adicionales para la operación de recuperación al seleccionar o desmarcar las casillas de verificación.

### Configure la fecha y hora actual para los archivos recuperados

Esta opción es eficaz sólo con los archivos de recuperación.

El valor predeterminado está **Habilitado**.

Esta opción define si recupera la fecha y hora de los archivos comprimidos o asigna los archivos a la fecha y hora actual.

### Validar copia de seguridad antes de la recuperación

El valor predeterminado es **deshabilitado**.

Esta opción define si se valida la copia de seguridad para garantizar que no se corrompió la copia de seguridad, antes de recuperar los datos.

### Verificar sistema de archivos después de la recuperación

Esta opción es eficaz sólo cuando se recupera discos o volúmenes.

Cuando funciona desde un dispositivo de inicio, esta opción no es eficaz para el sistema de archivos NTFS.

El valor predeterminado es **deshabilitado**.

Esta opción define si se verifica la integridad del sistema de archivos después de la recuperación del volumen.

### Reinicio automático del equipo si es necesario para la recuperación

Esta opción es eficaz cuando se realiza la recuperación en un equipo que ejecuta un sistema operativo.

El valor predeterminado es **deshabilitado**.

La opción define si se reinicio automático del equipo si se los requiere para la recuperación. Éste puede ser el caso cuando se tiene que recuperar un volumen bloqueado por el sistema operativo.

### Reinicio del equipo después de la recuperación

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

El valor predeterminado es **deshabilitado**.

Esta opción permite que el equipo reinicie con el sistema operativo recuperado sin interacción con el usuario.

### Cambiar SID después de finalizar la recuperación

Esta opción no es efectiva cuando el Agente de Acronis Backup & Recovery 10 para ESX/ESXi o el Agente de Acronis Backup & Recovery 10 para Hyper-V realiza la recuperación a una máquina virtual.

El valor predeterminado es **deshabilitado**.

Acronis Backup & Recovery 10 puede generar un identificador de seguridad único (SID) para el sistema recuperado. No necesita un nuevo SID cuando recupera un sistema sobre sí o cuando crea una réplica del sistema para restaurar el sistema original. Genere un nuevo SID si el original y el sistema recuperado funcionarán al mismo tiempo en el mismo grupo de trabajo o dominio.

### Utilizar FTP en modo activo

El valor predeterminado: **Deshabilitado**.

Habilite esta opción si el servidor FTP es compatible con el modo activo y desea utilizar este modo en la transferencia de archivos.

# 4 Bóvedas

Una bóveda es una ubicación para almacenar archivos de copia de seguridad. Para facilitar el uso y la administración, una bóveda está asociada a los metadatos de los archivos comprimidos. La referencia a estos metadatos agiliza y facilita las operaciones con los archivos comprimidos y las copias de seguridad almacenados en la bóveda.

Una bóveda puede organizarse en una unidad local o de red, un medio extraíble o un dispositivo de cinta conectados a Acronis Backup & Recovery 10 Storage Node.

No hay configuración para limitar el tamaño de una bóveda o la cantidad de copias de seguridad de una bóveda. Puede limitar el tamaño de cada archivo comprimido con una limpieza, pero el tamaño total de los archivos comprimidos almacenados en la bóveda solo se limita por el tamaño de almacenamiento.

**¿Por qué crear bóvedas?**

Le recomendamos que cree una bóveda en cada uno de los destinos donde desee almacenar archivos de copia de seguridad. Esto facilitará su trabajo de la siguiente manera.

**Acceso rápido a la bóveda**

No tendrá que recordar las rutas a las carpetas donde están almacenados los archivos comprimidos. Al crear un plan de copia de seguridad o una tarea que requiere la selección de un archivo comprimido o el lugar de destino de un archivo comprimido, la lista de bóvedas estará disponible para su rápido acceso sin tener que desplazarse por el árbol de carpetas.

**Gestión sencilla de archivos comprimidos**

Es posible acceder a una bóveda desde el panel **Navegación**. Una vez que haya seleccionado la bóveda, podrá examinar los archivos comprimidos allí almacenados y realizar las siguientes operaciones de gestión de archivos comprimidos:

- obtener una lista de las copias de seguridad incluidas en cada archivo comprimido,
- recuperar datos desde una copia de seguridad,
- examinar el contenido de una copia de seguridad,
- validar todos los archivos comprimidos de la bóveda o archivos o copias de seguridad individuales,
- montar la copia de seguridad de un volumen para copiar archivos desde la copia de seguridad a un disco físico,
- eliminar de manera segura los archivos comprimidos y las copias de seguridad de los archivos comprimidos.

Es muy recomendable crear bóvedas, aunque esto no es obligatorio. Puede optar por no usar los accesos directos y especificar siempre la ruta completa a la bóveda de los archivos comprimidos. Todas las operaciones anteriores, excepto la eliminación de archivos comprimidos y copias de seguridad, pueden realizarse sin crear bóvedas.

Como resultado de la operación de crear una bóveda, se añade el nombre de la bóveda a la sección **Bóvedas** del panel **Navegación**.

### Bóvedas centralizadas y personales

Una bóveda centralizada es una ubicación de red asignada por el administrador del servidor de gestión para que funcione como almacenamiento de los archivos de copia de seguridad. La bóveda centralizada puede ser gestionada por un nodo de almacenamiento (bóveda gestionada) o permanecer sin gestionar.

Una bóveda se denomina personal si fue creada usando una conexión directa entre la consola y un equipo gestionado. Las bóvedas personales son específicas para cada equipo gestionado.

### Formas de trabajar con la vista "Bóvedas"

**Bóvedas** (en el panel de navegación): elemento principal del árbol de bóvedas. Haga clic en este elemento para mostrar los grupos de bóvedas centralizadas y personales.

**Centralizadas**. Este grupo está disponible cuando la consola está conectada a un equipo gestionado o a un servidor de gestión. Expanda este grupo para mostrar una lista de las bóvedas centralizadas añadidas por el administrador del servidor de gestión.

Haga clic en cualquier bóveda centralizada del árbol de bóvedas para abrir la vista detallada de esta bóveda (pág. 132) y para realizar acciones en la bóveda (pág. 133), los archivos comprimidos (pág. 169) y las copias de seguridad (pág. 169) allí almacenados.

**Personales**. Este grupo está disponible cuando la consola está conectada a un equipo gestionado. Expanda este grupo para mostrar una lista de las bóvedas personales creadas en el equipo gestionado.

Haga clic en cualquier bóveda personal del árbol de bóvedas para abrir la vista detallada de esta bóveda (pág. 166) y realizar acciones en la bóveda (pág. 167), los archivos comprimidos (pág. 169) y las copias de seguridad (pág. 169) allí almacenados.

## 4.1 Bóvedas centralizadas

Una bóveda centralizada es una ubicación de red asignada por el administrador del servidor de gestión para que funcione como almacenamiento de los archivos de copia de seguridad. Una bóveda centralizada puede ser gestionada por un nodo de almacenamiento o permanecer sin gestionar. El tamaño y la cantidad total de archivos comprimidos almacenados en una bóveda centralizada están limitados solamente por el tamaño de almacenamiento.

Cuando el administrador del servidor de gestión ejecuta la creación de una bóveda centralizada, la ruta y el nombre de la bóveda se distribuyen a todos los equipos registrados en el servidor. El acceso directo a la bóveda aparece en los equipos del grupo **Bóvedas > Centralizadas**. Cualquier plan de copia de seguridad existente en los equipos, incluidos los planes locales, puede usar la bóveda centralizada.

En un equipo que no está registrado en el servidor de gestión, un usuario que tiene privilegios para realizar copias de seguridad en la bóveda centralizada puede realizar las copias al especificar la ruta completa a la bóveda. Si la bóveda es gestionada, los archivos comprimidos del usuario y otros archivos comprimidos almacenados en la bóveda serán gestionados por el nodo de almacenamiento.

### Bóvedas gestionadas

Una bóveda gestionada es una bóveda centralizada gestionada por un nodo de almacenamiento.

El nodo de almacenamiento lleva a cabo la limpieza (pág. 409) y la validación (pág. 414) para cada archivo comprimido almacenado en la bóveda gestionada, según se describe en los planes de copias de seguridad (pág. 411). Al crear una bóveda gestionada, un administrador puede especificar las

operaciones adicionales que el nodo de almacenamiento realizará : deduplicación y cifrado. Para obtener más información, consulte "Operaciones realizadas por los nodos de almacenamiento".

Cualquier bóveda gestionada es autónoma, es decir, contiene todos los metadatos que el nodo de almacenamiento necesita para la gestión de la bóveda. Una bóveda puede conectarse a otro nodo de almacenamiento. El nuevo nodo de almacenamiento recuperará los metadatos de la bóveda y recreará la base de datos que es necesaria para gestionar la bóveda. Para obtener más información, consulte "Conexión de una bóveda gestionada" (pág. 138).

**Acceso a bóvedas gestionadas**

Los usuarios deben tener privilegios de administrador o usuario para acceder a la bóveda. Los administradores del servidor de gestión obtienen los privilegios de administrador de manera predeterminada. Los privilegios para los demás usuarios pueden definirse durante la creación o edición de la bóveda. Para obtener más información, consulte "Privilegios de usuario en un nodo de almacenamiento" (pág. 76).

### Bóvedas sin gestionar

Una bóveda sin gestionar es una bóveda centralizada que no está gestionada por un nodo de almacenamiento. Para acceder a una bóveda sin gestionar, el usuario debe tener privilegios de acceso para la ubicación desde la red.

Cualquier usuario que tenga permiso para leer/grabar archivos en una bóveda sin gestionar podrá:

- realizar copias de seguridad de datos en la bóveda sin gestionar,
- recuperar datos de cualquier copia de seguridad ubicada en la bóveda sin gestionar,
- ver y gestionar todos los archivos comprimidos ubicados en la bóveda sin gestionar.

## 4.1.1 Cómo trabajar con la vista "Bóveda centralizada"

Esta sección describe brevemente los principales elementos de la vista **Bóveda centralizada** y sugiere formas de trabajar con ellos.

### Barra de herramientas de la bóveda

La barra de herramientas contiene botones operacionales que le permiten realizar operaciones con la bóveda centralizada seleccionada. Consulte la sección Acciones en bóvedas centralizadas (pág. 133) para obtener más información.

### Gráfico circular con leyenda

El **gráfico circular** le permite estimar la carga de la bóveda: muestra la proporción entre el espacio libre y el espacio ocupado de la bóveda. El gráfico circular no está disponible si la bóveda está ubicada en una biblioteca de cintas.

- espacio libre: espacio en el dispositivo de almacenamiento donde está ubicada la bóveda. Por ejemplo, si la bóveda está ubicada en un disco duro, el espacio libre de la bóveda es el espacio libre del volumen correspondiente.

- espacio ocupado: el tamaño total de los archivos de copia de seguridad y sus metadatos, si están ubicados en la bóveda.

La **leyenda** muestra la siguiente información sobre la bóveda:

- [únicamente para bóvedas gestionadas] el nombre del nodo de almacenamiento que gestiona la bóveda,
- ruta completa a la bóveda,
- cantidad total de archivos comprimidos y copias de seguridad almacenados en la bóveda,
- proporción entre el espacio ocupado y el tamaño de los datos originales,
- [únicamente para bóvedas gestionadas] estado de deduplicación (pág. 69) (Activado, Desactivado),
- [únicamente para bóvedas gestionadas] estado de cifrado (Sí, No).

### Contenido de la bóveda

La sección **Contenido de la bóveda** contiene la tabla y la barra de herramientas de archivos comprimidos. La tabla de archivos comprimidos muestra los archivos comprimidos y las copias de seguridad almacenados en la bóveda. Utilice la barra de herramientas de archivos comprimidos para realizar acciones en los archivos comprimidos y copias de seguridad seleccionados. La lista de copias de seguridad se expande al hacer clic en el signo "más" ubicado a la izquierda del nombre del archivo comprimido. Todos los archivos comprimidos están agrupados por tipo en las siguientes pestañas:

- La pestaña **Archivos comprimidos del disco** enumera todos los archivos comprimidos que contienen copias de seguridad del disco o volumen (imágenes).
- La pestaña **Archivos comprimidos de archivos** enumera todos los archivos comprimidos que contienen copias de seguridad de archivos.

**Secciones relacionadas:**

Operaciones con archivos comprimidos almacenados en una bóveda (pág. 169)

Operaciones con copias de seguridad (pág. 169)

Filtrado y ordenamiento de archivos comprimidos (pág. 171)

### Barras del panel "Acciones y herramientas"

- **[Nombre de la bóveda]** La barra **Acciones** está disponible al hacer clic en la bóveda en el árbol de bóvedas. Duplica las acciones de la barra de herramientas de la bóveda.
- **[Nombre del archivo comprimido]** La barra **Acciones** está disponible al seleccionar un archivo comprimido en la tabla de archivos comprimidos. Duplica las acciones de la barra de herramientas de archivos comprimidos.
- **[Nombre de la copia de seguridad]** La barra **Acciones** está disponible al expandir el archivo comprimido y hacer clic en cualquiera de sus copias de seguridad. Duplica las acciones de la barra de herramientas de archivos comprimidos.

## 4.1.2 Acciones en bóvedas centralizadas

Todas las operaciones descritas aquí se realizan al hacer clic en los botones correspondientes de la barra de herramientas de las bóvedas. También es posible acceder a estas operaciones desde la barra **Acciones de [nombre de la bóveda]** (en el panel **Acciones y herramientas**) y desde el elemento **Acciones de [nombre de la bóveda]** del menú principal.

La siguiente es una guía para realizar operaciones con bóvedas centralizadas.

| Operación | Procedimiento |
|---|---|
| Crear una bóveda gestionada o sin gestionar | 1. Haga clic en **Crear**.<br>2. En el campo **Tipo**, seleccione el tipo de bóveda: **Gestionada** o **Sin gestionar**<br>El procedimiento de creación de bóvedas centralizadas se describe en profundidad en las siguientes secciones:<br>▪ Crear una bóveda centralizada gestionada (pág. 135)<br>▪ Crear una bóveda centralizada sin gestionar (pág. 138) |
| Editar una bóveda gestionada o sin gestionar | 1. Seleccione la bóveda.<br>2. Haga clic en **Editar**.<br>Según la bóveda que seleccione (gestionada o sin gestionar), se abrirá la página Editar respectiva:<br>▪ La página **Editar bóveda gestionada** le permite cambiar el nombre de la bóveda (si está cifrada) y la información del campo **Comentarios**.<br>▪ La página **Edición de bóveda sin gestionar** permite editar el nombre de la bóveda y la información del campo **Comentarios**. |
| Validar una bóveda | 1. Seleccione la bóveda.<br>2. Haga clic en **Validar**.<br>Pasará a la página Validación (pág. 255) con una bóveda ya preseleccionada como origen. La validación de la bóveda verifica todos los archivos comprimidos de esta bóveda. |
| Eliminar una bóveda | 1. Seleccione la bóveda.<br>2. Haga clic en **Eliminar**.<br>Se le preguntará si desea conservar los archivos comprimidos almacenados en la bóveda o eliminar la bóveda junto con todos los archivos comprimidos. Los planes y las tareas que utilizan esta bóveda fallarán.<br>Si opta por mantener los archivos comprimidos de una bóveda gestionada, la bóveda se desconectará del nodo de almacenamiento. Posteriormente, podrá conectar esta bóveda al mismo u otro nodo de almacenamiento. |
| Explorar una bóveda sin gestionar | 1. Seleccione la bóveda sin gestionar.<br>2. Haga clic en **Explorar**.<br>La bóveda se podrá examinar con el programa estándar administrador de archivos. |
| Conectar la bóveda gestionada que se eliminó sin quitar su contenido | Haga clic en **Conectar**.<br>El procedimiento de conexión de una bóveda gestionada a un nodo de almacenamiento se describe en profundidad en la sección Conexión de una bóveda gestionada (pág. 138). |
| Cambiar las credenciales del usuario | Haga clic en **Cambiar usuario**. |

| | |
|---|---|
| para acceder a una bóveda | El cambio de credenciales del usuario está disponible únicamente para las bóvedas que residen en almacenamientos compartidos. |
| Actualizar la información de una bóveda | Haga clic en **Actualizar**.<br>Mientras revisa el contenido de la bóveda, pueden añadirse archivos comprimidos a la bóveda, como también eliminarse o modificarse. Haga clic en **Actualizar** para actualizar la información de la bóveda con los cambios más recientes. |
| **Acciones en una biblioteca de cintas de una bóveda gestionada** | |
| Definir las etiquetas de cintas y realizar un inventario de una biblioteca de cintas en una bóveda gestionada | Haga clic en **Gestionar cintas**.<br>En la ventana **Gestión de cintas**, defina las etiquetas para las cintas y actualice el inventario. Para obtener más información, consulte la sección Gestión de biblioteca de cintas (pág. 145). |
| Volver a explorar las cintas de una bóveda gestionada | Haga clic en **Volver a explorar cintas**.<br>La función "Volver a explorar" lee información sobre el contenido de las cintas seleccionadas por el usuario y actualiza la base de datos del nodo de almacenamiento.<br>Esta operación se describe en profundidad en la sección Volver a explorar (pág. 146). |

## Creación de una bóveda centralizada gestionada

***Para crear una bóveda centralizada gestionada, realice los siguientes pasos***

### Vault

**Nombre**

Especifique un nombre único para la bóveda. Está prohibida la creación de dos bóvedas centralizadas con el mismo nombre.

**Comentarios**

[Opcional] Introduzca la descripción distintiva de la bóveda que está creando.

**Tipo**

Seleccione el tipo **Gestionada**.

**Nodo de almacenamiento**

Seleccione el nodo de almacenamiento de Acronis Backup & Recovery 10 que gestionará la bóveda. Es posible que tenga que introducir credenciales de acceso para el nodo de almacenamiento.

**Ruta** (pág. 136)

Especifique el lugar donde se creará la bóveda. Las bóvedas centralizadas gestionadas pueden residir en una red compartida, SAN, NAS o en una unidad de disco duro local al nodo de almacenamiento.

**Ruta de la base de datos** (pág. 136)

Especifique una carpeta local en el servidor de almacenamiento para crear una base de datos específica de la bóveda. Esta base de datos almacenará los metadatos necesarios para catalogar los archivos comprimidos y realizar la deduplicación.

**Deduplicación**

[Opcional] Seleccione si desea habilitar la desduplicación de archivos comprimidos en la bóveda. La desduplicación minimiza el espacio de almacenamiento que ocupan los archivos

comprimidos y el tráfico de copias de seguridad. Reduce el tamaño de los archivos comprimidos de la bóveda al eliminar los datos redundantes, como los archivos duplicados o los bloques de discos.

La desduplicación no es posible en los dispositivos de cinta.

Para obtener más información sobre el funcionamiento de la desduplicación, consulte la sección Desduplicación (pág. 69).

**Compresión**

[Opcional] Seleccione si comprime o no las memorias de datos de la duplicación. Esta configuración está disponible solo si se habilita la desduplicación.

**Cifrado** (pág. 137)

[Opcional] Seleccione si desea proteger la bóveda con cifrado. Todo lo que se guarda en la bóveda se cifra y el nodo de almacenamiento descifra de modo claro todo lo que se lee por medio de una clave de cifrado específica de la bóveda almacenada en el nodo de almacenamiento.

Una vez que haya realizado todos los pasos obligatorios, haga clic en **Aceptar** para ejecutar la creación de la bóveda gestionada.

## Ruta de la bóveda

***Para especificar la ruta en la que se creará la bóveda gestionada***

1. Introduzca la ruta completa a la carpeta en el campo **Ruta** o seleccione la carpeta deseada en el árbol de carpetas. Las bóvedas gestionadas pueden organizarse:
   - en unidades del disco duro locales al nodo de almacenamiento
   - en una red compartida
   - en una Red de área de almacenamiento (SAN)
   - en un Almacenamiento conectado a la red (NAS)
   - en una biblioteca de cintas conectada de forma local al nodo de almacenamiento.

   Para crear una carpeta nueva para la bóveda en la ubicación seleccionada, haga clic en **Crear carpeta**.
2. Haga clic en **Aceptar**.

---

*Una bóveda puede crearse únicamente en una carpeta vacía.*

*No recomendamos crear una bóveda gestionada de* deduplicación *en un volumen FAT32, ya que una bóveda de este tipo almacena todos los elementos deduplicados en dos archivos potencialmente muy largos. Como el tamaño máximo de archivos en un sistema de archivos FAT está limitado a 4 GB, el nodo de almacenamiento puede detener su funcionamiento cuando se llegue a este límite.*

*Los permisos de la carpeta deberán permitir la cuenta de usuario bajo la cual el servicio de nodo de almacenamiento se ejecuta (predeterminada como **Usuario ASN**) para escribir a la carpeta. Cuando se asignan los permisos, especifique la cuenta de usuario de manera explícita (no simplemente **Todos**).*

---

## Ruta de la base de datos de la bóveda

***Para especificar la ruta en la que se creará la base de datos de la bóveda***

1. En las **Carpetas locales** del nodo de almacenamiento, seleccione la carpeta deseada o introduzca la ruta completa a la carpeta en el campo **Ruta**.

   Para crear una carpeta nueva para la base de datos, haga clic en **Crear carpeta**.

2. Haga clic en **Aceptar**.

Cuando elija una carpeta para la base de datos de la bóveda, tenga en cuenta las siguientes indicaciones:

- La carpeta deberá residir en una unidad fija. No intente colocar la base de datos en unidades extraíbles externas.
- El tamaño de la carpeta puede ser demasiado grande —se estima en 200 GB cada 8 TB de espacio utilizado, o alrededor del 2,5 por ciento.
- Los permisos de la carpeta deben permitir la cuenta de usuario bajo la cual el servicio del nodo de almacenamiento se ejecuta (por defecto, **usuario ASN**) para escribir a la carpeta. Cuando asigne permisos, especifique la cuenta de usuario explícitamente (no simplemente **Todas**).

## Cifrado de la bóveda

Si protege una bóveda con cifrado, todo lo que se guarda en la bóveda se cifra y el nodo de almacenamiento descifra de modo claro todo lo que se lee por medio de una clave de cifrado específica de la bóveda almacenada en el nodo. En caso de robo o acceso no autorizado al medio de almacenamiento, la persona no autorizada no podrá descifrar el contenido de la bóveda si no tiene acceso al nodo de almacenamiento.

Este cifrado no tiene relación alguna con el cifrado de archivos comprimidos especificado por el plan de copia de seguridad y realizado por un agente. Si el archivo comprimido ya está cifrado, el cifrado del lado del nodo de almacenamiento se aplica sobre el cifrado realizado por el agente.

***Para proteger la bóveda con cifrado***

1. Seleccione la casilla de verificación **Cifrar**.
2. En el campo **Introducir contraseña,** escriba la contraseña.
3. En el campo **Confirmar contraseña**, vuelva a escribir la contraseña.
4. Seleccione una de las siguientes opciones:
   - **AES 128:** se cifrará el contenido de la bóveda por medio del algoritmo estándar avanzado de cifrado (AES) con una clave de 128 bits.
   - **AES 192:** se cifrará el contenido de la bóveda por medio del algoritmo AES con una clave de 192 bits.
   - **AES 256:** se cifrará el contenido de la bóveda por medio del algoritmo AES con una clave de 256 bits.
5. Haga clic en **Aceptar**.

El algoritmo de cifrado AES funciona en el modo Cipher-block chaining (CBC) y utiliza una clave generada de manera aleatoria con un tamaño definido por el usuario de 128, 192 ó 256 bits. Cuanto más grande sea el tamaño de la clave, más tiempo tardará el programa en cifrar los archivos comprimidos almacenados en la bóveda y más seguros estarán los archivos comprimidos.

Luego, la clave de cifrado se cifra con AES-256 usando un hash SHA-256 de la contraseña como clave. La contraseña no se almacena en ninguna parte del disco; el hash de la contraseña se usa para verificación. Con esta seguridad de dos niveles, los archivos comprimidos están protegidos de cualquier acceso no autorizado, pero no es posible la recuperación de una contraseña perdida.

## Creación de una bóveda centralizada sin gestionar

***Para crear una bóveda centralizada sin gestionar, realice los siguientes pasos.***

**Bóveda**

**Nombre**

Especifique un nombre único para la bóveda. Está prohibida la creación de dos bóvedas centralizadas con el mismo nombre.

**Comentarios**

Introduzca la descripción distintiva de la bóveda.

**Tipo**

Seleccione el tipo **Sin gestionar**.

**Ruta** (pág. 138)

Especifique el lugar donde se creará la bóveda.

Una vez que haya realizado todos los pasos obligatorios, haga clic en **Aceptar** para ejecutar la creación de la bóveda centralizada sin gestionar.

## Ruta de la bóveda

***Para especificar la ruta en la que se creará la bóveda sin gestionar***

1. Introduzca la ruta completa a la carpeta en el campo Ruta o seleccione la carpeta deseada en el árbol de carpetas. Las bóvedas sin gestionar pueden organizarse:
   - Acronis Online Backup Storage
   - en una red compartida
   - en una Red de área de almacenamiento (SAN)
   - en un Almacenamiento conectado a la red (NAS)
   - en servidores FTP y SFTP.

   *Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

   Para crear una carpeta nueva para la bóveda, haga clic en Crear carpeta.

   *Una bóveda puede crearse únicamente en una carpeta vacía.*
2. Haga clic en Aceptar.

## Conexión de una bóveda gestionada

Una bóveda gestionada por un nodo de almacenamiento puede conectarse a otro nodo de almacenamiento. Esto puede ser necesario al retirar el hardware de un nodo de almacenamiento, cuando el nodo de almacenamiento se pierde o al equilibrar cargas entre nodos de almacenamiento. Como resultado, el primer nodo interrumpe la gestión de la bóveda. El segundo nodo explora los archivos comprimidos de la bóveda, crea y completa la base de datos correspondiente a la bóveda, e inicia la gestión de la bóveda.

Al eliminar una bóveda gestionada, tiene la opción de retener los archivos comprimidos incluidos en la bóveda. La ubicación resultante de dicha eliminación también puede conectarse al mismo nodo de almacenamiento u otro.

*Las bóvedas personales o centralizadas sin gestionar no pueden conectarse.*

***Para conectar una bóveda gestionada a un nodo de almacenamiento, realice los siguientes pasos.***

**Bóveda**

**Nodo de almacenamiento**

Seleccione el nodo de almacenamiento de Acronis Backup & Recovery 10 que gestionará la bóveda.

**Ruta**

Especifique la ruta a la ubicación donde están almacenados los archivos comprimidos.

**Ruta de la base de datos**

Especifique una carpeta local en el servidor de almacenamiento para crear una base de datos específica de la bóveda. Esta base de datos almacenará los metadatos necesarios para catalogar los archivos comprimidos y realizar la deduplicación.

**Contraseña**

Para la bóveda cifrada, proporcione la contraseña de cifrado.

Una vez que haya realizado todos los pasos obligatorios, haga clic en **Aceptar** para ejecutar la conexión de la bóveda. Este procedimiento puede durar bastante tiempo dado que el nodo de almacenamiento tiene que explorar los archivos comprimidos, escribir los metadatos en la base de datos y deduplicar los archivos comprimidos si originalmente la bóveda deduplicaba.

## 4.1.3 Bibliotecas de cintas

Esta sección describe en detalle cómo utilizar dispositivos de cintas robóticos como bóvedas para almacenar archivos comprimidos de copias de seguridad.

Una biblioteca de cintas (biblioteca robotizada) es un dispositivo de alta capacidad de almacenamiento que contiene:

- una o más unidades de cinta
- múltiples (hasta varios miles) ranuras para sujetar cartuchos de cinta
- uno o más cargadores (mecanismos robotizados) con la función de reubicar los cartuchos de cinta entre las ranuras y las unidades de cinta
- lectores de códigos de barras (opcional).

### Generalidades

Acronis Backup & Recovery 10 proporciona una compatibilidad completa para una biblioteca de cintas a través del Acronis Backup & Recovery 10 Storage Node. El nodo de almacenamiento debe instalarse en el equipo al que la biblioteca está conectada. El nodo de almacenamiento puede utilizar simultáneamente más de una biblioteca de cintas para conservar archivos comprimidos.

Para gestionar un dispositivo de biblioteca de cintas, el nodo de almacenamiento utiliza el Removable Storage Manager (RSM) de Windows. Consulte la sección Grupos de dispositivos RSM (pág. 141) para obtener más información.

Una base de datos dedicada del nodo de almacenamiento conserva la información del contenido de la copia de seguridad escrita en las cintas. Así, algunas operaciones (por ejemplo, Limpieza (pág. 408)) pueden realizarse con bastante rapidez sin acceder al dispositivo. Es posible ver el contenido de un archivo comprimido de copia de seguridad de datos ubicado en una cinta a través de la consola, incluso si la biblioteca de cintas está apagada, debido a la información de contenido almacenada en la base de datos. Para crear una copia de seguridad de datos diferencial o incremental, el programa

utiliza la base de datos en lugar de cargar, montar, rebobinar y leer una cinta sin la copia de seguridad completa. Sin embargo, se debe leer una cinta, por ejemplo, para validar (pág. 414) una copia de seguridad o para recuperar datos desde una copia de seguridad.

Una biblioteca de cintas puede conectarse localmente a un equipo en el que está instalado el agente, pero sólo en el caso de que la biblioteca se considera una única unidad de cinta. El agente puede utilizar dicho dispositivo para escribir y leer copias de seguridad de datos, pero el formato de la copia de seguridad es diferente al formato de las copias de seguridad en las cintas escritas a través de un nodo de almacenamiento. Para conseguir información sobre la legibilidad de los archivos comprimidos en las cintas, escritos por diferentes componentes de otras versiones de los productos por medio de Acronis Backup & Recovery 10, consulte la sección Tabla Compatibilidad de cintas (pág. 47).

Acronis Backup & Recovery 10 le permite establecer la distribución de las copias de seguridad por dispositivo. Por ejemplo, se puede utilizar un conjunto de cintas separado para realizar copias de seguridad de algunos datos específicos y las copias de seguridad de todos los otros datos serán escritas sobre cualquier cinta montada en el momento, que no pertenezca al conjunto de cintas. Vea la sección Soporte para cinta (pág. 117)s en búsqueda de más información.

Los esquemas de copia de seguridad (Abuelo-Padre-Hijo (pág. 35), Torres de Hanói (pág. 39)) le asisten considerablemente mediante la creación de unas reglas de retención y una programación efectivas para las copias de seguridad en una biblioteca de cintas. Combinados con las opciones de cinta, los esquemas de copia de seguridad le permiten volver a utilizar, en modo automático, las cintas que se consideran en blanco después de la eliminación de la copia de seguridad. Consulte la sección Rotación de cintas (pág. 149) para obtener más información.

## Hardware

Una biblioteca de cintas (biblioteca robotizada) es un dispositivo de alta capacidad de almacenamiento que contiene:

- una o más unidades de cinta
- múltiples (hasta varios miles) ranuras para sujetar cartuchos de cinta
- uno o más cargadores (mecanismos robotizados) con la función de reubicar los cartuchos de cinta entre las ranuras y las unidades de cinta
- lectores de códigos de barras (opcional).

Cada cinta puede tener una etiqueta especial pegada al costado del cartucho y consistirá de:

- un código de barras para escanear con un lector especial que generalmente se monta en un cargador
- un valor digital en un código de barras legible.

Dichas etiquetas se utilizan para identificar la cinta en una biblioteca de cintas o especialmente en un almacén externo.

Si todos los cartuchos en una biblioteca de cintas tienen códigos de barra, la biblioteca está lista para gestionarse automáticamente con un software.

Las bibliotecas de cintas son una solución económica para los almacenes de datos con gran capacidad. Además, la cinta es perfecta para comprimir ya que los cartuchos pueden almacenarse de forma externa para lograr una mayor seguridad de los datos. Sin embargo, leer incluso una pequeña cantidad de datos desde una biblioteca de cintas toma mucho más tiempo (desde varios segundos a varios minutos) que desde otros tipos de almacenes de datos. La práctica más adecuada para el uso de la cinta es "MENOS solicitudes para escribir/leer MAYOR cantidad de datos". Entonces, el acceso

sistemático a cantidades muy grandes de datos es más adecuado para una biblioteca de cintas que para el acceso aleatorio a pequeñas porciones de datos.

## Limitaciones

Las limitaciones del uso de la biblioteca de cintas son las siguientes:

1. La operación de consolidación (pág. 403) no es posible para los archivos comprimidos ubicados en las cintas. La eliminación de una sola copia de seguridad separada es imposible desde una cinta. Es posible eliminar todas las copias de seguridad almacenadas en una cinta. Sin embargo, después de esta operación, todas las copias de seguridad incrementales y diferenciales, almacenadas en otras cintas y basadas en las copias de seguridad eliminadas, no pueden utilizarse para la recuperación de datos. En las reglas de retención del plan de copia de seguridad **Personalizado**, la opción **Si la eliminación de una copia de seguridad afecta a otras copias de seguridad > Consolidar la copia de seguridad** está deshabilitada. Solo la opción **Postergar la eliminación** está disponible.
2. Deduplicación (pág. 404) no está disponible para archivos comprimidos ubicados en los dispositivos de almacenamiento de cintas.
3. La recuperación de archivos es posible desde una copia de seguridad de un disco almacenado en cinta, pero puede demorar mucho tiempo.
4. Una cinta con copias de seguridad escrita por el nodo de almacenamiento no puede leerse en un dispositivo de cintas conectado localmente a un equipo en el que el agente está instalado debido a la diferencia en el formato de la cinta. Para conseguir información sobre la legibilidad de los archivos comprimidos en las cintas, escritos por otros componentes de otras versiones de los productos por medio de Acronis Backup & Recovery 10, consulte la sección Tabla Compatibilidad de cintas (pág. 47).
5. No se utilizan las impresoras de códigos de barras.

## Grupos de dispositivos RSM

Acronis Backup & Recovery 10 utiliza Removable Storage Manager (RSM) de Windows para gestionar los cartuchos de cintas que pertenecen a las bibliotecas de cintas.

Para separar el acceso a los dispositivos por los diferentes programas, RSM utiliza los llamados Grupos de dispositivos que son grupos de dispositivos lógicos. Existen dos categorías de grupos de dispositivos en el administrador: **Sistema** y **Aplicación**.

Los grupos de dispositivos del **Sistema** incluyen el grupo **Libre**, el grupo **Importación** y el grupo **No reconocido**. Los grupos del **Sistema** contienen dispositivos que las aplicaciones no están utilizando actualmente. El grupo **Libre** contiene dispositivos que se consideran desocupados y que pueden ser utilizados por cualquier aplicación. Los grupos **Importación** y **No reconocido** son grupos temporales para dispositivos que son nuevos en una cierta biblioteca.

A través de RSM, una aplicación puede obtener sus propios grupos con sus nombres propios, mover el dispositivo desde el grupo **Libre** a sus propios grupos, utilizar los dispositivos de sus propios grupos con el objetivo correcto, regresar el dispositivo al grupo **Libre**, etc.

Acronis Backup & Recovery 10 Storage Node gestiona las cintas que pertenecen al grupo **Acronis**.

Si las ranuras de la biblioteca se llenan con cintas nuevas, se incluirán todas las cintas automáticamente en el grupo **Libre**.

Si una cinta se ha utilizado con anterioridad, el RSM intenta detectar la aplicación registrada que le concierne a la cinta. Si la aplicación no se encuentra, RSM enviará la cinta al grupo **No reconocido**. Si la aplicación no se encuentra, pero la base de datos del RSM no tiene información acerca de la cinta,

se enviará al grupo **Importación**. Si la base de datos de RSM dispone de la información, la cinta se envía a su propio grupo de la aplicación.

Acronis Backup & Recovery 10 Storage Node suministra el RSM para detectar las cintas escritas por las familias de productos Acronis True Image Echo, Acronis True Image 9.1 y los componentes de Acronis Backup & Recovery 10. El nodo de almacenamiento ubicará a todas las cintas escritas en formato **Acronis** en el grupo Acronis durante la operación Inventario (pág. 146).

Los componentes de Acronis Backup & Recovery 10 no utilizan el grupo **No reconocido**. Para utilizar una cinta de este grupo de manera forzada, envíe la cinta al grupo **Libre** utilizando el complemento de almacenamiento extraíble **(Panel de control Herramientas administrativas Gestión del equipo Almacenamiento extraíble Grupos de dispositivos)**.

*Si una cinta se ha enviado al grupo **Libre**, se considera una cinta en blanco y cualquier aplicación podrá acceder a ella. Por lo tanto, los datos de la cinta se perderán.*

Si se eliminan todas las copias de seguridad de una cinta, la misma no regresará al grupo **Libre**. Esta permanece en el grupo **Acronis** como una cinta en blanco para volver a ser utilizada. Así, si el nodo de almacenamiento necesita una cinta nueva, busca una cinta en blanco primero en el grupo **Acronis** y después en el grupo **Libre**.

Posteriormente, Acronis Backup & Recovery 10 Storage Node trabaja solo con cintas que pertenecen al grupo **Acronis**.

## Comenzar con el uso de la biblioteca de cintas

Si tiene un dispositivo de bibliotecas de cintas adjuntado a un equipo con Acronis Backup & Recovery 10 Storage Node instalado, todo lo que debe hacer para realizar una copia de seguridad en la biblioteca de cintas es crear una bóveda de archivo comprimido en el dispositivo bajo la gestión del nodo de almacenamiento.

### Requisitos previos

Un dispositivo de biblioteca de cintas debe instalarse en un equipo que funcione con Windows de acuerdo con las instrucciones de instalación del fabricante.

Si Removable Storage Manager (RSM) está incluido en su versión de Windows, debe estar activado.

En Microsoft Windows XP y Microsoft Windows Server 2003:

- Removable Storage Manager es parte del sistema operativo y está activado inicialmente.

Para activar Removable Storage Manager en Microsoft Windows Server 2008:

1. Haga clic en **Herramientas administrativas > Administrador del servidor > Funciones > Añadir función**.
2. Seleccione la casilla de verificación **Removable Storage Manager**.

Para activar Removable Storage Manager en Microsoft Windows Vista:

1. Haga clic en **Panel de control > Programas > Programas y funciones > Activar o desactivar las funciones de Windows**.
2. Seleccione la casilla de verificación **Removable Storage Management**.

Llene las ranuras de la biblioteca con cartuchos de cintas. Si una cinta no obtiene un código de barras o si el código de barras está dañado, puede definir la etiqueta de la cinta más tarde para identificarla.

Debe tener instalado Acronis Backup & Recovery 10 Management Server y Acronis Backup & Recovery 10 Management Console en equipos locales o remotos, así como Acronis Backup & Recovery 10 Storage Node en el equipo que contiene la biblioteca de cintas y registrado en el servidor de gestión.

## La biblioteca de cintas como una bóveda gestionada

Para habilitar las operaciones de protección de datos utilizando una biblioteca de cintas, debe crear una bóveda gestionada en la biblioteca de cintas. Puede crear una bóveda desde la vista **Bóvedas centralizadas** de la consola. Consulte la sección Creación de una bóveda centralizada (pág. 135) para obtener más información.

Pero la manera más simple es crear una bóveda desde la vista **Nodos de almacenamiento**. Además, seleccione el nodo de almacenamiento al cual está conectada la biblioteca de cintas y haga clic en **Crear bóveda**. Se visualizará la página **Crear bóveda centralizada** con los parámetros preseleccionados. Todo lo que debe hacer es especificar el **Nombre** de la bóveda antes de hacer clic en **Aceptar**.

Una vez que la bóveda se haya creado, es posible acceder a ella desde la vista **Bóvedas centralizadas** de la consola. A continuación, la biblioteca de cintas puede utilizarse para crear copias de seguridad.

Acronis Backup & Recovery 10 permite crear solo una bóveda por dispositivo de cinta.

Si todos los cartuchos en una biblioteca de cintas tienen códigos de barra y el grupo **Libre** de RSM contiene suficientes cintas para un esquema de cintas elegido, la biblioteca está lista para trabajar completamente de manera automática.

Puede comenzar a trabajar con la bóveda aunque todas las ranuras de la biblioteca de cintas estén vacías. Si no hay cintas disponibles en las ranuras de las bibliotecas de cintas durante la operación de copia de seguridad, la ventana **Tareas que necesitan interacción** le pedirá que cargue una cinta.

Si no se puede leer el código de barras de una cinta, otra ventana **Tareas que necesitan interacción** le pedirá que etiquete la cinta.

## Acciones en una bóveda de biblioteca de cintas

Si una bóveda de biblioteca de cintas está seleccionada en el panel **Navegación** de la consola, la barra de herramientas de la página de las **Bóvedas centralizadas** contendrá las siguientes dos acciones que son utilizadas solo para bibliotecas de cintas:

- **Gestionar cintas** muestra la ventana **Gestión de cintas** permitiéndole actualizar la información en las ranuras de la biblioteca, las cintas del inventario en las ranuras y definir las etiquetas para las cintas. Si hay una nueva etiqueta asignada a una cinta, la acción le permite expulsar la cinta temporalmente para realizar la misma etiqueta fuera del cartucho.
- **Volver a explorar las cintas** muestra la ventana **Volver a explorar la cinta**, que sirve para seleccionar las ranuras e iniciar el procedimiento Volver a explorar (pág. 146) para leer información especial en el contenido de las cintas especificadas.

También están habilitadas las funciones **Editar**, **Eliminar**, **Validar** y **Actualizar** en la bóveda de biblioteca de cintas.

Se debe tener en cuenta que estas funciones tienen algunas funciones específicas para una biblioteca de cintas. Por lo tanto, la operación **Editar** le permite sustituir un dispositivo de biblioteca de cintas

sin la operación **Volver a explorar**. La operación **Eliminar** borra toda la información en la bóveda de biblioteca de cintas seleccionada de la base de datos del nodo de almacenamiento, es decir, la operación elimina los datos del contenido de todas las cintas siempre que los datos sean utilizados por el nodo en el dispositivo de biblioteca de cintas.

*En la operación **Eliminar**, el contenido de la bóveda será eliminado de la base de datos del nodo de almacenamiento sin acceder a las cintas. Los planes y las tareas que utilizan esta bóveda fallarán.*

*Los archivos comprimidos de copia de seguridad, que pertenecen a una bóveda centralizada de eliminación en la biblioteca de cintas, también se eliminarán, pero estos archivos comprimidos pueden recuperarse con cualquier nodo de almacenamiento a través de la operación **Volver a explorar**.*

## Acciones con archivos comprimidos en cintas en una biblioteca

Las siguientes son funciones comunes para la gestión de datos de archivos comprimidos para un archivo comprimido de copia de seguridad seleccionado en la vista **Bóvedas centralizadas** de la consola cuando la bóveda actual es una biblioteca de cintas: **Validar**, **Eliminar**, **Eliminar todos los archivos comprimidos**. La eliminación en la base de datos del nodo de almacenamiento se lleva a cabo sin acceder a las cintar. Un archivo comprimido de copia de seguridad eliminado de una bóveda de biblioteca de cintas puede restaurarse después de la eliminación a través de la operación Volver a explorar (pág. 146), que se lleva a cabo en todas las cintas conservando todos los datos del archivo comprimido.

La operación **Volver a explorar** para una cinta, de donde se eliminó una copia de seguridad, puede recuperar la copia de seguridad ya que recrea la información en el contenido de la copia de seguridad en la base de datos del nodo de almacenamiento.

*Si todas las copias de seguridad se eliminan de una cinta, se considera libre. Por lo que las copias de seguridad eliminadas se perderán irrevocablemente después de escribir por primera vez en la cinta.*

## Creación de copias de seguridad en bibliotecas de cintas

Al crear una política/plan de copias de seguridad con un destino de biblioteca de cintas, establece la copia de seguridad de la misma manera que con otros dispositivos de almacenamiento. La única diferencia consiste en las opciones de Soporte para cintas (pág. 117) adicionales que se pueden configurar durante la creación de la política/plan de copia de seguridad. Estas opciones le permite especificar cómo la política/plan de copias de seguridad creada utiliza cintas desde la biblioteca de cintas, sin embargo las opciones predeterminadas aumentan la eficiencia en el uso de la biblioteca de cintas completa y cada cinta.

Para ver y cambiar las opciones de cintas, seleccione **Opciones > Opciones predeterminadas de copia de seguridad y recuperación > Opciones predeterminadas de copia de seguridad > Soporte para cintas** del menú superior.

Para cambiar las configuraciones de la política/plan de copias de seguridad que se crearán haga clic en **Cambiar...** en la sección de **Opciones de copia de seguridad** en la página **Crear política/plan de copias de seguridad**. Abre la ventana **Opciones copia de seguridad** donde se encuentra la página de **Soporte para cintas** con los valores predefinidos.

Cuando realice la copia de seguridad en la cinta y llega al final de la cinta, se montará una cinta en blanco automáticamente y la operación continuará en la cinta nueva.

Mientras se esté ejecutando una tarea de copia de seguridad, se puede acceder a la siguiente información específica de la cinta desde la consola:

- la cantidad de cintas que la operación de copia de seguridad está utilizando actualmente
- las etiquetas de las cintas que la tarea utilizó hasta el momento en caso de que exista una división de copias de seguridad
- la etiqueta de la cinta que se está escribiendo actualmente.

## Recuperación desde una biblioteca de cintas

La recuperación de datos desde archivos comprimidos ubicados en dispositivos de cintas se realiza de la misma manera que con los demás dispositivos de almacenamiento.

Para realizar la recuperación, cree una tarea de recuperación, seleccione la bóveda del dispositivo de cinta y seleccione el archivo comprimido y la copia de seguridad de donde recuperar los datos. Al crear la tarea, el programa utiliza la base de datos del nodo de almacenamiento en lugar de acceder a las cintas. Sin embargo, la selección de los datos que va a recuperar (por ejemplo, algunos archivos o volúmenes específicos) debe leer de una o más cintas, por lo que puede llevar algún tiempo.

El programa busca las cintas y las introduce automáticamente en el orden correcto. Aparece la ventana **Tareas que necesitan interacción** si no se encuentra la cinta necesaria.

Tenga en cuenta que una operación de recuperación de datos puede necesitar el acceso a varias cintas. Por ejemplo, la recuperación de datos desde una copia de seguridad incremental comúnmente necesita la carga, el montaje, el rebobinado y la lectura de las siguientes cintas que contienen las copias de seguridad de datos:

- las cintas que almacenan la copia de datos incremental seleccionada para recuperar los datos
- las cintas que almacenan la última copia de seguridad completa creada antes de la copia de seguridad incremental seleccionada
- las cintas que almacenan la última copia de seguridad diferencial creada después de la última copia de seguridad completa, pero antes de la copia de seguridad incremental seleccionada, si fuera necesario
- las cintas que contienen todas las copias de seguridad incrementales creadas después de las últimas copias de seguridad diferenciales o completas antes de la copia de seguridad incremental seleccionada, si fuera necesario.

Mientras se esté ejecutando una tarea de recuperación, es posible acceder a la siguiente información específica de la cinta desde la consola de gestión:

- las etiquetas de todas las cintas que puedan necesitarse para la operación
- la etiqueta de la cinta que se está leyendo actualmente.
- las etiquetas de las cintas que ya se han leído
- las etiquetas de las cintas que todavía están esperando ser leídas con información sobre su disponibilidad actual (cargadas o no).

## Gestión de una biblioteca de cintas

Para gestionar una biblioteca de cintas, el producto posee las siguientes tareas/procedimientos:

- Inventario (pág. 146)
- Volver a explorar (pág. 146)
- Etiquetado (pág. 147)

Cualquier usuario con acceso a la bóveda gestionada en una biblioteca de cintas puede llevar a cabo estas operaciones. Sin embargo, dos o más usuarios no pueden gestionar una unidad de biblioteca de cintas simultáneamente ya que algunas operaciones pueden demorar minutos, horas o incluso días.

Por ejemplo, si un usuario inicia una tarea de **Volver a explorar** de una biblioteca de cintas, todas las solicitudes de los otros usuarios de realizar la misma tarea se cancelarán automáticamente porque ya se está ejecutando en la bóveda.

## Inventario

Un nodo de almacenamiento necesita información acerca de una cinta en su propia base de datos para poder operar con la cinta. Entonces, después de que se crea la bóveda, generalmente el próximo paso es inventariar cintas.

Inventariar es un procedimiento que permite al nodo de almacenamiento reconocer cintas que están cargadas actualmente en las ranuras de la biblioteca de cintas. Es relativamente rápido y normalmente necesita el código de barras del cartucho sin leer los datos de la cinta. Si no se puede leer un código de barras, la cinta se montará para leer solo su GUID identificador.

El procedimiento de **Inventariar** puede ser ejecutado manualmente por un usuario o automáticamente cuando se necesita el acceso a cintas recientemente agregadas.

Para iniciar el procedimiento, seleccione la bóveda de la biblioteca de cintas en el panel de **Navegación** de la consola, haga clic en **Gestionar cintas** y después haga clic en **Iniciar inventario** en la ventana **Gestión de cintas**.

Cuando el inventario haya finalizado, un usuario tiene la lista de cintas que están cargadas actualmente en la biblioteca.

Realice el procedimiento cada vez que cargue nuevas cintas a las ranuras de la biblioteca de cintas.

## Volver a explorar

Según se indica anteriormente, el nodo de almacenamiento conserva la información acerca de las cintas y su contenido en una base de datos dedicada. La tarea **Volver a explorar** lee la información acerca del contenido de las cintas seleccionadas por el usuario y actualiza la base de datos.

La tarea puede llevar mucho tiempo por lo que solo se puede iniciar manualmente. Puede seleccionar cada ranura con una cinta que desea volver a explorar antes de que comience la tarea.

Ejecutar la tarea **Volver a explorar**:

- para cintas que son desconocidas para el nodo de almacenamiento
- si se pierde o se daña la base de datos del nodo de almacenamiento
- para cintas cuyo contenido está desactualizado (por ejemplo, el contenido de una cinta que se ha modificado a través de otro nodo de almacenamiento o de forma manual).

Tenga en cuenta que una cinta puede conservar algunas copias de seguridad que se han eliminado antes de la nueva exploración de la cinta. Por lo tanto, antes de que la tarea finalice, todas dichas copias de seguridad se recuperarán en la base de datos del nodo de almacenamiento y se vuelven accesibles para la recuperación de datos.

Al volver a explorar, la etiqueta de una cinta debe guardarse en la base de datos del nodo de almacenamiento. Si una ranura, seleccionada para el procedimiento, contiene una cinta que todavía no tiene ninguna etiqueta, la tarea **Volver a explorar** de la cinta se detiene para llevar a cabo el procedimiento Etiquetado (pág. 147).

## Etiquetado

Cuando no se encuentra una cinta necesaria para la recuperación de datos, la ventana de **Tarea necesita interacción** le pedirá al usuario traer la cinta e insertarla en una ranura de la biblioteca de cintas. Entonces, todos los cartuchos de cintas necesitan un código de barras u otras etiquetas legibles.

Si una cinta no obtiene una etiqueta, deberá definirla antes de que la cinta se utilice.

Si necesita aplicar una etiqueta específica a una cinta (por ejemplo, la etiqueta "MiTrabajo" para un cinta dedicada a realizar copias de seguridad de los archivos de la carpeta C:\trabajo) en vez de una etiqueta de código de barras, utilice también el procedimiento de **Etiquetado**.

Para ejecutar el procedimiento, seleccione la bóveda de biblioteca de cintas en el panel de **Navegación** de la consola y haga clic en **Gestionar cintas** en la barra de herramientas. A continuación, la ventana **Gestión de cintas** mostrará una lista de las ranuras de la biblioteca que contienen cintas. El campo de datos de la ranura indica la etiqueta de la cinta de las cintas que pertenecen al grupo **Libre** o al grupo **Acronis**. También se muestran las etiquetas de las cintas que están en el grupo **Importados** y contienen copias de seguridad escritas por Acronis (este puede ser el caso si trae una cinta de otra biblioteca de cintas).

De manera predeterminada, una cinta sin utilizar con un código de barras obtiene una etiqueta que es igual al código de barras. Si un código de barras está ausente o dañado, el nombre de la etiqueta se creará automáticamente. Puede aceptar las etiquetas propuestas o proporcionar su propia etiqueta como texto simple.

Los nombres de las cintas de los grupos **Libre** o **Importados** se pueden modificar si la cuenta de usuario que ejecuta el servicio de nodo de almacenamiento (**Usuario ASN**) tiene permisos de escritura para esos grupos. Estos permisos no se asignan al **Usuario ASN** durante la instalación, por lo que es posible que deba añadirlos manualmente.

Para definir su propia etiqueta para una cinta, seleccione un campo de datos relacionado, escriba una nueva etiqueta, haga clic en **Expulsar cinta**, escriba la misma etiqueta en el cartucho de la cinta (para asociarla con la etiqueta) e insértela de nuevo en la misma ranura.

Una vez que todas las etiquetas necesarias de las cintas estén especificadas, pulse **Establecer etiquetas** para almacenar las etiquetas en la base de datos del nodo de almacenamiento.

## Soporte de cintas

Estas opciones son efectivas cuando el destino de la copia de seguridad es una bóveda gestionada ubicada en una biblioteca de cintas.

**Las opciones de Soporte para Cintas** le permiten especificar cómo las tareas de copias de seguridad distribuirán las copias de seguridad entre las cintas.

---

*Algunas combinaciones de las opciones de cintas pueden degradar la eficiencia en el uso de la biblioteca de cintas entera y de cada cinta. Si no se ve obligado a modificar estas opciones debido a necesidades específicas, no las cambie.*

---

Un archivo comprimido puede ocupar varias cintas. En tales casos se utiliza un llamado **conjunto de cintas** para conservar las copias de seguridad de datos.

> Un **conjunto de cintas** es un grupo lógico de una o más cintas que contienen copias de seguridad de los datos específicos protegidos. Un conjunto de cintas también puede contener copias de seguridad de otros datos.

Un **conjunto de cintas separado** es un conjunto de cintas que contiene copias de seguridad de los datos específicos protegidos. Otras copias de seguridad no pueden escribirse en un conjunto de cintas separado.

### (Para la política o el plan de copias de seguridad a crear) Utilice un conjunto de cintas separado

El valor predeterminado: **Deshabilitado**.

Si no cambia esta opción, entonces las copias de seguridad, que pertenecen a la política o al plan que se está creando, pueden escribirse sobre cintas que contienen copias de seguridad escritos por diferentes políticas de copia de seguridad y que contienen datos de diferentes equipos. De la misma manera, las copias de seguridad de otras políticas pueden escribirse en cintas que contienen las copias de seguridad de esta política. No tendrá problemas con dichas cintas, ya que el programa gestiona todas las cintas automáticamente.

Cuando está opción está habilitada, las copias de seguridad, que pertenecen a la política o al plan que se está creando, se ubicarán en un conjunto de cintas separado. Otras copias de seguridad no se escribirán en este conjunto de cintas.

### Si la consola está conectada al servidor de gestión

La opción **Utilizar un conjunto de cintas separado** tiene definiciones más precisas. Para crear una política de copias de seguridad puede utilizar un conjunto de cintas separado para todos los equipos o para cada equipo.

La opción **Un único conjunto de cintas para todos los equipos** está seleccionada de manera predeterminada. Generalmente, esta opción asegura un uso más eficiente de las cintas que la opción **Utilizar un conjunto de cintas separado para cada equipo**. Sin embargo, la segunda puede ser útil, por ejemplo, cuando existen requisitos especiales para almacenar las cintas con copias de seguridad desde un equipo específico externo.

Cuando la opción **Utilizar un conjunto de cintas separado** está habilitada, puede suceder que se tenga que escribir la copia de seguridad en una cinta que esté actualmente fuera del dispositivo de biblioteca de cintas. Qué hay que hacer en este caso.

- **Pedir la interacción del usuario**: la tarea de copia de seguridad entrará en el estado **Necesita interacción** y esperará a que se cargue la cinta, con la etiqueta requerida, al dispositivo de biblioteca de cintas.
- **Utilizar una cinta en blanco**: la copia de seguridad se escribirá en una cinta en blanco, por lo que la operación se detendrá sólo si no hay ninguna cinta en blanco en la biblioteca.

### Utilizar siempre una cinta en blanco

Si no cambia las opciones a continuación, entonces cada copia de seguridad se escribirá en una cinta especificada por la opción **Utilizar un conjunto de cintas separado**. Con algunas de las siguientes opciones habilitadas, el programa añadirá cintas nuevas al conjunto de cintas cada vez que se cree una copia de seguridad completa, incremental o diferencial.

- **Para cada copia de seguridad completa**

El valor predeterminado: **Deshabilitado**.

Cuando esta opción está habilitada, cada copia de seguridad completa se escribirá en una cinta en blanco. Se cargará la cinta a una unidad especialmente destinada para esta operación. Si la opción **Utilizar un conjunto de cintas separado** está habilitada, sólo las copias de seguridad incrementales y diferenciales de los datos se añadirán al final de la cinta.

- **Para cada copia de seguridad diferencial**

El valor predeterminado: **Deshabilitado**.

Cuando esta opción está habilitada, cada copia de seguridad diferencial se escribirá en una cinta en blanco. Esta opción está disponible sólo cuando se selecciona la opción de utilizar una cinta en blanco para cada copia de seguridad completa.

- **Para cada copia de seguridad incremental**

El valor predeterminado: **Deshabilitado**.

Cuando esta opción está habilitada, cada copia de seguridad incremental se escribirá en una cinta en blanco. Esta opción sólo está disponible cuando se selecciona la opción de utilizar una cinta en blanco para cada copia de seguridad completa y diferencial.

### Rotación de cintas

Si se eliminan todas las copias de seguridad de una cinta, es decir, si se elimina la información acerca de la última copia de seguridad en la cinta de la base de datos del nodo de almacenamiento, la cinta se considera vacía y puede volver a utilizarse durante el ciclo de copias de seguridad. La misma rotación de cintas le permite arreglarse con la cantidad mínima de cartuchos en lugar de tener que trabajar siempre con cintas utilizadas.

Acronis Backup & Recovery 10 le permite conseguir una automatización completa de la rotación de cintas mientras se realizan las copias de seguridad en la biblioteca de cintas.

Esta sección le proporciona información útil para elegir un esquema de copia de seguridad y las opciones de cintas para la rotación de cintas.

Para calcular la cantidad de cintas necesarias para los esquemas de rotación de cintas, puede utilizar el método descrito en la sección Planificación de cintas (pág. 162).

## Elección de un esquema de copia de seguridad

Al crear una política/plan de copias de seguridad con una biblioteca de cintas como destino, se habilitan los siguientes esquemas de copia de seguridad: **Realizar una copia de seguridad ahora**, **Realizar una copia de seguridad más tarde**, **Abuelo-padre-hijo**, **Torres de Hanói**, o **Personalizado**. El esquema de copia de seguridad **Simple está deshabilitado**, ya que la consolidación de la copia de seguridad es imposible para los archivos comprimidos ubicados en cintas.

Acronis Backup & Recovery 10 proporciona automatización de rotación de cintas para esquemas de copia de seguridad **Abuelo-padre-hijo**, **Torres de Hanói** y **Personalizado**.

Abuelo-padre-hijo (pág. 35) (GFS) y Torres de Hanói (pág. 39) (ToH) son los esquemas de copia de seguridad más populares para utilizar en dispositivos de bibliotecas de cintas. Estos esquemas están optimizados para mantener el mejor balance entre el tamaño del archivo comprimido de la copia de seguridad, la cantidad de puntos de recuperación disponibles del archivo comprimido y la cantidad de cintas necesarias para la compresión.

Si su archivo comprimido debe proporcionar una recuperación con una resolución diaria para los últimos días, una resolución semanal para las últimas semanas y una resolución mensual para cualquier momento en el pasado, entonces el esquema más adecuado para usted es el esquema **Abuelo-Padre-Hijo**.

Si el objetivo principal es proporcionar protección de datos durante el periodo más largo con un mínimo uso de cintas utilizadas, permanentemente cargadas a una pequeña biblioteca de cintas (por

ejemplo, cargador automático), la mejor solución probablemente sea elegir el esquema **Torres de Hanói**.

El esquema de copia de esquema **Personalizado** le permite especificar reglas de programación y retención para definir la rotación de cintas deseada. Utilice este esquema, cuando el uso de los esquemas **Abuelo-Padre-Hijo** y **Torres de Hanói** no sean suficiente. Por ejemplo, si el tamaño completo de datos protegidos es considerablemente menor que el tamaño de la cinta, la mejor opción es utilizar el esquema de copia de seguridad **Personalizado** con copias de seguridad completas diarias/semanales/mensuales, algunas reglas simples de retención y opciones de cintas predeterminadas.

## Criterio de elección

Cada vez que esté a punto de diseñar un esquema de rotación de cintas para una política/plan de copias de seguridad que va a crear, debe tomar como principio los siguientes argumentos:

- el tamaño completo de los datos que va a proteger
- el tamaño aproximado de los cambios diarios de los datos
- el tamaño aproximado de los cambios semanales de los datos
- los requisitos del esquema de copia de seguridad (frecuencia, rendimiento y duración de operaciones de copia de seguridad)
- los requisitos para conservar las copias de seguridad (periodo mínimo/máximo de conservación de copias de seguridad; necesidad de almacenar los cartuchos de cintas externamente)
- capacidad de la biblioteca de cintas (número de controladores, cargadores, ranuras y cintas disponibles; capacidad de las cintas)
- requisitos para la recuperación de datos (duración máxima)

Es necesario que analice cada argumento que sea relevante para su caso y seleccione el criterio de elección principal. Después, elija un esquema de copia de seguridad y especifique las opciones de cintas.

Tenga en cuenta que todo esquema de copia de datos combinado con diferentes opciones de cintas tendrá resultados bastante diferentes para el uso eficiente de las cintas y los dispositivos.

## Caso a analizar

Supongamos que necesita automatizar una rotación de cintas para el caso si:

- el tamaño completo de los datos que va a proteger es aproximadamente de 320 GB
- el tamaño aproximado de los cambios diarios de los datos es de 16 GB
- el tamaño aproximado de los cambios semanales de los datos no es mayor a 40 GB
- la capacidad de la cinta es de 400 GB.

Analicemos los resultados de una combinación de esquemas GFS y Torre de Hanoi con opciones diferentes de las cintas para el caso.

Todos los ejemplos analizados a continuación tienen un enfoque simplista a un caso real, pero le proporcionan una concepción general de la distribución de las copias de seguridad en las cintas.

### Leyenda de las cifras de ejemplo del caso

Toda copia de seguridad diaria/incremental (16 GB) se muestra en las cifras como un rectángulo verde:  .

Las copias de seguridad semanales/diferenciales (40 GB) se muestran como un rectángulo azul:  .

Una copia de seguridad mensual (320 GB) se representa como un rectángulo naranja:

 .

Una cinta completa (400 GB) se representa como un rectángulo gris:

 .

## Uso del esquema de rotación de cintas Abuelo-Padre-Hijo (GFS)

La rotación de cintas para el esquema de copias de seguridad GFS está definida substancialmente por las opciones de cintas especificadas para la política o el plan de copias de seguridad a crear.

Supongamos que las configuraciones GFS son las siguientes:

- **Comienzo de la copia de seguridad en:** **23:00:00**
- **Copia de seguridad en:** **Días hábiles**
- **Semanalmente/mensualmente:** **Viernes**
- **Mantener copias de seguridad:** **Diariamente: 2 semanas; Semanalmente: 2 meses; Mensualmente: 1 año**.

El objetivo principal es lograr una automatización total de la rotación de cintas para estas configuraciones.

Tenga en cuenta que una copia de seguridad mensual es completa, una copia de seguridad semanal es diferencial y una copia de seguridad mensual es incremental en esta implementación del esquema GFS. La primera copia de seguridad siempre es completa. Entonces si la política o el plan de copias de seguridad comienza el miércoles y las copias de seguridad completas deben crearse todos los cuartos viernes del mes, el miércoles la primera copia de seguridad será completa en lugar de ser incremental.

Existen ejemplos analizados que muestran cómo el esquema GFS puede combinarse con diferentes opciones de cintas en las siguientes secciones:

- Ejemplo 1 GFS (pág. 152). La opción **Utilizar un conjunto de cintas separado** está seleccionada. Todas las opciones de **Utilizar siempre una cinta en blanco** están desactivadas. Requiere 25 cintas en rotación.
- Ejemplo 2 GFS (pág. 155) La opción **Utilizar un conjunto de cintas separado** está seleccionada. La opción de **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa la opción** está seleccionada. Las otras opciones de **Utilizar siempre una cinta en blanco** están desactivadas. Requiere 16 cintas en rotación.
- Ejemplo 3 GFS (pág. 156) La opción **Utilizar un conjunto de cintas separado** está seleccionada. Todas las opciones de **Utilizar siempre una cinta en blanco** están seleccionadas. Requiere 28 cintas en rotación.

Estos ejemplos demuestran cómo la cantidad de cintas requeridas para la rotación automatizada depende de las opciones de cintas. Si una biblioteca de cintas no tiene suficientes cintas para la rotación automática, la ventana **Tareas que necesitan interacción** le pedirá algunas veces cargar una cinta en blanco a la biblioteca.

## Ejemplo 1 GFS

Supongamos que el plan de copia de seguridad tiene las siguientes opciones de cinta:

- La opción **Utilizar un conjunto de cintas separado** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa** está desactivada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad incremental** está desactivada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad diferencial** está desactivada.

Imaginemos que la primera operación de copia de seguridad está programada para el viernes, 1 de enero. A las 23:00 de ese día, se crea la primera copia de seguridad completa (320 GB en la cinta cuyo tamaño es de 400 GB). Como la opción **Utilizar un conjunto de cintas separado** está seleccionada, se expulsa la cinta actualmente montada (si no es una cinta en blanco). Entonces se carga especialmente una cinta en blanco para realizar una copia de seguridad de los datos. La cinta está marcada con el número 01 en la figura siguiente. De acuerdo con la leyenda descrita en la sección Caso a analizar (pág. 150), la copia de seguridad completa se muestra como un rectángulo naranja en la figura.

Las configuraciones del esquema de copia de seguridad GFS especificadas impulsa la copia de seguridad de los datos solo los **Días hábiles**, por lo que la próxima copia de seguridad se crea a la misma hora (**23:00**) el lunes 4 de enero. Esta copia de seguridad es una copia incremental (16 GB) que se escribe sobre la misma cinta 01, ya que **Utilizar siempre una cinta en blanco: para cada copia de seguridad incremental** está desactivada. La copia de seguridad aparece como un rectángulo verde en la figura.


Las próximas tres copias de seguridad incrementales se escriben sobre la cinta 01 el 5, 6 y 7 de enero. Como consecuencia, el espacio libre de la cinta es de solo 16 GB al momento.

El 8 de enero, la copia de seguridad diferencial de datos (40 GB) se registra sobre la misma cinta 01, ya que **Utilizar siempre una cinta en blanco: para cada copia de seguridad diferencial** está desactivada. Sin embargo, la cinta llega a su final después de que se escriben los primeros 16 GB de la copia de seguridad. A continuación, el cargador desmonta y expulsa la cinta de la unidad y la ubica en una ranura. Más adelante, se carga y se monta una cinta en blanco sobre la misma unidad y después la copia de seguridad (últimos 24 GB) continúa desde el principio de la cinta nueva.

La próxima figura representa el archivo comprimido de la copia de seguridad de datos al momento. La copia de seguridad diferencial aparece como un rectángulo azul en la figura. El número 1 en el rectángulo gris marca la copia incremental creada el lunes de la 1.ª semana del año.


A partir de entonces, las copias de seguridad se escriben sobre la cinta 02:

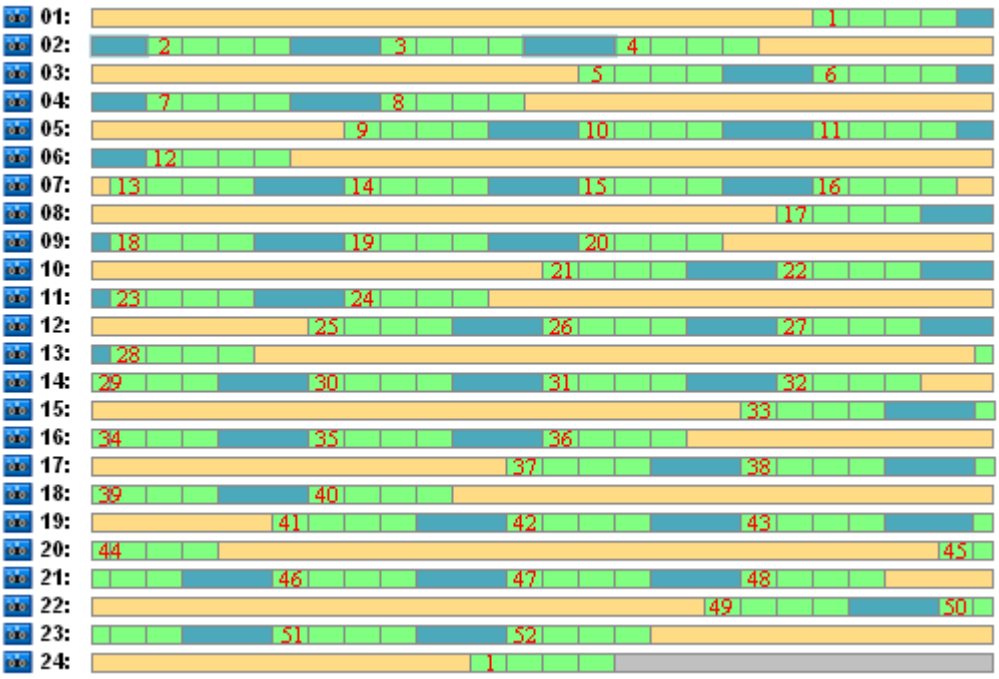
- cuatro copias de seguridad incrementales y una diferencial en la segunda semana
- cuatro copias de seguridad incrementales y una diferencial en la tercera semana
- cuatro copias de seguridad incrementales en la cuarta semana.

La próxima copia de seguridad completa (320 GB) debería escribirse el viernes de la cuarta semana. Sin embargo, la cinta 02 tiene solo 104 GB de espacio libre al momento. Entonces, después de que la cinta llega a su final, el registro continúa desde el comienzo de la cinta en blanco 03.


Tenga en cuenta que la tarea **Limpieza** se ejecuta después de cada operación de copia de seguridad para el esquema GFS. Esta tarea elimina todas las copias de seguridad antiguas. La próxima figura muestra rectángulos gris oscuro en representación de las copias de seguridad eliminadas hasta el momento.


Físicamente, las copias de seguridad eliminadas permanecen en las cintas; sin embargo la información acerca de las copias de seguridad se elimina de la base de datos del nodo de almacenamiento.

La siguiente figura muestra las copias de seguridad eliminadas como real, pero revela el uso de la cinta durante todo el año para el esquema de copia de seguridad GFS en combinación con las opciones de cintas especificadas. Un número en el rectángulo verde indica una copia de seguridad incremental creada el lunes de la semana correspondiente del año.




**Uso de la cinta durante el primer año**

La próxima figura muestra el uso real de las cintas con espacio libre en vez de las copias de seguridad eliminadas el primer viernes del año siguiente. En ese momento la copia de seguridad diferencial (rectángulo azul) se escribe sobre la cinta 24.


La copia de seguridad completa almacenada en la cinta 01 se elimina después de que se crea la próxima copia de seguridad completa sobre las cintas 23 y 24 el viernes de la semana n.º 52. Como todas las copias de seguridad de la cinta 01 se han eliminado, la cinta se considera virgen y puede volver a utilizarse.

Un análisis más completo del ejemplo comprueba que la cantidad máxima de cintas necesarias para almacenar la copia de seguridad de los datos es de 25. Este máximo ocurre en la semana n.º 16 del año siguiente.

Las figuras anteriores muestran que la recuperación de datos necesita una o dos cintas para una copia de seguridad completa, dos o tres cintas para una copia de seguridad diferencial y una, dos o tres cintas para una copia de seguridad incremental.

Por ejemplo, si necesitamos recuperar datos de una copia de seguridad creada el lunes de la semana n.º 52, la tarea necesitará las siguientes cintas:

- La cinta 23 con una copia de seguridad incremental (marcada con "52") y una copia de seguridad diferencial creada el viernes de la semana n.º 51
- La cinta 21 y la cinta 22 que contienen una copia de seguridad completa creada el viernes de la semana n.º 48.

El ejemplo revela las siguientes deficiencias de la combinación esquemática con las opciones de cintas especificadas:

- normalmente cualquier recuperación de datos es un largo proceso que requiere la carga, el montaje, el rebobinado y la lectura de una (3% - para copias de seguridad que se muestran en la figura "Uso de la cinta durante el primer año"), dos (65%) o tres (32%) cintas
- se utilizan 22 cintas para almacenar 13 copias de seguridad completas mensuales cuando el tamaño de copia de seguridad mensual es menor que el tamaño de la cinta, por lo que la conservación de datos es más costosa

- se necesitan 25 cintas para una rotación completa de un año de las copias de seguridad de datos.

## Ejemplo 2 GFS

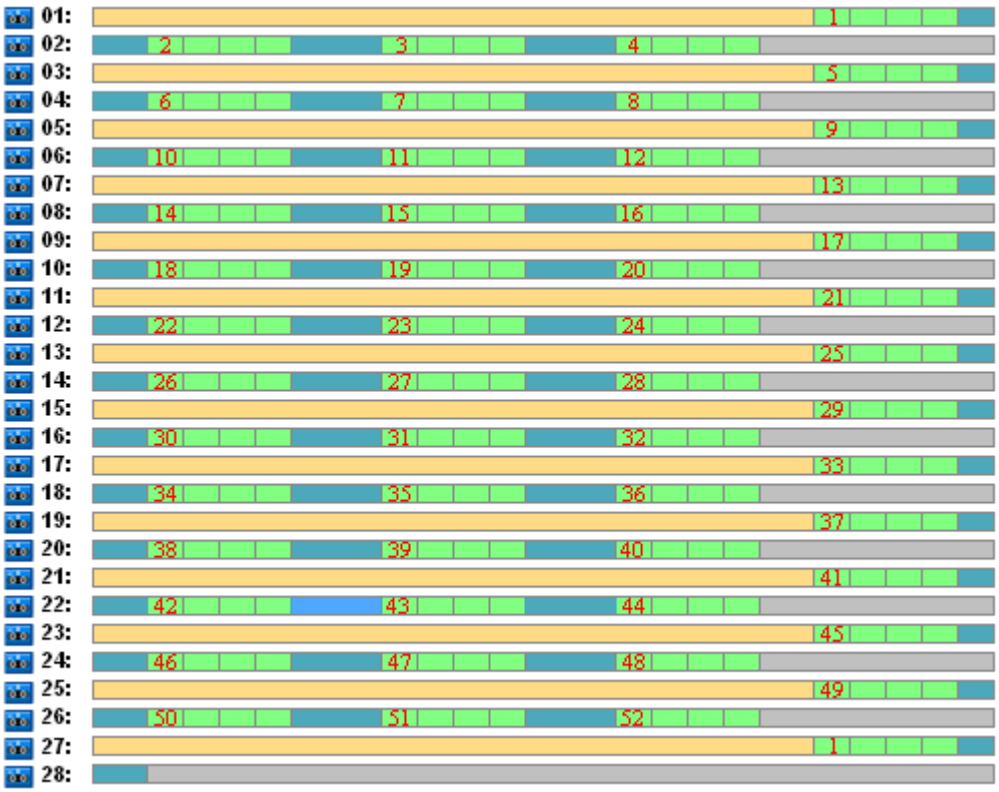
Supongamos que el plan de copia de seguridad tiene las siguientes opciones de cinta:

- La opción **Utilizar un conjunto de cintas separado** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad incremental** está desactivada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad diferencial** está desactivada.

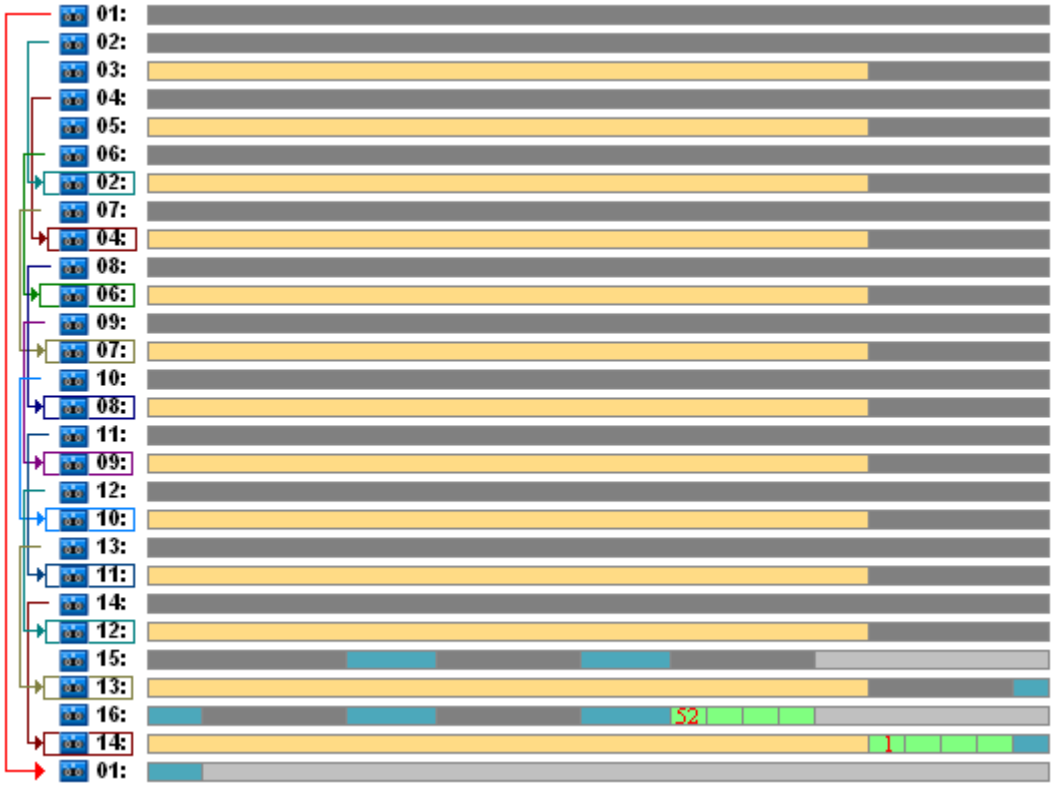
El ejemplo tiene solo una diferencia del anterior. Eso es que la selección de la opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa**.

La siguiente figura muestra las copias de seguridad eliminadas como real, pero revela el uso de la cinta durante todo el año para el esquema de copia de seguridad GFS en combinación con las opciones de cintas especificadas. Un número en el rectángulo verde indica una copia de seguridad incremental creada el lunes de la semana correspondiente del año.

Si todas las copias de seguridad deben conservarse durante el año, el archivo comprimido necesitará 28 cintas.



Ya que el esquema de copias de seguridad GFS impulsa la eliminación automática de copias de seguridad antiguas, el primer viernes del segundo año las cintas solo conservan las copias de seguridad que se muestran en la siguiente figura.




Esta figura demuestra que el esquema de rotación de cintas del **Ejemplo 2 GFS** es más adecuado para el caso que el **Ejemplo 1 GFS**. Las ventajas del esquema de rotación de cintas del **Ejemplo 2 GFS** para el caso analizado son las siguientes:

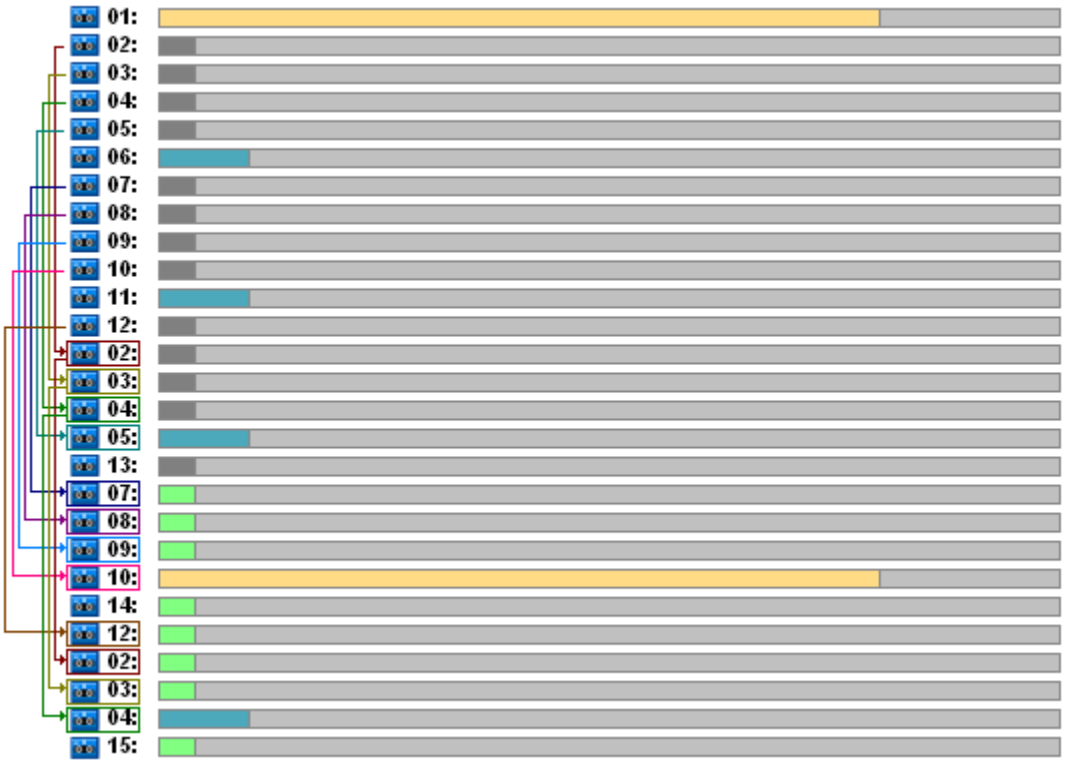
- utiliza 16 cintas en vez de 25
- una tarea de recuperación de datos requiere una (25%) o dos (75%) cintas
- la recuperación de datos de una copia de seguridad completa necesita solo una cinta que realice la recuperación de datos desde una copia de seguridad incremental o diferencial más rápido.

## Ejemplo 3 GFS

Imaginemos que el plan de copia de seguridad tiene las siguientes opciones de cinta:

- La opción **Utilizar un conjunto de cintas separado** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad incremental** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad diferencial** está seleccionada.

Estas opciones definen el esquema de rotación de cintas clásico para GFS. La figura muestra el comienzo del esquema de rotación que utiliza 8 cintas para copias de seguridad diarias, 6 cintas para copias de seguridad semanales y 13 cintas para copias de seguridad mensuales (ya que hay 13 ciclos de cuatro semanas en un año) para el caso analizado. Y se necesita una cinta para la próxima copia de seguridad. En total, este esquema de rotación combinado con las opciones necesita 28 cintas.




Para recuperar los datos se necesita solo una cinta para realizar una copia de seguridad completa, dos cintas para una copia de seguridad diferencial y dos o tres cintas para una copia de seguridad incremental.

Este esquema tiene las siguientes ventajas:

- el acceso a cualquier copia de seguridad completa necesita solo una cinta
- la eliminación de las copias de seguridad libera una cinta por lo que se puede volver a utilizar.

La principal desventaja es la gran cantidad de cintas necesarias que se utilizan 5-10%.

Si debemos realizar una copia de seguridad diaria durante una semana (4 copias de seguridad) y una copia de seguridad semanal durante un mes (4 copias de seguridad), la cantidad total de cintas necesarias será igual a 4+4+13+1 = 22.

## Uso del esquema de rotación de cintas Torres de Hanói

El esquema ToH requiere menos cintas para la rotación en comparación con el esquema GFS. Así, el esquema ToH es la mejor opción para pequeñas bibliotecas de cintas, especialmente para cargadores automáticos.

Una vez que se haya seleccionado el esquema de copias de seguridad ToH, es posible especificar la programación del esquema y la cantidad de niveles.

Se recomienda utilizar cinco niveles si está aplicando Torres de Hanói a las copias de seguridad semanales y ocho niveles si lo está aplicando a copias de seguridad diarias. En el primer caso, la

rotación incluye 16 sesiones semanales para garantizar que el período de recuperación (la cantidad mínima de días que puede volver atrás en el archivo comprimido) sea de 8 semanas. La rotación de las cintas para el segundo caso incluye 128 sesiones diarias, es decir, permite que el periodo de recuperación sea igual a 64 días. El período de recuperación siempre es la mitad de la cantidad de sesiones.

Cada nivel adicional duplica no solo la cantidad de sesiones sino también la edad de la copia de seguridad más antigua.

Volvamos al caso analizado descrito en la sección Caso para analizar (pág. 150) y supongamos que las configuraciones ToH son las siguientes:

- **Programación:** **Iniciar la tarea cada 1 día a las 23:00. Repetir una vez.**
- **Número de niveles: 5**

El esquema Torres de Hanói con cinco niveles garantiza que el período de recuperación sea de 8 días. Designaremos las copias de seguridad de los niveles con los números del 1 al 5 con las letras A, B, C, D y E respectivamente. Así la plantilla de rotación para la secuencia de copia de seguridad en el archivo comprimido es la siguiente: E-A-B-A-C-A-B-A-D-A-B-A-C-A-B-A. En el esquema ToH de cinco niveles todas las copias de seguridad del primer nivel (A) son incrementales, en el quinto nivel (E) completas y otras copias de seguridad en los niveles 2, 3 y 4 (B, C y D) son diferenciales.

La rotación de cintas para el esquema ToH depende substancialmente de las opciones de cintas, cuya configuración predeterminada no siempre proporciona un uso óptima de las cintas y de toda la biblioteca de cintas.

El objetivo es elegir las opciones de cintas que requieran una cantidad mínima de cintas en la rotación.

Existen ejemplos analizados que muestran cómo el esquema ToH puede combinarse con diferentes opciones de cintas en las siguientes secciones:

- Ejemplo 1 de ToH (pág. 158) La opción **Utilizar un conjunto de cintas separado** está seleccionada. Todas las opciones de **Utilizar siempre una cinta en blanco** están desactivadas. Requiere 5 cintas en rotación.
- Ejemplo 2 de ToH (pág. 160) La opción **Utilizar un conjunto de cintas separado** está seleccionada. La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa la opción** está seleccionada. Las otras opciones de **Utilizar siempre una cinta en blanco** están desactivadas. Requiere 4 cintas en rotación.
- Ejemplo 3 de ToH (pág. 161) La opción **Utilizar un conjunto de cintas separado** está seleccionada. Todas las opciones de **Utilizar siempre una cinta en blanco** están seleccionadas. Requiere 7 cintas en rotación.

El **Ejemplo 2 de ToH** requiere 4 cintas, que es el mínimo para el caso. Así, la configuración de sus opciones de cintas es la mejor en comparación con la opciones de otros ejemplos.

## Ejemplo 1 de ToH

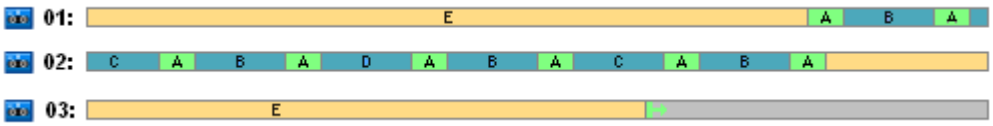
Supongamos que el plan de copia de seguridad tiene las siguientes opciones de cinta:

- La opción **Utilizar un conjunto de cintas separadas** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa** está desactivada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad incremental** está desactivada

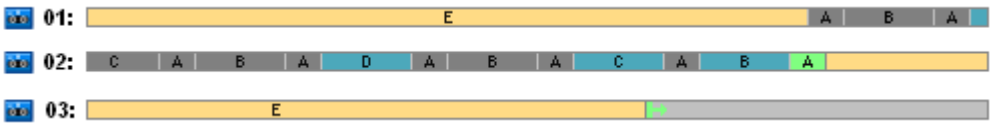
 

- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad diferencial** está desactivada.

La figura a continuación muestra el uso de las cintas para el esquema ToH combinado con las opciones de cintas mencionadas anteriormente. La parte repetida del esquema contiene 16 sesiones de copia de seguridad. La figura muestra el estado del archivo comprimido de la copia de seguridad en el momento en el que la sesión n.º 17 ha terminado.

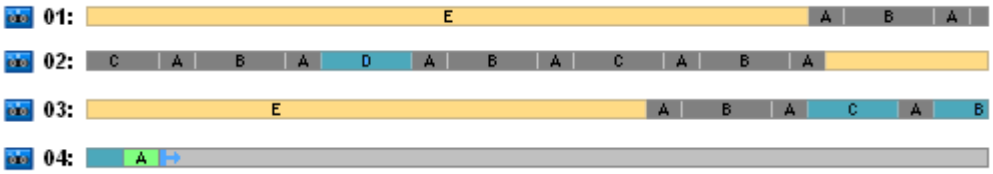



Como el esquema de copia de seguridad Torres de Hanói necesita la presencia de solo una copia de seguridad en cada nivel, todas las copias de seguridad desactualizadas se eliminan automáticamente. En la siguiente figura las copias de seguridad eliminadas están representadas con rectángulos gris oscuro. En realidad, la copia de seguridad eliminada todavía está almacenada en las cintas, pero su información se elimina de la base de datos del nodo de almacenamiento.




La figura muestra la copia de seguridad completa almacenada en la cinta 01 en ese momento, que no puede eliminarse ya que es la base de las copias de seguridad diferenciales (D, C, B) e incrementales (A) almacenadas en la cinta 02. La eliminación de la copia de seguridad completa se posterga hasta que las cuatro copias de seguridad mencionadas anteriormente se eliminen.

La próxima figura muestra el contenido de las cintas en el momento antes de la creación de una nueva copia de seguridad en el nivel D:




En ese momento, el archivo comprimido de datos ocupa cuatro cintas y el tamaño total de las copias de seguridad escritas hasta el momento es el máximo para el ejemplo. Sin embargo, si en el futuro se escribe una copia de seguridad completa al final de una cinta, el archivo comprimido ocupará cinco cintas.

Tras crear la próxima copia de seguridad en el nivel D, la cinta 01 es liberada y puede volver a utilizarse.

Tengamos en cuenta que el esquema Torre de Hanoi (ToH) combinado con las opciones específicas tiene las siguientes propiedades para el caso analizado:

- la última figura muestra que los datos recuperados necesitan la carga y el montaje de hasta tres cintas (una cinta: 16%, dos cintas: 72%, tres cintas: 12%) como también el rebobinado y la lectura de una (6%), dos (50%) o tres (44%) copias de seguridad
- un esquema de cinco niveles necesita hasta cinco cintas para este caso.

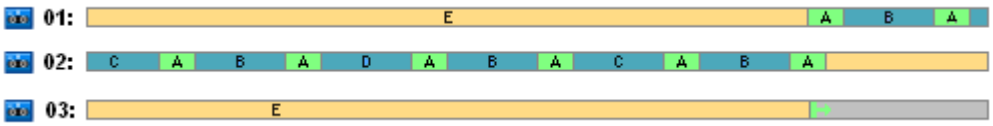
## Ejemplo 2 de ToH

Supongamos que el plan de copia de seguridad tiene las siguientes opciones de cinta:

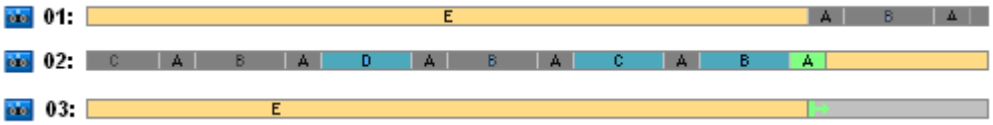
- La opción **Utilizar un conjunto de cintas separadas** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad incremental** está desactivada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad diferencial** está desactivada.

La única diferencia entre el **Ejemplo 2 de ToH** y el **Ejemplo 1 de ToH** es que la opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa la opción** está seleccionada.

La primera figura muestra el uso de cintas para el esquema ToH combinado con las opciones de cintas mencionadas anteriormente. La parte repetida del esquema contiene 16 sesiones de copia de seguridad. La figura muestra el estado del archivo comprimido de la copia de seguridad en el momento en el que la sesión n.º 17 ha terminado.

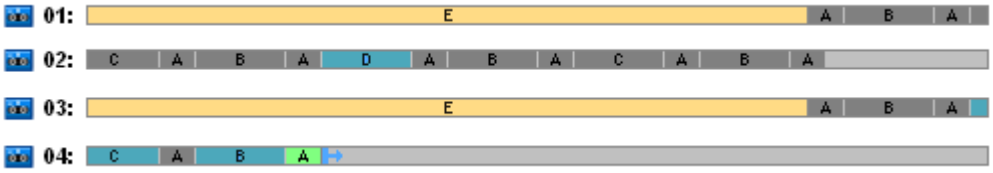



En la figura a continuación, las copias de seguridad eliminadas en ese momento están representadas con rectángulos gris oscuros.




La figura indica que existen dos copias de seguridad completas de nivel E porque en ese momento la primera copias de seguridad completa funciona como base para las copias de seguridad diferenciales D, C y B que funcionan a su vez como base para la copia de seguridad incremental A. Por lo tanto, la eliminación de la copias de seguridad se postergará hasta que no se eliminen las copias de seguridad D, C, B y A.

La próxima figura muestra el uso de cinta en el momento antes de crear una nueva copia de seguridad en el nivel D:




En ese momento, el archivo comprimido de la copia de seguridad ocupa cuatro cintas. Es la cantidad máxima de cintas necesarias en el ejemplo.

Después de que se crea la próxima copia de seguridad en el nivel D, las cintas 01 y 02 se liberan y pueden volver a utilizarse.

Tengamos en cuenta que el esquema Torre de Hanoi (ToH) combinado con las opciones específicas tiene las siguientes propiedades para el caso analizado:

- la recuperación de datos necesita el acceso a las copias de seguridad almacenadas en una (25%) o dos (75%) cintas
- el esquema de cinco niveles puede necesitar hasta cuatro cintas.

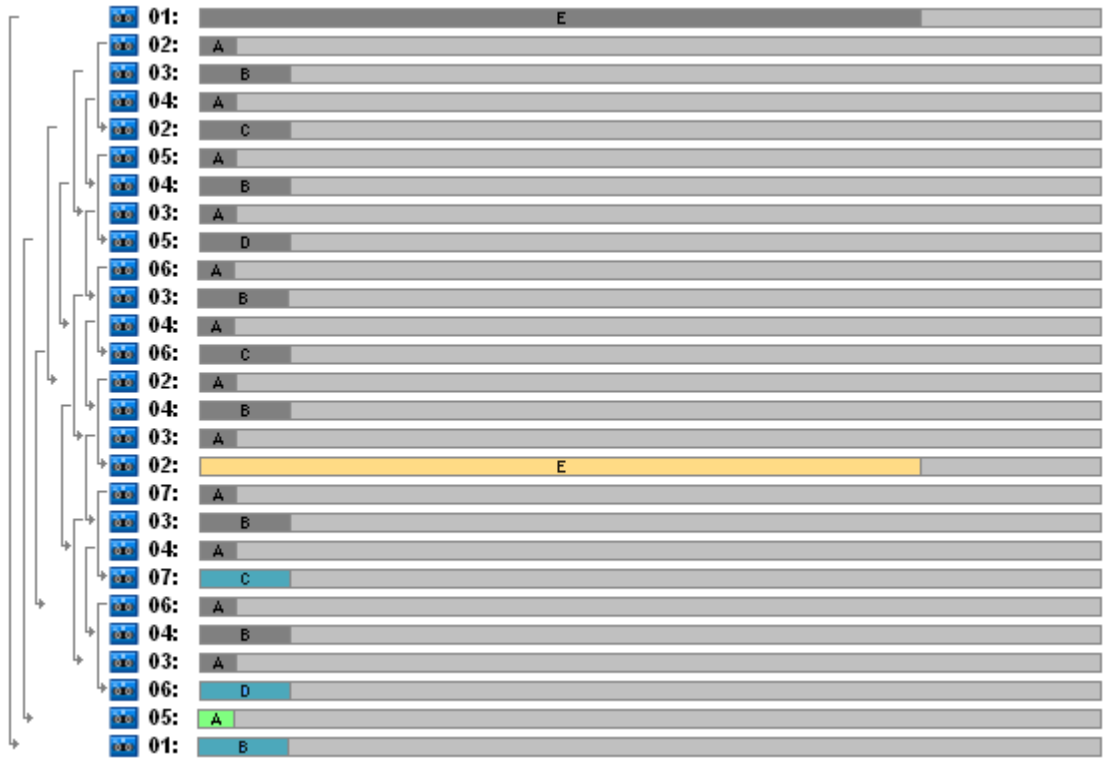
Así, en este caso específico, la selección de la opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa** aumenta considerablemente la eficiencia de la uso de cintas en la biblioteca.

## Ejemplo 3 de ToH

Imaginemos que el plan de copia de seguridad tiene las siguientes opciones de cinta:

- La opción **Utilizar un conjunto de cintas separadas** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad incremental** está seleccionada
- La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad diferencial** está seleccionada.

La figura muestra la rotación de cintas para el esquema ToH con estas opciones.




La cantidad máxima de cintas utilizadas en la rotación es siete, siendo mayor que el esquema ToH clásico de cinco niveles.

Se utilizan dos cintas adicionales para:

1. conservar una copia de seguridad (eliminación postergada) ya que es una base para las copias de seguridad de otros niveles

2. conservar una copia de seguridad anterior en un nivel hasta que se haya creado correctamente una nueva copia de seguridad en el nivel.

El ejemplo demuestra que se reduce la eficiencia del uso de las cintas. Además, la recuperación de datos necesita el acceso a las copias de seguridad almacenadas en una (copias de seguridad completas, 6%), dos (copias de seguridad diferenciales, 44%) o tres (copias de seguridad incrementales, 50%) cintas. Así, la operación lleva en promedio más tiempo que en los ejemplos anteriores.

## Planificación de cintas

Una vez que ha especificado el esquema de copia de seguridad y las opciones de cintas, debe determinar la cantidad mínima de cintas necesarias para conseguir la automatización completa de la rotación de cintas.

Para simplificar la planificación de las cintas, descartemos la posibilidad de que las cintas calculadas puedan contener copias de seguridad de otros datos. Está implícito que la opción **Utilizar un conjunto de cintas separado** está habilitada.

Para calcular la cantidad de cintas debe tener en cuenta las siguientes consideraciones:

- el tamaño de la copia de seguridad completa
- el tamaño medio de las copias de seguridad incrementales
- el tamaño medio de las copias de seguridad diferenciales
- el nivel de compresión especificado para la copia de seguridad de los datos
- el esquema de rotación de cintas (frecuencia de las copias de seguridad, reglas de retención)
- las opciones de adición de cintas
- los requisitos de compatibilidad con archivos comprimidos de cartuchos de cintas externos.

No existe ninguna fórmula común para calcular la cantidad de cintas necesarias en todas las combinaciones posibles de las consideraciones anteriormente mencionadas. Pero la manera general de obtener una cantidad de cintas para un caso incluye los siguientes pasos:

1. Establezca (o escriba) una cadena de copias de seguridad hasta que la primera copia de seguridad pueda eliminarse
2. Tenga en cuenta las opciones de adición de cintas; la cadena puede dividirse en conjuntos de cintas
3. Calcule la cantidad de cintas en cada conjunto de cintas
4. La suma de los valores calculados nos da el número total de cintas que se necesitan en ese caso.

## Planificación de cintas: Ejemplo 1

Imaginemos una situación con las siguientes características:

- El tamaño total de la copia de seguridad completa es **F_GB**
- El tamaño medio de las copias de seguridad incrementales es **I_GB**
- El tamaño medio de las copias de seguridad diferenciales es **D_GB**
- El nivel de compresión proporciona un coeficiente de reducción medio de **CL**
- El esquema de rotación de cintas es **Torres de Hanói** con **cuatro** niveles
- Las opciones de cintas son las siguientes:
  - La opción **Utilizar un conjunto de cintas separadas** está seleccionada

    - La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa** está desactivada
    - La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad incremental** está desactivada
    - La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad diferencial** está desactivada
- El tamaño de la cinta es **T_GB**.

El esquema Torres de Hanói con cuatro niveles (A, B, C y D) especifica la siguiente línea de copias de seguridad en las cintas antes de eliminar la primera copia de seguridad: D (completa), A, B, A, C, A, B, A, D, A, B, A, C. Las opciones de cintas especificadas no requieren el uso de una cinta en blanco para ninguna copia de seguridad, por lo que la línea de copias de seguridad se dividirá automáticamente y continuará en una cinta nueva cuando llegue al final de la cinta actual. Existe un conjunto de cintas para calcular.

Cantidad total de cintas necesarias = redondear ((2*F_GB + 6*I_GB + 5*D_GB) * CL / T_GB) + 1.

El Ejemplo 1 de ToH (pág. 158), descrito anteriormente, está basado en el esquema de copias de seguridad Torres de Hanói de cinco niveles con las mismas opciones de cintas. Su línea de copias de seguridad ha sido la siguiente: E (completa), A, B, A, C, A, B, A, D, A, B, A, C, A, B, A, E, A, B, A, C, A, B, A, D.

Cantidad total de cintas necesarias = redondear ((2*F_GB + 12*I_GB + 11*D_GB) * CL / T_GB) + 1 = redondear ( (2*320 + 12*16 + 11*40) * 1 / 400 ) + 1 = redondear ( 3.18 ) + 1 = 5 (cintas).

## Planificación de cintas: Ejemplo 2

Imaginemos una situación con las siguientes características:

- El tamaño total de la copia de seguridad completa es **F_GB**
- El tamaño medio de las copias de seguridad incrementales es **I_GB**
- El tamaño medio de las copias de seguridad diferenciales es **D_GB**
- El nivel de compresión proporciona un coeficiente de reducción medio de **CL**
- El esquema de rotación de cintas es **Personalizado** con las siguientes configuraciones:
    - **Copia de seguridad completa: cada 10 días**
    - **Copia de seguridad diferencial: cada 2 días**
    - **Copia de seguridad incremental: cada 1 día, cada 6 horas**
    - **Reglas de retención: Eliminar las copias de seguridad que tengan más de 5 días de antigüedad**
- Las opciones de cintas son las siguientes:
    - La opción **Utilizar un conjunto de cintas separado** está seleccionada
    - La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad completa** está seleccionada
    - La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad incremental** está desactivada
    - La opción **Utilizar siempre una cinta en blanco: para cada copia de seguridad diferencial** está desactivada
- El tamaño de la cinta es **T_GB**.

El caso define la línea de copias de seguridad que está formada por dos secciones. La figura siguiente muestra las secciones en el momento antes de que la primera copia de seguridad se elimine. En la

figura, las copias de seguridad completas, diferenciales e incrementales se muestran con rectángulos naranjas, azules y verdes respectivamente.


En ese momento, algunas copias de seguridad se eliminan con la tarea Limpieza. Se posterga la eliminación de copias de seguridad desactualizadas que se muestran con colores oscuros, ya que estas copias de seguridad son básicas para las copias de seguridad reales.


Debido a que la correlación exacta entre el tamaño de la cinta y el tamaño de la copia de seguridad es desconocida, es imposible determinar la cantidad de cintas que estarán en blanco tras la eliminación. Así, el cálculo ignora esta posibilidad.

El conjunto de cintas 01 debería contener (redondear (( F_GB + 4*D_GB + 5*7*I_GB) * CL / T_GB)) cintas para almacenar las copias de seguridad. El conjunto de cintas 02 necesita (redondear (( F_GB + 1*D_GB + 7*I_GB) * CL / T_GB)) cintas. La suma de los valores calculados nos da el número total de cintas que se necesitan en ese caso.

## ¿Qué debo hacer si...?

- **¿Qué debo hacer si tengo que mover cintas con copias de seguridad de una biblioteca de cintas a otra?**

  1. Si ambas bibliotecas de cintas están conectadas al mismo equipo con Acronis Backup & Recovery 10 Storage Node instalado (es decir, las bibliotecas son gestionadas por el mismo nodo de almacenamiento), la base de datos del nodo de almacenamiento tiene toda la información necesaria acerca del contenido de las cintas que se han movido. Entonces, todo lo que tiene que hacer es ejecutar el procedimiento de inventario (pág. 146) para la bóveda gestionada en la biblioteca donde se han ubicado las cintas.
  2. Si mueve cintas a una biblioteca de cintas gestionada por otro nodo de almacenamiento, debe volver a explorar (pág. 146) cada cinta reubicada para suministrar al nodo de almacenamiento información acerca de las copias de seguridad que contiene la cinta.

- **¿Qué debo hacer si necesito utilizar una cinta de la biblioteca de cintas en el dispositivo de cintas local y viceversa?**

  Los agentes de Acronis crean copias de seguridad en cintas en un formato diferente al formato utilizado por el nodo de almacenamiento. Esta es la razón por la cual es imposible intercambiar cintas entre dispositivos de cintas conectados al nodo de almacenamiento y a un equipo gestionado: un agente en un dispositivo de cintas conectado localmente no puede leer una cinta escrita por el nodo de almacenamiento. Sin embargo, el nodo de almacenamiento puede leer cintas escritas por otro agente. Para obtener información completa acerca de la compatibilidad de los formatos de cintas en Acronis Backup & Recovery 10, consulte la tabla Compatibilidad de cintas (pág. 47).

- **¿Qué debo hacer si tengo que volver a instalar el nodo de almacenamiento o conectar la biblioteca de cintas a otro equipo?**

  Instale el nodo de almacenamiento en el equipo al que está conectado la biblioteca de cintas, cree una bóveda centralizada en la biblioteca de cintas y después vuelva a explorar cada cinta que contenga copias de seguridad.

- **¿Qué debo hacer si he perdido mi nodo de almacenamiento y necesito recuperar datos de una cinta?**

  Si sabe cuál es la cinta de la que debe recuperar información y tiene un dispositivo de cintas con una bóveda gestionada por un nodo de almacenamiento, inserte el cartucho de la cinta en el dispositivo, diríjase a la vista **Bóvedas centralizadas** de la consola, seleccione la bóveda, vuelva a explorar la cinta, seleccione el archivo comprimido y la copia de seguridad de la que desea recuperar los datos y cree la tarea de recuperación.

  Si no sabe cuál es la cinta que contiene los datos que desea recuperar, debe volver a explorar cada cinta hasta que encuentre los datos. Generalmente, todos los pasos que debe seguir son los mismos que los mencionados anteriormente, excepto que debe aplicarse una nueva exploración a una cantidad de cintas en lugar de a una sola cinta.

- **¿Qué debo hacer si necesito recuperar datos de una cinta Echo?**

  Utilice la tabla de la sección Tabla de compatibilidad de cintas (pág. 47) para averiguar qué componentes de Acronis Backup & Recovery 10 pueden leer los datos de su cinta.

## 4.2 Bóvedas personales

Una bóveda se denomina personal si fue creada usando una conexión directa entre la consola y un equipo gestionado. Las bóvedas personales son específicas para cada equipo gestionado. Cualquier usuario que pueda registrarse en el sistema puede ver las bóvedas personales. El permiso de un usuario de realizar una copia de seguridad en una bóveda personal está definido por el permiso del usuario para la carpeta o el dispositivo donde está ubicada la bóveda.

Una bóveda personal puede residir en una red compartida, un servidor FTP, un dispositivo extraíble, Acronis Online Backup Storage, un dispositivo de cintas o en una unidad de disco duro local en el equipo. Acronis Secure Zone se considera una bóveda personal disponible para todos los usuarios que puedan iniciar sesión en el sistema. Las bóvedas personales se crean automáticamente al realizar la copia de seguridad en cualquiera de las ubicaciones anteriores.

Las bóvedas personales pueden ser utilizadas por planes de copia de seguridad locales o tareas locales. Los planes de copia de seguridad centralizados no pueden utilizar bóvedas personales, a excepción de Acronis Secure Zone.

### Uso compartido de una bóveda personal

Múltiples equipos pueden encontrarse en la misma ubicación física; por ejemplo, en la misma carpeta compartida. Sin embargo, cada uno de los equipos posee su propio acceso directo al árbol de las **Bóvedas**. Los usuarios que realizan una copia de seguridad en una carpeta compartida pueden ver y gestionar los archivos comprimidos de otros usuarios según sus permisos de acceso para esa carpeta. Para facilitar la identificación de los archivos comprimidos, la vista **Bóveda personal** tiene la columna **Propietario** que muestra el propietario de cada archivo comprimido. Para obtener más información sobre el concepto de propietario, consulte Propietarios y credenciales (pág. 33).

### Metadatos

La carpeta **.meta** se crea durante la creación de la copia de seguridad en cada una de las bóvedas personales. Esta carpeta contiene información adicional sobre los archivos comprimidos y las copias de seguridad almacenados en la bóveda, como los propietarios de los archivos o el nombre del equipo. Si elimina accidentalmente la carpeta .meta, esta se creará nuevamente de manera automática la próxima vez que acceda a la bóveda. Pero es posible que se pierda alguna información, como los nombres de los propietarios y los nombres de los equipos.

### 4.2.1 Cómo trabajar con la vista "Bóveda personal"

Esta sección describe brevemente los principales elementos de la vista **Bóveda personal** y sugiere formas de trabajar con ellos.

#### Barra de herramientas de la bóveda

La barra de herramientas contiene botones operacionales que le permiten realizar operaciones con la bóveda personal seleccionada. Consulte la sección Acciones en bóvedas personales (pág. 167) para obtener más información.

#### Gráfico circular con leyenda

El **gráfico circular** le permite estimar la carga de la bóveda: muestra la proporción entre el espacio libre y el espacio ocupado de la bóveda.

- espacio libre: espacio en el dispositivo de almacenamiento donde está ubicada la bóveda. Por ejemplo, si la bóveda está ubicada en un disco duro, el espacio libre de la bóveda es el espacio libre del volumen correspondiente.

- espacio ocupado: el tamaño total de los archivos de copia de seguridad y sus metadatos, si están ubicados en la bóveda. No se tienen en cuenta otros archivos que un usuario pueda colocar en esta carpeta.

La **leyenda** muestra la siguiente información sobre la bóveda:

- ruta completa a la bóveda,
- cantidad total de archivos comprimidos y copias de seguridad almacenados en la bóveda,
- proporción entre el espacio ocupado y el tamaño de los datos originales.

#### Contenido de la bóveda

La sección **Contenido de la bóveda** contiene la tabla y la barra de herramientas de archivos comprimidos. La tabla de archivos comprimidos muestra los archivos comprimidos y las copias de seguridad almacenados en la bóveda. Utilice la barra de herramientas de archivos comprimidos para realizar acciones en los archivos comprimidos y copias de seguridad seleccionados. La lista de copias de seguridad se expande al hacer clic en el signo "más" ubicado a la izquierda del nombre del archivo comprimido. Todos los archivos comprimidos están agrupados por tipo en las siguientes pestañas:

- La pestaña **Archivos comprimidos del disco** enumera todos los archivos comprimidos que contienen copias de seguridad del disco o volumen (imágenes).
- La pestaña **Archivos comprimidos de archivos** enumera todos los archivos comprimidos que contienen copias de seguridad de archivos.

**Secciones relacionadas:**

Operaciones con archivos comprimidos almacenados en una bóveda (pág. 169)

Operaciones con copias de seguridad (pág. 169)

Filtrado y ordenamiento de archivos comprimidos (pág. 171)

#### Barras del panel "Acciones y herramientas"

- **[Nombre de la bóveda]** La barra **Acciones** está disponible al hacer clic en la bóveda en el árbol de bóvedas. Duplica las acciones de la barra de herramientas de la bóveda.

- **[Nombre del archivo comprimido]** La barra **Acciones** está disponible al seleccionar un archivo comprimido en la tabla de archivos comprimidos. Duplica las acciones de la barra de herramientas de archivos comprimidos.
- **[Nombre de la copia de seguridad]** La barra **Acciones** está disponible al expandir el archivo comprimido y hacer clic en cualquiera de sus copias de seguridad. Duplica las acciones de la barra de herramientas de archivos comprimidos.

### 4.2.2 Acciones en bóvedas personales

***Para acceder a las acciones***

1. Conecte la consola en el servidor de gestión.
2. En el panel de **Navegación**, haga clic en **Bóvedas** > **>Personal**.

Todas las operaciones descritas aquí se realizan al hacer clic en los botones correspondientes de la barra de herramientas de las bóvedas. También es posible acceder a estas operaciones desde el elemento acciones de **[nombre de la bóveda]** del menú principal.

La siguiente es una guía para realizar operaciones con bóvedas personales.

| Para | Realizar |
|---|---|
| Crear una bóveda personal | Haga clic en **Crear**.<br>El procedimiento de creación de bóvedas personales se describe en profundidad en la sección Creación de una bóveda personal (pág. 168). |
| Edición de una bóveda | 1. Seleccione la bóveda.<br>2. Haga clic en **Editar**.<br>La página **Edición de bóveda personal** permite editar el nombre y la información de la bóveda en el campo **Comentarios**. |
| Cambiar la cuenta de usuario para acceder a una bóveda | Haga clic en **Cambiar usuario**.<br>En el cuadro de diálogo que aparece, proporcione las credenciales necesarias para acceder a la bóveda. |
| Crear Acronis Secure Zone | Haga clic en **Crear Acronis Secure Zone**.<br>El procedimiento de creación de Acronis Secure Zone se describe en profundidad en la sección Creación de Acronis Secure Zone (pág. 271). |
| Explorar el contenido de una bóveda | Haga clic en **Explorar**.<br>En la ventana Explorar que aparece, examine el contenido de la bóveda seleccionada. |
| Validar una bóveda | Haga clic en **Validar**.<br>Pasará a la página Validación (pág. 255), en donde esta bóveda ya estará preseleccionada como origen. La validación de la bóveda verifica todos los archivos comprimidos almacenados en la bóveda. |
| Eliminar una bóveda | Haga clic en **Eliminar**.<br>La operación de eliminación en realidad solo quita el acceso directo a la carpeta desde la vista **Bóvedas**. La carpeta en sí permanece intacta. Tiene la opción de conservar o eliminar los archivos comprimidos incluidos en la carpeta. |
| Actualizar la información de la tabla de bóvedas | Haga clic en **Actualizar**. |

| | |
|---|---|
| | Mientras revisa el contenido de la bóveda, pueden añadirse archivos comprimidos a la bóveda, como también eliminarse o modificarse. Haga clic en **Actualizar** para actualizar la información de la bóveda con los cambios más recientes. |

## Creación de una bóveda personal

***Para crear una bóveda personal***

1. En el campo **Nombre**, introduzca un nombre para la bóveda que se está creando.
2. [Opcional] En el campo **Comentarios**, añada una descripción de la bóveda.
3. En el campo **Ruta**, haga clic en **Cambiar...**
   En la ventana **Ruta de la bóveda personal** que se abre, especifique una ruta a la carpeta que se usará como la bóveda. Una bóveda personal puede organizarse en un medio extraíble o separable, en una red de intercambio, o en un FTP.
4. Haga clic en **Aceptar**. Como resultado, la bóveda creada aparecerá en el grupo **Personales** del árbol de bóvedas.

## Combinación y movimiento de bóvedas personales

***¿Qué sucede si necesito mover la bóveda existente de un lugar a otro?***

Haga lo siguiente

1. Asegúrese de que ninguno de los planes de copia de seguridad utilice la bóveda existente mientras mueve los archivos o deshabilita temporalmente (pág. 201) los programas de los planes en cuestión.
2. Mueva la carpeta de la bóveda con todos sus archivos comprimidos a un nuevo lugar manualmente mediante un administrador de archivos de terceros.
3. Cree una nueva bóveda.
4. Edite los planes y las tareas de la copia de seguridad: redirija su destino a la nueva bóveda.
5. Elimine la bóveda anterior.

***¿Cómo puedo combinar dos bóvedas?***

Supongamos que tiene dos bóvedas, *A* y *B*, en uso. Los planes de copia de seguridad utilizan ambas bóvedas. Decide dejar solo la bóveda *B* y mover allí todos los archivos comprimidos de la bóveda *A*.

Para eso, haga lo siguiente

1. Asegúrese de que ninguno de los planes de copia de seguridad utilice la bóveda *A* mientras realiza la combinación o deshabilita temporalmente (pág. 201) los programas de los planes en cuestión.
2. Mueva los archivos comprimidos a la bóveda *B* manualmente mediante un administrador de archivos de terceros.
3. Edite los planes de copia de seguridad que utilizan la bóveda *A*: redirija su destino a la bóveda *B*.
4. En el árbol de bóvedas, seleccione la bóveda *B* para verificar si se muestran los archivos comprimidos. Si no aparecen, haga clic en **Actualizar**.
5. Elimine la bóveda *A*.

## 4.3 Operaciones comunes

### 4.3.1 Operaciones con archivos comprimidos almacenados en una bóveda

Para realizar cualquier operación con un archivo comprimido, primero deberá seleccionarlo. Si el archivo comprimido está protegido con una contraseña, se le solicitará que la introduzca.

Todas las operaciones descritas a continuación se realizan haciendo clic en los botones correspondientes de la barra de herramientas. También es posible acceder a estas operaciones desde la barra **Acciones de [nombre del archivo comprimido]** (en el panel **Acciones y herramientas**) y desde el elemento **Acciones de [nombre del archivo comprimido]** del menú principal respectivamente.

La siguiente es una guía para realizar operaciones con los archivos comprimidos almacenados en una bóveda.

| Operación | Procedimiento |
|---|---|
| Validar un archivo comprimido | Haga clic en **Validar**.<br>La página **Validación** (pág. 255) se abrirá con el archivo comprimido preseleccionado como origen.<br>La validación de un archivo comprimido verificará todas las copias de seguridad del archivo comprimido. |
| Exportación de archivos comprimidos | Haga clic en **Exportar**.<br>La página **Exportar** (pág. 264) se abrirá con el archivo comprimido preseleccionado como origen. La exportación de un archivo comprimido crea un duplicado del mismo con todas sus copias de seguridad en la ubicación que se especifique. |
| Eliminar un solo archivo comprimido o varios archivos comprimidos | 1. Seleccione los archivos comprimidos o uno de los archivos comprimidos que desee eliminar.<br>2. Haga clic en **Eliminar**.<br>El programa duplica la selección en la ventana **Eliminación de copias de seguridad** (pág. 171) que tiene casillas de verificación para cada archivo comprimido y cada copia de seguridad. Revise la selección y efectúe las correcciones necesarias (seleccione las casillas de verificación de los archivos comprimidos deseados) y después confirme la eliminación. |
| Eliminar todos los archivos comprimidos de la bóveda | Tenga en cuenta que si se aplicaron filtros a la lista de bóvedas, verá solo una parte del contenido de la bóveda. Asegúrese de que la bóveda no contenga archivos comprimidos que necesite conservar antes de iniciar la operación.<br>Haga clic en **Eliminar todo**.<br>El programa duplica la selección en la nueva ventana que tiene casillas de verificación para cada archivo comprimido y cada copia de seguridad. Revise la selección y efectúe las correcciones necesarias, y después confirme la eliminación. |

### 4.3.2 Operaciones con copias de seguridad

Para realizar cualquier operación con una copia de seguridad, primero deberá seleccionarla. Para seleccionar una copia de seguridad, expanda el archivo comprimido y después haga clic en la copia

de seguridad. Si el archivo comprimido está protegido con una contraseña, se le solicitará que la introduzca.

Todas las operaciones descritas a continuación se realizan haciendo clic en los botones correspondientes de la barra de herramientas. También es posible acceder a estas operaciones desde la barra **Acciones de "[nombre de la copia de seguridad]"** (en el panel **Acciones y herramientas**) y desde el elemento **Acciones de "[nombre de la copia de seguridad]"** del menú principal.

La siguiente es una guía para realizar operaciones con copias de seguridad.

| Operación | Procedimiento |
|---|---|
| Ver el contenido de la copia de seguridad en una ventana separada | Haga clic en **Ver contenido**.<br>En la ventana **Contenido de la copia de seguridad**, examine el contenido de la copia de seguridad. |
| Recuperar | Haga clic en **Recuperar**.<br>La página **Recuperar datos** se abrirá con la copia de seguridad preseleccionada como origen. |
| Recuperar un disco/volumen como un equipo virtual | Haga clic con el botón secundario en la copia de seguridad del disco y después seleccione **Recuperar como equipo virtual**.<br>La página **Recuperar datos** se abrirá con la copia de seguridad preseleccionada como origen. Seleccione la ubicación y el tipo de equipo virtual nuevo, y después continúe como si se tratara de una recuperación de disco o volumen regular. |
| Validar una copia de seguridad | Haga clic en **Validar**.<br>La página **Validación (pág. 255)** se abrirá con la copia de seguridad preseleccionada como origen. La validación de la copia de seguridad de un archivo imita la recuperación de todos los archivos de la copia de seguridad en un destino simulado. La validación de la copia de seguridad de un disco calcula la suma de comprobación por cada bloque de datos guardado en la copia de seguridad. |
| Exportación de una copia de seguridad | Haga clic en **Exportar**.<br>La página **Exportar** (pág. 264) se abrirá con la copia de seguridad preseleccionada como origen. La exportación de una copia de seguridad crea un nuevo archivo comprimido con una copia autosuficiente de la copia de seguridad en la ubicación que se especifique. |
| Eliminar una sola o varias copias de seguridad | Seleccione una de las copias de seguridad que desee eliminar y después haga clic en **Eliminar**.<br>El programa duplica la selección en la ventana **Eliminación de copias de seguridad** (pág. 171) que tiene casillas de verificación para cada archivo comprimido y cada copia de seguridad. Revise la selección y efectúe las correcciones necesarias (seleccione las casillas de verificación de las copias de seguridad deseadas) y después confirme la eliminación. |
| Eliminar todos los archivos comprimidos y las copias de seguridad de la bóveda | Tenga en cuenta que si se aplicaron filtros a la lista de bóvedas, verá solo una parte del contenido de la bóveda. Asegúrese de que la bóveda no contenga archivos comprimidos que necesite conservar antes de iniciar la operación.<br>Haga clic en **Eliminar todo**.<br>El programa duplica la selección en la ventana **Eliminación de copias de seguridad** (pág. 171) que tiene casillas de verificación para cada archivo comprimido y cada copia de seguridad. Revise la selección y efectúe las correcciones necesarias, y después confirme la eliminación. |

### 4.3.3 Eliminación de archivos comprimidos y copias de seguridad

La ventana **Eliminación de copias de seguridad** muestra la misma pestaña que la vista de las bóvedas, pero con casillas de verificación para cada archivo comprimido y copia de seguridad. El archivo comprimido o la copia de seguridad que eligió eliminar tienen la marca de verificación. Revise el archivo comprimido o la copia de seguridad que seleccionó para eliminar. Si necesita eliminar otros archivos comprimidos y copias de seguridad, seleccione las casillas de verificación respectivas y después haga clic en **Eliminar seleccionados** y confirme la eliminación.

Los filtros de esta ventana provienen de la lista de archivos comprimidos de la vista de bóvedas. Por lo tanto, si se aplicaron algunos filtros a la lista de archivos comprimidos, aquí se mostrarán solo los archivos comprimidos y las copias de seguridad correspondientes a estos filtros. Para ver todo el contenido, limpie todos los campos de los filtros.

#### ¿Qué sucede si elimino una copia de seguridad que es la base de una copia de seguridad incremental o diferencial?

Para conservar la consistencia de los archivos comprimidos, el programa consolidará las dos copias de seguridad. Por ejemplo, elimina una copia de seguridad completa, pero retiene la siguiente incremental. Las copias de seguridad se combinarán en una sola copia de seguridad completa que tendrá la fecha de la copia de seguridad incremental. Cuando elimina una copia de seguridad incremental o diferencial desde la mitad de la cadena, el tipo de copia de seguridad resultante será incremental.

Tenga en cuenta que la consolidación es solo un método para eliminar y no una alternativa a la eliminación. La copia de seguridad resultante no tendrá los datos que estaban en la copia de seguridad eliminada y que no estaban en la copia de seguridad incremental o diferencial retenida.

Debe haber suficiente espacio en la bóveda para los archivos temporales creados durante la consolidación. Las copias de seguridad resultantes de la consolidación siempre usarán la compresión máxima.

### 4.3.4 Filtrado y ordenamiento de archivos comprimidos

La siguiente es una guía para filtrar y ordenar archivos comprimidos en la tabla de archivos comprimidos.

| Para | Haga lo siguiente |
|---|---|
| Ordenar los archivos de copia de seguridad por cualquier columna | Haga clic en el encabezado de la columna para ordenar los archivos comprimidos en orden ascendente.<br>Haga clic nuevamente sobre este para ordenar los archivos comprimidos en orden descendente. |
| Filtrar los archivos por nombre, propietario o equipo | En el campo ubicado debajo del encabezado de la columna correspondiente, escriba el nombre del archivo comprimido (el nombre del propietario o del equipo).<br>Como resultado, verá la lista de archivos comprimidos cuyos nombres (nombres de los propietarios o de los equipos) coinciden total o solo parcialmente con el valor introducido. |

#### Configuración de la tabla de archivos comprimidos

De manera predeterminada, la tabla muestra siete columnas, las otras están ocultas. De ser necesario, puede ocultar las columnas que se muestran y mostrar las ocultas.

### *Mostrar u ocultar columnas*

1. Haga clic con el botón derecho en el encabezado de cualquier columna para abrir el menú contextual. Los elementos del menú que no estén seleccionados corresponden a los encabezados de las columnas presentadas en la tabla.
2. Haga clic sobre los elementos que quiera mostrar/ocultar.

# 5 Programación

El programador de Acronis ayuda a que el administrador adapte los planes de copia de seguridad a la rutina diaria de la empresa y al estilo de trabajo de cada empleado. Las tareas de los planes se iniciarán de forma sistemática y los datos importantes estarán protegidos.

El programador usa la hora local del equipo donde se encuentra el plan de copia de seguridad. Antes de crear una programación, asegúrese de que la configuración de fecha y hora del equipo sea correcta.

### Programación

Para definir cuándo se debe ejecutar una tarea, tendrá que especificar uno o varios sucesos. La tarea se iniciará ni bien ocurran los sucesos. En la siguiente tabla se enumeran los sucesos disponibles para el sistema operativo Windows.

| Suceso |
|---|
| Período: diariamente, semanalmente, mensualmente |
| Tiempo transcurrido desde que se completó correctamente la última copia de seguridad<br>(especifique la duración) |
| Inicio de sesión del usuario<br>(cualquier usuario, usuario actual, especifique la cuenta de usuario) |
| Usuario desconectado*<br>(cualquier usuario, usuario actual, especifique la cuenta de usuario)<br>*Apagar no es lo mismo que desconectar la sesión. La tarea no se ejecutará como un apagado del sistema. |
| Inicio del sistema |
| Cambio en el espacio libre<br>(especifique la cantidad de espacio libre que se cambió en cualquiera de los volúmenes seleccionados para realizar una copia de seguridad o que contienen los datos seleccionados para realizar la copia) |
| Suceso en el registro de sucesos de Windows<br>(especifique los parámetros del suceso) |
| Cuando se produzca una alerta de Acronis Drive Monitor |

### Condición

Para operaciones de copia de seguridad únicamente, puede especificar una o varias condiciones además de los sucesos. Cuando ocurre alguno de los sucesos, el programador verifica la condición y ejecuta la tarea si la condición se cumple. En el caso de varias condiciones, deben cumplirse todas simultáneamente para que se ejecute la tarea. En la siguiente tabla se enumeran las condiciones disponibles para el sistema operativo Windows.

| Condición: ejecute la tarea solo si |
|---|
| El usuario está inactivo (se está ejecutando el protector de pantalla o el equipo está bloqueado). |
| El servidor de ubicación no está disponible |
| El horario de ejecución de la tarea se encuentra dentro del intervalo especificado. |

| |
|---|
| Todos los usuarios cerraron la sesión. |
| Transcurrió el período especificado desde que la última copia de seguridad se completó correctamente. |

En caso de que el suceso ocurra, pero la condición (o alguna de ellas) no se cumpla, el comportamiento del programador estará definido por la opción de copia de seguridad Condiciones de inicio de la tarea (pág. 115).

### Posibles situaciones

- **¿Qué sucede si ocurre un suceso (y se cumple una condición, si la hubiera) mientras la ejecución de la tarea anterior no se completó?**

  Se omitirá el suceso.
- **¿Qué sucede si ocurre un suceso mientras el programador está esperando que se cumpla la condición necesaria para el suceso anterior?**

  Se omitirá el suceso.
- **¿Qué sucede si la condición no se cumple durante un tiempo prolongado?**

  Si retrasar la copia de seguridad resulta riesgoso, puede forzar la condición (pedir a los usuarios que cierren la sesión) o ejecutar la tarea manualmente. Para solucionar la situación de forma automática, puede establecer el intervalo después del cual la tarea se ejecutará, independientemente de la condición.

## 5.1 Programación diaria

La programación diaria es eficaz tanto para los sistemas operativos Windows como Linux.

***Para especificar una programación diaria:***

En el área **Programar**, seleccione el parámetro apropiado de la siguiente manera:

| | |
|---|---|
| **Cada: <...> día(s)** | Establezca la cantidad de días que desea que transcurra entre la ejecución de las tareas. Por ejemplo, si establece Cada 2 día(s), la tarea se iniciará día de por medio. |

En el área **Durante el día ejecute la tarea...**, seleccione una de las siguientes opciones:

| | |
|---|---|
| **Una vez a las: <...>** | Establezca la hora en la cual se ejecutará la tarea una vez. |
| **Cada: <...>**<br>**Desde: <...>**<br>**Hasta: <...>** | Establezca la cantidad de veces que se reiniciará la tarea durante el intervalo especificado. Por ejemplo, si establece la frecuencia de la tarea como Cada 1 hora Desde 10:00:00 hasta 22:00:00, la tarea se ejecutará 12 veces: desde las 10:00 hasta las 22:00 durante un día. |

En el área **Vigente...**, establezca las siguientes opciones:

| | |
|---|---|
| **Desde: <...>** | Establezca una fecha para que se habilite esta programación (una fecha de entrada en vigencia). Si se desmarca esta casilla de verificación, la tarea se iniciará el día y la hora más próximos a los que especificó anteriormente. |
| **Hasta: <...>** | Establezca una fecha para que se deshabilite esta programación. Si se desmarca esta casilla de verificación, la tarea se ejecutará durante una cantidad indefinida de días. |

La configuración de programación avanzada (pág. 181) está disponible únicamente para equipos registrados en Acronis Backup & Recovery 10 Management Server. Para especificar esta configuración, haga clic en **Cambiar** en el área **Ajustes avanzados**.

Toda la configuración se muestra en el campo **Resultado** en la parte inferior de la ventana.

## Ejemplos

**Programación diaria "Simple"**

Se ejecuta la tarea todos los días a las 18:00.

Los parámetros de programación se establecen de la siguiente manera:

1. Cada: **1** día(s).
2. Una vez a las: **18:00:00.**
3. Vigente:

   Desde: **no establecido**. La tarea se iniciará en el día actual, si se creó antes de las 18:00. Si creó la tarea después de las 18:00, se iniciará por primera vez al día siguiente a las 18:00.

   Hasta: **no establecido**. La tarea se llevará a cabo durante una cantidad indefinida de días.

**Programación "Intervalo de tres horas durante tres meses"**

Ejecutar la tarea cada tres horas. La tarea se inicia en una fecha determinada (digamos, 15 de septiembre de 2009) y termina al cabo de tres meses.

Los parámetros de programación se establecen de la siguiente manera:

1. Cada: **1** día(s).
2. Cada: **3** horas

   Desde: **12:00:00.** (medianoche) Hasta: **21:00:00**: en este caso, la tarea se realizará 8 veces por día con un intervalo de 3 horas. Después de la última repetición diaria a las 21:00, llega el día siguiente y la tarea vuelve a comenzar desde la medianoche.
3. Vigente:

   Desde: **15/09/09**. Si 15 de septiembre de 2009 es la fecha actual de creación de la tarea y, digamos, 13:15 es la hora de creación, la tarea se iniciará cuando llegue el intervalo más próximo: a las 15:00 en nuestro ejemplo.

   Hasta: **15/12/09**. En esta fecha la tarea se llevará acabo por última vez, pero continuará disponible en la vista **Tareas**.

**Varias programaciones diarias para una tarea**

En algunos casos, es posible que necesite que la tarea se ejecute varias veces por día, o incluso varias veces por día con intervalos distintos. En esas ocasiones, sería conveniente añadir varias programaciones para una única tarea.

Por ejemplo, supongamos que la tarea debe ejecutarse cada 3 días, desde el 20/09/09, cinco veces por día:

- por primera vez a las 08:00.
- por segunda vez a las 00:00. (mediodía)
- por tercera vez a las 15:00.
- por cuarta vez a las 17:00
- por quinta vez a las 19:00.

Lo más obvio es añadir cinco programaciones simples. Si lo analiza un minuto, seguro se le ocurrirá una manera más conveniente. Como puede ver, el intervalo entre la primera y la segunda repetición de la tarea es de 4 horas y entre la tercera, la cuarta y la quinta es de 2 horas. En este caso, la manera más conveniente es añadir dos programaciones a la tarea.

**Primera programación diaria**

1. Cada: **3** día(s).
2. Cada: **4** horas.
   Desde: **08:00:00.** Hasta: **12:00:00.**
3. Vigente:
   Desde: **09/20/2009**.
   Hasta: **no establecido**.

**Segunda programación diaria**

1. Cada: **3** día(s).
2. Cada: **2** hora(s).
   Desde: **15:00:00.** Hasta: **19:00:00.**
3. Vigente:
   Desde: **09/20/2009**.
   Hasta: **no establecido**.

## 5.2 Programación semanal

La programación semanal es eficaz tanto para los sistemas operativos Windows como de Linux.

***Para especificar una programación semanal:***

En el área **Programar**, seleccione el parámetro apropiado de la siguiente manera:

| | |
|---|---|
| **Cada: <...> semana(s) el: <...>** | Especifique una cantidad de semanas y los días en los que desea que se ejecute la tarea. Por ejemplo: con la configuración Cada **2** semana(s) el **Lun** la tarea se realizará lunes de por medio. |

En el área **Durante el día ejecute la tarea...**, seleccione una de las siguientes opciones:

| | |
|---|---|
| **Una vez a las: <...>** | Establezca la hora en la cual se ejecutará la tarea una vez. |
| **Cada: <...>**<br>**Desde: <...>**<br>**Hasta: <...>** | Establezca la cantidad de veces que se ejecutará la tarea durante el intervalo especificado. Por ejemplo: si establece la frecuencia de la tarea como Cada **1** hora Desde **10:00:00** hasta **22:00:00**, la tarea se llevará a cabo 12 veces desde las 10:00 hasta las 22:00 durante un día. |

En el área **Vigente...**, establezca las siguientes opciones:

| | |
|---|---|
| **Desde: <...>** | Establezca una fecha para que se habilite esta programación (una fecha de entrada en vigencia). Si se desmarca esta casilla de verificación, la tarea se iniciará el día y la hora más próximos a los que especificó anteriormente. |
| **Hasta: <...>** | Establezca una fecha para que se deshabilite esta programación. Si se desmarca esta casilla de verificación, la tarea se llevará a cabo durante una cantidad indefinida de semanas. |

La configuración de programación avanzada (pág. 181) está disponible únicamente para equipos registrados en Acronis Backup & Recovery 10 Management Server. Para especificar esta configuración, haga clic en **Cambiar** en el área **Ajustes avanzados**.

Toda la configuración se muestra en el campo **Resultado** en la parte inferior de la ventana.

## Ejemplos

**Programación "Un día de la semana"**

La tarea se ejecuta todos los viernes a las 10 p. m., se inicia un día en particular (digamos, 14/05/09) y finaliza al cabo de seis meses.

Los parámetros de programación se establecen de la siguiente manera:

1. Cada: **1** semana(s) los: **Vier**.
2. Una vez a las: **10:00:00 p. m**.
3. Vigente:

   Desde las: **13/05/09**. La tarea se iniciará el viernes siguiente a las 10 p. m.

   Hasta: **13/11/09**. La tarea se realizará por última vez en esta fecha, pero continuará disponible en la vista Tareas pasada esta fecha. (Si la fecha no cayera un viernes, la tarea se realizaría por última vez el viernes anterior a esa fecha).

Esta programación se utiliza comúnmente cuando se crea un esquema de copia de seguridad personalizado. La programación similar a "Un día de la semana" se añade a las copias de seguridad completas.

**Programación "Días hábiles"**

Ejecute la tarea todas las semanas los días hábiles: de lunes a viernes. Durante un día hábil, la tarea se inicia sólo una vez a las 21:00.

Los parámetros de programación se establecen de la siguiente manera:

1. Cada: **1** semana(s) los: **<Días hábiles>**: al seleccionar la casilla de verificación <Días hábiles> se marcarán automáticamente las casillas de verificación correspondientes (**Lun**, **Mar**, **Miér**, **Jue** y **Vier**) y las demás quedarán como están.
2. Una vez a las: **21:00:00.**
3. Vigente:

   Desde: **vacío**. Si creó la tarea, digamos, el lunes a las 11:30, se iniciará por primera vez el mismo día a las 21:00. Si creó la tarea, digamos, el viernes después de las 21:00, esta se iniciará por primera vez el siguiente día hábil (en nuestro ejemplo, el lunes) a las 21:00.

   Fecha de finalización: **vacío**. La tarea se reiniciará durante una cantidad indefinida de semanas.

Esta programación se utiliza comúnmente cuando se crea un esquema de copia de seguridad personalizado. La programación "Días hábiles" se añade a las copias de seguridad incrementales, mientras que las copias de seguridad completas se programan para realizarse un día de la semana. Para obtener más información, consulte el ejemplo de copias de seguridad completas e incrementales más limpieza en la sección Esquema de copia de seguridad personalizado (pág. 229).

**Varias programaciones semanales para una tarea**

En los casos en los que la tarea deba llevarse a cabo en diferentes días de las semanas con intervalos distintos, sería conveniente añadir una programación dedicada para cada día de la semana deseado, o para varios días.

Por ejemplo, si necesita que la tarea se ejecute con la siguiente programación:

- Lunes: dos veces, a las 00:00 (mediodía) y a las 21:00
- Martes: cada 3 horas, de 09:00 a 21:00
- Miércoles: cada 3 horas, de 09:00 a 21:00

- Jueves: cada 3 horas, de 09:00 a 21:00
- Viernes: dos veces, a las 00:00 y a las 21:00 (es decir, igual que los lunes)
- Sábado: una vez a las 21:00
- Domingo: una vez a las 21:00

Al combinar los horarios iguales, se pueden añadir las tres programaciones siguientes a la tarea:

**Primera programación**

1. Cada: **1** semana(s) los: **Lun**, **Vier**.
2. Cada: **9** horas
   Desde: **00:00:00.** Hasta: **21:00:00**.
3. Vigente:
   Desde: **no establecido**.
   Hasta: **no establecido**.

**Segunda programación**

1. Cada **1** semana(s) los: **Mar**, **Miér**, **Jue**.
2. Cada **3** horas
   Desde **09:00:00.** Hasta **21:00:00**.
3. Vigente:
   Desde: **no establecido**.
   Hasta: **no establecido**.

**Tercera programación**

1. Cada: **1** semana(s) los: **Sáb, Dom**.
2. Una vez a las: **21:00:00**.
3. Vigente:
   Desde: **no establecido**.
   Hasta: **no establecido**.

## 5.3 Programación mensual

La programación mensual es eficaz tanto para los sistemas operativos Windows como Linux.

***Para especificar una programación mensual:***

En el área **Programar**, seleccione el parámetro apropiado de la siguiente manera:

| | |
|---|---|
| **Meses: <...>** | Seleccione los meses en los que desea ejecutar la tarea. |
| **Días: <...>** | Seleccione los días específicos en el mes para llevar a cabo la tarea. También puede seleccionar el último día del mes, independientemente de cuál sea la fecha. |
| **Los: <...> <...>** | Seleccione los días específicos de las semanas para ejecutar la tarea. |

En el área **Durante el día ejecute la tarea...**, seleccione una de las siguientes opciones:

| | |
|---|---|
| **Una vez a las: <...>** | Establezca la hora en la cual se ejecutará la tarea una vez. |

| | |
|---|---|
| **Cada: <...>**<br>**Desde: <...>**<br>**Hasta: <...>** | Establezca la cantidad de veces que se ejecutará la tarea durante el intervalo especificado. Por ejemplo: si establece la frecuencia de la tarea como Cada **1** hora Desde **10:00:00** hasta **22:00:00**, la tarea se llevará a cabo 12 veces desde las 10:00 hasta las 22:00 durante un día. |

En el área **Vigente...**, establezca las siguientes opciones:

| | |
|---|---|
| **Desde: <...>** | Establezca una fecha para que se habilite esta programación (una fecha de entrada en vigencia). Si se desmarca esta casilla de verificación, la tarea se iniciará el día y la hora más próximos a los que especificó anteriormente. |
| **Hasta: <...>** | Establezca una fecha para que se deshabilite esta programación. Si se desmarca esta casilla de verificación, la tarea se ejecutará durante una cantidad indefinida de meses. |

La configuración de programación avanzada (pág. 181) está disponible únicamente para equipos registrados en Acronis Backup & Recovery 10 Management Server. Para especificar esta configuración, haga clic en **Cambiar** en el área **Ajustes avanzados**.

Toda la configuración se muestra en el campo **Resultado** en la parte inferior de la ventana.

## Ejemplos

**Programación "Último día de cada mes"**

Ejecute la tarea una vez a las 22:00 durante el último día de cada mes.

Los parámetros de programación se establecen de la siguiente manera:

1. Meses: **<Todos los meses>**.
2. Días: **Último**. La tarea se ejecutará el último día de cada mes, independientemente de cuál sea la fecha.
3. Una vez a las: **22:00:00**.
4. Vigente:
   Desde: **vacío**.
   Hasta: **vacío**.

Esta programación se utiliza comúnmente cuando se crea un esquema de copia de seguridad personalizado. La programación "Último día de cada mes" se añade a las copias de seguridad completas, mientras que las copias de seguridad diferenciales se programan para realizarse una vez por semana y las incrementales, los días hábiles. Para obtener más información, consulte el ejemplo de Copias de seguridad completas mensuales, diferenciales semanales e incrementales diarias más limpieza en la sección Esquema de copia de seguridad personalizado (pág. 229).

**Programación "Estación"**

La tarea se ejecuta todos los días hábiles durante las estaciones de otoño de 2009 y 2010 (para el hemisferio norte). Durante un día hábil, la tarea se realiza cada 6 horas desde las 12:00 (medianoche) hasta las 18:00.

Los parámetros de programación se establecen de la siguiente manera:

1. Meses: **septiembre, octubre, noviembre**.
2. Los: **<todos los> <días hábiles>**.
3. Cada: **6** horas.
   Desde: **12:00:00.** Hasta: **18:00:00**.
4. Vigente:

Desde: **30/08/09**. En realidad, la tarea se iniciará el primer día hábil de septiembre. Al establecer esta fecha, lo único que definimos es que la tarea debe iniciarse en 2009.

Hasta: **1/12/10**. En realidad, la tarea finalizará el último día hábil de noviembre. Al establecer esta fecha, lo único que definimos es que la tarea debe finalizar en 2010, cuando termina el otoño en el hemisferio norte.

**Varias programaciones mensuales para una tarea**

En los casos en los que la tarea deba ejecutarse en diferentes días de las semanas con intervalos distintos según el mes, sería conveniente añadir una programación dedicada para cada mes deseado, o para varios meses.

Supongamos que la tarea entra en vigencia el 1/11/09.

- Durante el invierno en el hemisferio norte, la tarea se ejecuta una vez a las 22:00 todos los días hábiles.
- Durante la primavera y el otoño (también del norte), la tarea se ejecuta cada 12 horas todos los días hábiles.
- Durante el verano (también del norte), la tarea se ejecuta todos los días primero y quince de cada mes a las 22:00.

Por lo tanto, se añaden las tres programaciones siguientes a la tarea:

**Primera programación**

1. Meses: **diciembre**, **enero**, **febrero**.
2. Los: **<todos> <todos los días hábiles>**
3. Una vez a las: **22:00:00**.
4. Vigente:

   Desde: **11/01/2009**.

   Hasta: **no establecido**.

**Segunda programación**

1. Meses: **marzo**, **abril**, **mayo**, **septiembre**, **octubre**, **noviembre**.
2. Los: **<todos> <todos los días hábiles>**.
3. Cada: **12 horas**

   Desde: **12:00:00.** Hasta: **00:00:00.**
4. Vigente:

   Desde: **11/01/2009**.

   Hasta: **no establecido**.

**Tercera programación**

1. Meses: **junio**, **julio**, **agosto**.
2. Días: **1**, **15**.
3. Una vez a las: **22:00:00**.
4. Vigente:

   Desde: **11/01/2009**.

   Hasta: **no establecido**.

## 5.4 Configuraciones de programación avanzadas

Las siguientes configuraciones avanzadas están disponibles cuando se configura una programación diariamente, semanalmente o mensualmente en una política de copias de seguridad.

### Utilice Wake-on-LAN

Cuando se habilite esta configuración, Acronis Backup & Recovery 10 Management Server utilizará la funcionalidad Wake-On-LAN (WOL) para activar equipos registrados que están desactivados en el momento programado para iniciar una copia de seguridad, una operación de limpieza o de validación. Si la tarea de copia de seguridad se inicia en cada equipo con una demora (consulte la próxima configuración), el servidor de gestión activa los equipos de acuerdo con esas demoras.

Antes de utilizar esta configuración, asegúrese de haber habilitado Wake-on-LAN en los equipos registrados. Las configuraciones del sistema básico de entrada/salida (BIOS), del adaptador de red y del sistema operativo del equipo deben permitir la activación del mismo cuando está en estado desactivado, también conocido como el estado de energía S5 o G2.

### Distribuir la hora de inicio en la ventana de tiempo

Cuando esta configuración se habilita, se inicia la tarea de copia de seguridad en cada equipo registrado con una demora específica a partir de la hora de inicio configurada en la política. Esto distribuye las horas de inicio reales de las tareas en un intervalo de tiempo.

Esta configuración puede resultarle útil al crear una política de copias de seguridad para realizar copias de seguridad de múltiples equipos en una ubicación de la red, para evitar así una carga excesiva de la red.

Los valores de demora van de cero a un valor máximo de demora especificado y se determinan según el método de distribución elegido.

El valor de demora de cada equipo se determina cuando se implementa la política en el equipo y permanece igual hasta que la misma se edita y se modifica el valor máximo de demora.

Las condiciones, si hubiera, se verificarán en el momento de inicio real de la tarea en cada equipo.

Los siguientes ejemplos muestran esta configuración.

**Ejemplo 1**

Suponga que está implementando una política de copias de seguridad con la siguiente programación en tres equipos:

Ejecutar la tarea: **Diaria**
Una vez a las: **09:00:00**

**Distribuir la hora de inicio en la ventana de tiempo**
Demora máxima: **1 hora(s)**
Método de distribución: **Aleatorio**

Entonces la hora de inicio de la tarea en cada equipo puede ser cualquier momento entre las 09:00:00 y las 09:59:59 , por ejemplo:

Primer equipo: Cada día a las 09:30:03

Segundo equipo: Cada día a las 09:00:00

Tercer equipo: Cada día a las 09:59:59

**Ejemplo 2**

Suponga que está implementando una política de copias de seguridad con la siguiente programación en tres equipos:

Ejecutar la tarea: **Diaria**
Cada: **2 hora(s)** Desde las: **09:00:00** Hasta las: **11:00:00**

**Distribuir la hora de inicio en la ventana de tiempo**
Demora máxima: **1 hora(s)**
Método de distribución: **Aleatorio**

Entonces la hora de la primer ejecución de la tarea en cada equipo puede ser cualquier momento entre las 09:00:00 y las 09:59:59 y el intervalo entre la primera y la segunda ejecución es de exactamente dos horas, por ejemplo:

Primer equipo: Cada día a las 09:30:03 y 11:30:03

Segundo equipo: Cada día a las 09:00:00 y 11:00:00

Tercer equipo: Cada día a las 09:59:59 y 11:59:59

***Para especificar las configuraciones avanzadas***

1. Conéctese al servidor de gestión o a un equipo registrado en el mismo y después comience a crear una política de copias de seguridad o un plan de copia de seguridad.
2. En **Cómo crear copias de seguridad**, seleccione el esquema Simple, Torres de Hanói o Personalizado y después haga clic en **Cambiar** para especificar una programación para el esquema.
3. Debajo de **Ejecutar la tarea**, seleccione **Diariamente**, **Semanalmente** o **Mensualmente**.
4. En el área **Configuraciones avanzadas**, haga clic en **Cambiar**.
5. Para habilitar el uso de la funcionalidad Wake-On-LAN, seleccione la casilla de verificación **Utilizar Wake-on-LAN**.
6. Para distribuir las horas de inicio de las tareas de copia de seguridad centralizadas, seleccione la casilla de verificación **Distribuir la hora de inicio de la ventana de tiempo** y después especifique el valor máximo de demora y el método de distribución.

## 5.5 Al producirse un evento del Registro de sucesos de Windows

Este tipo de programación solo funciona en los sistemas operativos Windows.

Puede programar una tarea de copia de seguridad para que se inicie cuando se registre un suceso en particular en uno de los registros de sucesos de Windows, como los registros de la aplicación, de seguridad o del sistema.

Por ejemplo, podría crear un plan de copia de seguridad que realice automáticamente una copia de seguridad completa de emergencia con sus datos en cuanto Windows detecte que se está por producir un error en su unidad de disco duro.

### Parámetros

**Nombre del registro**

Especifica el nombre del registro. Seleccione en la lista el nombre de un registro estándar (**Aplicación, Seguridad** o **Sistema**) o escríbalo. Por ejemplo: **Sesiones de Microsoft Office**

**Origen del suceso**

Especifica el origen del suceso que, por lo general, indica qué programa o componente del sistema generó el suceso. Por ejemplo: **disco**

**Tipo de suceso**

Especifica el tipo de suceso: **Error**, **Advertencia**, **Información**, **Auditoría correcta** o **Error en auditoría**.

**Id. suceso**

Especifica el número del suceso, que suele identificar los tipos de sucesos en particular entre sucesos del mismo origen.

Por ejemplo, un suceso **Error** con Origen de suceso **disco** e Id. suceso **7** ocurre cuando Windows descubre un bloque dañado en un disco, mientras que un suceso **Error** con Origen de suceso **disco** e Id. suceso **15** ocurre cuando no se puede obtener acceso a un disco porque todavía no está preparado.

## Ejemplos

**Copia de seguridad de emergencia "Bloque dañado"**

La aparición repentina de uno o más bloques dañados en un disco duro generalmente indica que pronto se producirá un error en la unidad de disco duro. Supongamos que desea crear un plan de copia de seguridad para copiar datos del disco duro en cuanto se presente tal situación.

Cuando Windows detecta un bloque dañado en un disco duro, registra un suceso en el **disco/** de origen del suceso y el número de suceso **7** en el registro del **Sistema**; el tipo de suceso es **Error**.

Al crear un plan, escriba o seleccione las siguientes opciones en el área **Programar**:

- **Nombre del registro**: **Sistema**
- **Origen del suceso**: **disco**
- **Tipo de suceso**: **Error**
- **Id. suceso**: **7**

***Importante:*** *Para garantizar que dicha tarea se realice a pesar de la presencia de bloques dañados, debe hacer que la tarea omita los bloques dañados. Para eso, en* ***Opciones de copia de seguridad****, vaya a* ***Manejo de errores*** *y luego marque la casilla de verificación* ***Ignorar los sectores defectuosos****.*

**Copia de seguridad previa a la actualización en Vista**

Supongamos que desea crear un plan de copia de seguridad que realice copias de seguridad del sistema automáticamente, por ejemplo, que cree una copia de seguridad del volumen donde está instalado Windows, cada vez que Windows esté por instalar actualizaciones.

Una vez descargadas las actualizaciones y programada su instalación, el sistema operativo Microsoft Windows Vista registra un suceso con el origen de sucesos **Microsoft-Windows-WindowsUpdateClient** y el número de suceso **18** en el registro del **sistema**; el tipo de suceso es **Información**.

Al crear un plan, escriba o seleccione las siguientes opciones en el área **Programar**:

- **Nombre del registro**: **Sistema**
- **Origen del suceso**: **Microsoft-Windows-WindowsUpdateClient**
- **Tipo de suceso**: **Información**

- **Id. suceso**: **18**

***Consejo:*** *Para configurar un plan de copia de seguridad similar para equipos con Microsoft Windows XP, reemplace el texto de* ***Origen del suceso*** *por* ***Agente de Windows Update*** *y no modifique los demás campos.*

### Cómo ver sucesos en el Visor de sucesos

*Para abrir un registro en el Visor de sucesos:*

1. En el escritorio o en el menú **Inicio**, haga clic con el botón secundario en **Mi PC** y luego haga clic en **Administrar**.
2. En la consola **Administración del equipo**, expanda **Herramientas del sistema** y luego expanda **Visor de sucesos**.
3. En el **Visor de sucesos**, haga clic en el nombre del registro que desea ver; por ejemplo, **Aplicación**.

   ***Nota:*** *Para poder abrir el registro de seguridad (****Seguridad****), debe ser miembro del grupo de Administradores.*

*Para ver las propiedades de un suceso, incluidos el origen y el número del suceso:*

1. En el **Visor de sucesos**, haga clic en el nombre del registro que desea ver; por ejemplo, **Aplicación**.

   ***Nota:*** *Para poder abrir el registro de seguridad (****Seguridad****), debe ser miembro del grupo de Administradores.*

2. En la lista de sucesos del panel derecho, haga doble clic en el nombre del suceso cuyas propiedades desea ver.
3. En el cuadro de diálogo **Propiedades del suceso**, se podrán ver las propiedades de dicho suceso, como el origen (que se muestra en el campo **Origen**) y el número del suceso (que se muestra en el campo **Id. suceso**).

Cuando termine, haga clic en **Aceptar** para cerrar el cuadro de diálogo **Propiedades del suceso**.

## 5.6 Cuando se produzca una alerta de Acronis Drive Monitor

Esta programación está vigente en sistemas operativos Windows cuando está instalado Acronis® Drive Monitor™.

Acronis Drive Monitor informa sobre el estado del disco duro al utilizar el sistema de supervisión interno del disco duro (S.M.A.R.T.). Basado en alertas de Acronis Drive Monitor, puede configurar copias de seguridad de emergencia de sus datos además de las copias de seguridad habituales. La copia de seguridad de emergencia dará comienzo cuando sus datos junto con su disco duro estén a punto de fallar.

La copia de seguridad comienza tan pronto como el estado del disco alcanza un nivel crítico o de advertencia. Puede observar el indicador del estado del disco, para cada disco, como un porcentaje, con tan sólo abrir Acronis Drive Monitor.

Las alertas acerca de la temperatura del disco no dan comienzo a la copia de seguridad.

***Consejo:*** *Si su plan de copia de seguridad usa el esquema personalizado de la copia de seguridad (pág. 229), puede configurar esta copia de seguridad de emergencia simplemente añadiendo programación extra al mismo*

*plan de copia de seguridad. Cuando utilice un esquema de copia de seguridad diferente, necesitará crear un plan de copia de seguridad por separado.*

## 5.7 Condiciones

Las condiciones otorgan más flexibilidad al programador y le permiten llevar a cabo tareas de copia de seguridad con respecto a ciertas condiciones. Cuando ocurre un suceso especificado (consulte la sección "Programación (pág. 173)" para ver los sucesos disponibles), el programador verifica la condición especificada y lleva a cabo la tarea si se cumple con dicha condición.

En caso de que el suceso ocurra pero la condición (o alguna de ellas si son varias) no se cumpla, el comportamiento del programador estará definido por la opción de copia de seguridad **Condiciones de inicio de la tarea** (pág. 115). Allí, podrá determinar la importancia de las condiciones para la estrategia de copia de seguridad:

- condiciones obligatorias: la ejecución de la tarea de copia de seguridad se pone en espera hasta que se cumplan todas las condiciones.
- condiciones opcionales, pero la ejecución de la tarea de copia de seguridad tiene mayor prioridad: la ejecución de la tarea de copia de seguridad se pone en espera durante el intervalo especificado. Si el intervalo finaliza y las condiciones no se cumplieron, la tarea se ejecuta de todas maneras. Con esta configuración, el programa controla la situación automáticamente cuando las condiciones no se cumplen durante mucho tiempo y una mayor demora de la copia de seguridad no es conveniente.
- la hora de inicio de la tarea de copia de seguridad es importante: la tarea de copia de seguridad se omite si no se cumplieron las condiciones a la hora en que se debería iniciar la tarea. Omitir la tarea es conveniente si necesita realizar copias de seguridad de datos estrictamente a la hora especificada, especialmente si los sucesos ocurren con cierta frecuencia.

*Las condiciones están disponibles tan solo cuando el esquema personalizado de copia de seguridad (pág. 229) esté siendo utilizado. Puede establecer las condiciones de forma separada para una copia de seguridad completa, incremental y diferencial.*

### Incorporación de varias condiciones

Si se añaden varias condiciones, deben cumplirse todas simultáneamente para que se lleve a cabo la tarea.

**Ejemplo:**

Es necesario ejecutar la tarea de copia de seguridad después de que en el equipo gestionado se cambie el espacio libre en al menos 1 GB, pero solo si todos los usuarios cerraron sesión y han pasado 12 horas desde la última copia de seguridad.

Establezca la opción de copia de seguridad para programación, condiciones y **Condiciones de inicio de la tarea** de la siguiente manera:

- Programación: **Al cambiar el espacio libre**; Valor: Ejecutar la tarea si el espacio libre cambió en al menos: **1 GB**.
- Condición: **El usuario cerró la sesión**; Valor: Ejecutar la tarea programada solo si todos los usuarios cerraron sesión.
- Condición: **Tiempo transcurrido desde la última copia de seguridad**; Valor: Tiempo transcurrido desde la última copia de seguridad: **12 hora(s)**.
- Condiciones de inicio de la tarea: **Esperar hasta que se cumplan las condiciones**.

Si el espacio libre cambia en más de 1 GB, el programador esperará a que se cumplan ambas condiciones simultáneamente y, luego, ejecutará la tarea de copia de seguridad.

### 5.7.1 El usuario está inactivo

*Se aplica a: Windows*

"El usuario está inactivo" significa que se está ejecutando el protector de pantalla o que el equipo está bloqueado.

**Ejemplo:**

Ejecutar la tarea de copia de seguridad en el equipo gestionado todos los días a las 21:00, preferentemente cuando el usuario esté inactivo. Si el usuario sigue activo a las 23:00, ejecute la tarea de todos modos.

- Suceso: **Diariamente**, Cada **1** día(s); Una vez a las: **21:00:00**.
- Condición: **El usuario está inactivo**.
- Condiciones de inicio de la tarea: **Esperar hasta que se cumplan las condiciones**, pero ejecutar la tarea de todos modos después de **2** hora(s).

Como resultado:

(1) Si el usuario queda inactivo antes de las 21:00, la tarea de copia de seguridad se inicia a las 21:00.

(2) Si el usuario queda inactivo entre las 21:00 y las 23:00, la tarea de copia de seguridad se inicia inmediatamente después de que este hecho ocurra.

(3) Si el usuario todavía está activo a las 23:00, la tarea de copia de seguridad se inicia de todos modos.

### 5.7.2 El servidor de ubicación no está disponible

*Se aplica a: Windows, Linux*

"El servidor de ubicación está disponible" significa que el equipo que alberga el destino para almacenar los archivos comprimidos en una unidad de red está disponible.

**Ejemplo:**

La creación de copias de seguridad de los datos en la ubicación de red se realiza los días hábiles a las 21:00 h. Si el servidor de ubicación no estuviera disponible en ese momento (por ejemplo, debido a trabajos de mantenimiento), la creación se omite y se espera al siguiente día hábil para iniciar la tarea. Se supone que directamente no se debería iniciar la tarea de copia de seguridad, en lugar de que ocurra un error.

- Suceso: **Semanalmente**, Cada **1** semana en **<días hábiles>**; Una vez a las **21:00:00.**
- Condición: **El servidor de ubicación no está disponible**
- Condiciones de inicio de la tarea: **Omitir la ejecución de la tarea**.

Como resultado:

(1) Si son las 21:00 h y el servidor de la ubicación está disponible, la tarea de copia de seguridad se iniciará a tiempo.

(2) Si son las 21:00 h pero el servidor no está disponible en ese momento, la tarea de copia de seguridad se iniciará el siguiente día hábil si el servidor de la ubicación está disponible.

(3) Si es imposible que el servidor de la ubicación esté disponible en días laborables a las 21:00 h, la tarea nunca se iniciará.

### 5.7.3 Coincidir con intervalo

*Se aplica a: Windows, Linux*

Limita la hora de inicio de una tarea de copia de seguridad a un intervalo especificado.

#### Ejemplo

Una empresa usa distintas ubicaciones en el mismo dispositivo de almacenamiento conectado a la red para realizar copias de seguridad de servidores y datos de usuarios. El día hábil empieza a las 08:00 y termina a las 17:00. Las copias de seguridad de los datos de los usuarios deben realizarse en cuanto ellos cierren la sesión, pero no antes de las 16:30 ni después de las 22:00. Todos los días, se hacen copias de seguridad de los servidores de la empresa a las 23:00. Por lo tanto, es preferible que las copias de seguridad de los datos de los usuarios se realicen antes de dicho horario, para liberar ancho de banda de la red. Al especificar el límite superior a las 22:00, se supone que realizar copias de seguridad de los datos de los usuarios no debería llevar más de una hora. Si un usuario ha iniciado sesión durante del intervalo especificado, o si cierra la sesión en cualquier otro momento, no se realizan copias de seguridad de los datos de los usuarios, es decir, se omite la ejecución de la tarea.

- Suceso: **Al cerrar sesión**, el siguiente usuario: **Cualquier usuario**.
- Condición: **Coincidir con intervalo,** desde las **16:30:00** hasta las **22:00:00**.
- Condiciones de inicio de la tarea: **Omitir la ejecución de la tarea**.

Como resultado:

(1) si el usuario cierra la sesión entre las 16:30:00 y las 22:00:00, la tarea de copia de seguridad se iniciará inmediatamente después de dicho cierre de sesión.

(2) si el usuario cierra la sesión en algún otro horario, la tarea se omitirá.

#### Posibles situaciones

*¿Qué sucede si se programa una tarea para ejecutarse en un horario en particular que está fuera del intervalo especificado?*

Por ejemplo:

- Suceso: **Diariamente**, Cada **1** día(s); Una vez a las **15:00:00**.
- Condición: **Coincidir con intervalo**, desde las **18:00:00** hasta las **23:59:59**.

En este caso, el hecho de que se inicie la tarea y el horario en que lo hará depende de las condiciones de inicio de la tarea:

- Si las condiciones de inicio de la tarea son **Omitir la ejecución de tarea**, la tarea nunca se ejecutará.
- Si las condiciones de inicio de la tarea son **Esperar hasta que se cumplan las condiciones** y la casilla de verificación **Ejecutar la tarea de todos modos después de** está *desmarcada*, la tarea (programada para ejecutarse a las 15:00) se iniciará a las 18:00, la hora en la que se cumple la condición.

- Si las condiciones de inicio de la tarea son **Esperar hasta que se cumplan las condiciones** y la casilla de verificación **Ejecutar la tarea de todos modos después de** está *marcada* con, digamos, el tiempo de espera de **1 hora**, la tarea (programada para ejecutarse a las 15:00) se iniciará a las 16:00, la hora en la que se cumple la condición.

### 5.7.4 El usuario cerró la sesión

*Se aplica a: Windows*

Permite poner en espera la ejecución de una tarea de copia de seguridad hasta que todos los usuarios cierren la sesión en Windows en el equipo gestionado.

#### Ejemplo

Ejecutar la tarea de copia de seguridad a las 20:00 el primer y el tercer viernes de cada mes, preferentemente cuando todos los usuarios hayan cerrado la sesión. Si alguno de los usuarios todavía no hubiera cerrado la sesión a las 23:00, la tarea se ejecuta de todos modos.

- Suceso: **Mensualmente**, Meses: **<Todos>**; Los: **<Primer>**, **<Tercer>** **<Viernes>**; Una vez a las **20:00:00**.
- Condición: **El usuario cerró la sesión**.
- Condiciones de inicio de la tarea: **Esperar hasta que se cumplan las condiciones** pero ejecutar la tarea de todos modos después de **3** hora(s).

Como resultado:

(1) Si, para las 20:00, todos los usuarios cerraron la sesión, la tarea de copia de seguridad se iniciará a las 20:00.

(2) Si el último usuario cierra la sesión entre las 20:00 y las 23:00, la tarea de copia de seguridad se inicia inmediatamente después de que este hecho ocurra.

(3) Si alguno de los usuarios todavía no hubiera cerrado sesión a las 23:00, la tarea de copia de seguridad se iniciará de todos modos.

### 5.7.5 Tiempo transcurrido desde la última copia de seguridad

*Se aplica a: Windows, Linux*

Permite poner en espera la ejecución de una tarea de copia de seguridad hasta que transcurra el intervalo especificado desde la última finalización correcta de la copia de seguridad.

#### Ejemplo:

Ejecutar la tarea de copia de seguridad al iniciarse el sistema, pero sólo si han transcurrido más de 12 horas desde la última tarea de copia de seguridad con éxito.

- Suceso: **Al iniciar**, Comenzar la tarea al iniciarse el equipo.
- Condición: **Tiempo transcurrido desde la última copia de seguridad**, Tiempo que transcurrió desde la última copia de seguridad: **12** hora(s).
- Condiciones de inicio de la tarea: **Esperar hasta que se cumplan las condiciones**.

Como resultado:

(1) si el equipo se reinicia antes de que transcurran 12 horas desde la finalización de la última tarea de copia de seguridad con éxito, el programador esperará a que transcurran 12 horas y entonces iniciará la tarea.

(2) si el equipo se reinicia una vez transcurridas 12 horas desde la finalización de la última tarea de copia de seguridad con éxito, la tarea de copia de seguridad se iniciará inmediatamente.

(3) si el equipo no se reinicia nunca, la tarea nunca se iniciará. De ser necesario, puede iniciar la copia de seguridad manualmente desde la vista **Planes y tareas de copia de seguridad**.

# 6 Gestión directa

Esta sección cubre las operaciones que pueden realizarse directamente en un equipo gestionado al utilizar la conexión directa de consola-agente. El contenido de esta sección es aplicable a las ediciones avanzadas y autónomas de Acronis Backup & Recovery 10.

## 6.1 Administrar un equipo gestionado

Esta sección describe las vistas que están disponibles a través del árbol de navegación de la consola conectada a un equipo gestionado y explica cómo trabajar en cada vista.

### 6.1.1 Tablero

Utilice el Tablero para estimar rápidamente si los datos se han protegido con éxito en el equipo. El tablero muestra el resumen de las actividades de los agentes Acronis Backup & Recovery 10 y permite identificar y resolver rápidamente cualquier problema.

#### Alertas

La sección Alertas llama su atención sobre los problemas que han ocurrido en el equipo y le ofrece maneras para repararlos o examinarlos. Los problemas más críticos se muestran en la parte superior. Si no hay alertas o advertencias en ese momento, el sistema muestra "No hay alertas ni advertencias".

#### Tipos de alertas

La siguiente tabla muestra los tipos de mensajes que podría observar.

| | Descripción | Solución | Comentario |
|---|---|---|---|
| | Tareas fallidas: X | Resolver | **Resolve**r abrirá la vista **Planes y tareas de copia de seguridad** con las tareas fallidas, donde puede examinar la causa del fallo. |
| | Tareas que necesitan interacción: X | Resolver | Cuando una tarea requiere interacción humana, el Tablero muestra un mensaje para informarle qué acción hay que llevar a cabo (por ejemplo, introducir un nuevo CD o Detener/Reintentar/Ignorar cuando ocurre un error). |
| | Falla al intentar comprobar la licencia desde la edición actual. Faltan X día(s) para que el software deje de funcionar.<br>Asegúrese de que dispone de una licencia válida en el Servidor de Licencia Acronis . | Conectar | El agente Acronis Backup & Recovery 10 conecta al Servidor de Licencia Acronis al comienzo y luego cada 1–5 días (1 día predeterminado), como se ve especificado por los parámetros de configuración de agente.<br>Si la comprobación de licencia no es exitosa durante 1–60 días, como lo especifican los parámetros de configuración del agente (predeterminada en 30 días), el agente dejará de funcionar hasta que se realice una última comprobación de licencia exitosa. |

| | | | |
|---|---|---|---|
| | No puede realizar la comprobación de la clave de la licencia para la edición actual de X días. O bien el Acronis License Server no estaba disponible o los datos de la clave de licencia estaban dañados. Compruebe la conectividad con el servidor y ejecute el Acronis License Server para gestionar las licencias.<br>Asegúrese de que dispone de una licencia válida en el Servidor de Licencia Acronis . | Conectar | Acronis Backup & Recovery 10 detenido. Durante los últimos *X* días, el agente no pudo comprobar si su licencia estaba disponible en el Servidor de Licencias Acronis.<br>Probablemente esto se debe a que el servidor de licencias no está disponible. También puede querer asegurarse que las licencias se encuentren en el servidor de licencia, o que los datos de la clave de la licencia no estén corruptos.<br>Luego de comprobación exitosa de licencia, el agente comenzará a funcionar. |
| | La versión de prueba del producto caduca en *X* día(s)<br>Asegúrese de que dispone de una licencia válida en el Servidor de Licencia Acronis . | Conectar | Cuando se instala la versión de prueba del producto, el programa inicia la cuenta atrás de los días que faltan para que el periodo de prueba caduque. |
| | El período de prueba ha finalizado. Inicie el instalador e ingrese la clave de licencia completa.<br>Asegúrese de que dispone de una licencia válida en el Servidor de Licencia Acronis . | Conectar | El periodo de prueba de 15 días ha caducado. Introduzca una clave de licencia completa |
| | Bóvedas con poco espacio libre: X | Ver bóvedas | **La vista de bóvedas** lo conducirá a la vista **Bóvedas** donde podrá examinar el tamaño de bóveda, el espacio libre, el contenido y dar los pasos necesarios para incrementar el espacio libre. |
| | El dispositivo de inicio no se creó | Crear ahora | Para poder recuperar un sistema operativo cuando un equipo no se puede iniciar, debe:<br>1. Realizar una copia de seguridad del volumen del sistema (y del volumen de inicio, si es diferente).<br>2. Crear al menos un dispositivo de inicio (pág. 410).<br>**Crear ahora** ejecutará el Generador de dispositivos de inicio (pág. 406). |
| | No se han creado copias de seguridad durante *X* días | Crear copia de seguridad ahora | El Tablero le advierte que no se ha realizado ninguna copia de seguridad de los datos en el equipo durante un periodo considerablemente largo de tiempo.<br>**Realizar copia de seguridad ahora** lo llevará a la página **Crear un plan de copia de seguridad** donde puede configurar y ejecutar la operación de copia de seguridad instantáneamente.<br>Para configurar el intervalo de tiempo que se considera crítico, seleccione **Opciones > Opciones de consola > Alertas según el momento**. |
| | No ha estado conectado al servidor de | Ver los | Este tipo de mensaje puede aparecer en un equipo que está registrado en un servidor de |

| | | | |
|---|---|---|---|
| | gestión durante X días | equipos | gestión. El Tablero le advierte que se puede haber perdido la conexión o que el servidor puede no estar disponible y por lo tanto el equipo no está siendo gestionado de forma centralizada. |

### Actividades

El calendario le permite explorar el historial de las actividades del agente Acronis Backup & Recovery 10 en el equipo. Haga clic con el botón derecho en la fecha resaltada y seleccione **Ver registro** para ver la lista de las entradas del registro filtradas por fecha.

En la sección **Ver** (a la derecha del calendario), puede seleccionar las actividades para resaltar dependiendo de la presencia y gravedad de los errores.

| | Cómo se determina |
|---|---|
| **Errores** | Se resalta la fecha en rojo si se aparece al menos una entrada de "Error" en el registro en esta fecha. |
| **Advertencias** | Se resalta la fecha en amarillo si no aparece ninguna entrada de "Error" y se encuentra al menos una entrada de "Advertencia" en el registro en esta fecha. |
| **Información** | Se resalta la fecha en verde si sólo se encuentran entradas de "Información" en el registro en esta fecha (actividad normal). |

El enlace **Seleccionar fecha actual** aplica la fecha actual a la selección.

### Vista Sistema

Muestra estadísticas resumidas de los planes de copia de seguridad, tareas e información breve sobre la última copia de seguridad. Haga clic en los elementos de esta sección para obtener la información correspondiente. Esto te llevará a la vista **Planes y tareas de copia de seguridad** (pág. 192) con tareas o planes de seguridad prefiltrados. Por ejemplo, si se hace clic en **Local** en **Planes de copia de seguridad**, la vista **Planes y tareas de copia de seguridad** se abrirá con los planes de copia de seguridad filtrados por origen **Local**.

## Tareas que necesitan interacción

Esta ventana acumula todas las tareas que necesitan la interacción del usuario en un sitio. Esto le permite especificar su decisión como, por ejemplo, confirmar el reinicio o volver a intentarlo después de liberar espacio del disco, en todas las tareas. Hasta que por lo menos una tarea necesite su interacción, puede abrir esta ventana en cualquier momento desde el **Tablero** (pág. 190) del equipo gestionado.

Si selecciona la casilla de verificación para el parámetro **No mostrar esta ventana cuando las tareas necesitan interacción. Veré esta información en los detalles de tareas y en el tablero.** Las tareas se mostrarán en el **Tablero** entre otras alertas y advertencias.

O bien, puede revisar el estado de ejecución de la tarea en la vista **Planes y tareas de copia de seguridad** (pág. 192) y especificar su decisión en cada tarea en el panel **Información** (o en la ventana **Detalles de tareas** (pág. 201)).

## 6.1.2 Planes y tareas de la copia de seguridad

La vista **Planes y tareas de la copia de seguridad** lo mantiene informado de la protección de datos en un equipo determinado. Le permite monitorizar y gestionar las tareas y los planes de copias de seguridad.

Un plan de copias de seguridad es una serie de reglas que especifica cómo se protegerán los datos en un equipo determinado. Físicamente, un plan de copias de seguridad es un paquete de tareas configuradas para la ejecución en un equipo gestionado. Para averiguar lo que está haciendo exactamente un plan de copias de seguridad en un equipo, active el estado de ejecución de un plan de copias de seguridad (pág. 193). Un estado de copia de seguridad es un estado acumulado de las tareas del plan. El estatus de un plan de copias de seguridad (pág. 194) le ayuda a estimar si los datos se encuentran correctamente protegidos.

Una tarea es una serie de acciones secuenciales que deben realizarse en un equipo cuando pasa cierto tiempo o cuando ocurre un determinado evento. Para tener un control del progreso actual de una tarea, examine su estado (pág. 195). Compruebe el estatus (pág. 196) de una tarea para determinar el resultado de una tarea.

### Modo de trabajo

- Use filtros para mostrar los planes de copias de seguridad que desee (tareas) en la tabla de planes de copias de seguridad. De manera predeterminada, la tabla muestra los planes del equipo gestionado por orden alfabético. También puede ocultar las columnas innecesarias y mostrar las ocultas. Para obtener más detalles, consulte la sección Filtrar y ordenar los planes de copias de seguridad (pág. 200).
- En la tabla de copia de seguridad, seleccione el plan (tarea) de copia de seguridad.
- Utilice los botones de la barra de herramientas para llevar a cabo una acción en el plan (tarea) seleccionado. Para obtener más detalles, consulte la sección Acciones en planes y tareas de la copia de seguridad (pág. 197). Puede ejecutar, editar, detener y eliminar los planes y tareas creados.
- Para revisar información detallada sobre el plan (tarea) seleccionado, utilice el panel **Información**. De manera predeterminada, el panel se encuentra minimizado. Para expandir el panel, haga clic en la flecha tipo  . El contenido del panel también está duplicado en las ventanas **Detalles del plan** (pág. 203) y **Detalles de la tarea** (pág. 201) respectivamente.

## Comprender los estados y estatus

## Estados de ejecución de planes de copia de seguridad

Un plan de copias de seguridad puede encontrarse en uno de los siguientes estados: **Inactiva, esperando, ejecutando, deteniendo, necesita interacción**.

Los nombres de los estados del plan son los mismos que para las tareas ya que el estado de un plan es el estado acumulado de las tareas del plan.

| | Estado | Cómo se determina | Cómo manejarlo |
|---|---|---|---|
| 1 | **Necesita interacción** | Al menos una tarea necesita la interacción del usuario.<br>En caso contrario, consulte el punto 2. | Identifique las tareas que necesitan interacción (el programa mostrará la acción a realizar) -> Detenga las tareas o active su ejecución (cambiar dispositivo, proporcionar espacio adicional a la bóveda, ignorar los errores de lectura, crear la Acronis Secure Zone no encontrada). |
| 2 | **Ejecución de** | Al menos una tarea se está ejecutando.<br>En caso contrario, vea el punto 3. | No se necesita tomar ninguna medida. |

| | | | |
|---|---|---|---|
| 3 | **Esperando** | Al menos una tarea se encuentra en espera.<br>De lo contrario, consulte el punto 4. | Esperando las condiciones. Esta situación es bastante normal, pero retrasar una copia de seguridad durante mucho tiempo es peligroso. La solución sería ajustar el plazo máximo o forzar la situación (pedir al usuario que cierre la sesión, permitir la conexión a la red que se necesita).<br>Esperar mientras otra tarea consume los recursos necesarios. Un caso extraordinario de espera puede ocurrir cuando, por alguna razón en particular, el comienzo de una tarea dura mucho más de lo normal, y esto evita que comience otra diferente. La situación se resuelve automáticamente cuando la tarea que está obstruyendo el proceso finaliza. Contemple la posibilidad de interrumpir una tarea si tarda demasiado tiempo y evita que comience la tarea siguiente.<br>Un solapamiento continuo de las tareas podría derivar de uno o varios planes programados de manera incorrecta. En este caso, lo lógico es editar el plan. |
| 4 | **Deteniendo** | Al menos una tarea está deteniéndose.<br>De lo contrario, consulte el punto 5. | No se necesita tomar ninguna medida. |
| 5 | **Inactiva** | Todas las tareas se encuentran inactivas. | No se necesita tomar ninguna medida. |

## Estatus del plan de copias de seguridad

Un plan de copias de seguridad puede tener uno de los siguientes estatus: **Error; Advertencia; OK**.

El estatus de un plan de copias de seguridad deriva de los resultados de la última ejecución de las tareas de los planes.

| | Estado | Cómo se determina | Cómo manejarlo |
|---|---|---|---|
| 1 | **Error** | Por lo menos una de las tareas ha fallado.<br>De lo contrario, consulte el punto 2. | Identifique las tareas falladas -> Compruebe el registro de tareas para encontrar la causa del fallo y después lleve a cabo una o más de las siguientes tareas:<br>▪ Elimine la causa del fallo -> [opcionalmente] Inicie la tarea fallida manualmente<br>▪ Modifique el plan local para prevenir su futuro fallo en caso de que un plan local haya fallado<br>▪ Modifique la política de copias de seguridad en el servidor de gestión en caso de que un plan centralizado haya fallado<br>Cuando se crea un plan o un política de copias de seguridad, el administrador puede activar la opción para detener la ejecución del plan de copias de seguridad en el momento que se detecta el estatus de Error. Se puede reanudar la ejecución del plan de copias de seguridad utilizando el botón Reiniciar. |
| 2 | **Advertencia** | Por lo menos una tarea se ha completado correctamente con advertencias.<br>En caso contrario, vea el | Consulte el registro para leer las advertencias -> [opcionalmente] Realice las acciones para prevenir las advertencias o fallos futuros. |

| | | | |
|---|---|---|---|
| | | punto 3. | |
| 3 | **OK** | Todas las tareas se han completado correctamente. | No se necesita tomar ninguna medida. Tenga en cuenta que un plan de copias de seguridad puede estar OK si aún no se ha iniciado ninguna de las tareas o si alguna de las tareas se detienen o se está deteniendo. Estas situaciones se consideran normales. |

## Estados de las tareas

Una tarea puede encontrarse en uno de los siguientes estados: **Inactiva**, **esperando**, **ejecutando**, **deteniendo**, **necesita interacción**. El estado inicial de una tarea es **Inactiva**.

Una vez que la tarea ha comenzado manualmente o que tiene lugar el evento especificado en la programación, la tarea pasa al estado **Ejecutando** o al estado **Esperando**.

**Ejecución**

Una tarea cambia al estado **Ejecutando** cuando tiene lugar el evento especificado en la programación Y se cumplen todas las condiciones configuradas en el plan de copias de seguridad Y no se está ejecutando ninguna otra tarea que consuma los recursos necesarios. En este caso, nada impide que la tarea se ejecute.

**Esperando**

Una tarea cambia al estado **Esperando** cuando la tarea está preparada para comenzar pero otra tarea que utiliza los mismos recursos continúa ejecutándose. Particularmente, no es posible ejecutar en un equipo más de una tarea de copia de seguridad o más de una tarea de recuperación al mismo tiempo. Una tarea de copia de seguridad y una de recuperación tampoco pueden ejecutarse de manera simultánea. Una vez que la tarea deja de consumir el recurso, la tarea en espera pasa al estado **Ejecutando**.

Una tarea también puede cambiar al estado **Esperando** cuando se lleva a cabo el evento especificado en la programación pero no se cumple una condición configurada en el plan de copias de seguridad. Para obtener más información, consulte Condiciones de inicio de la tarea (pág. 115).

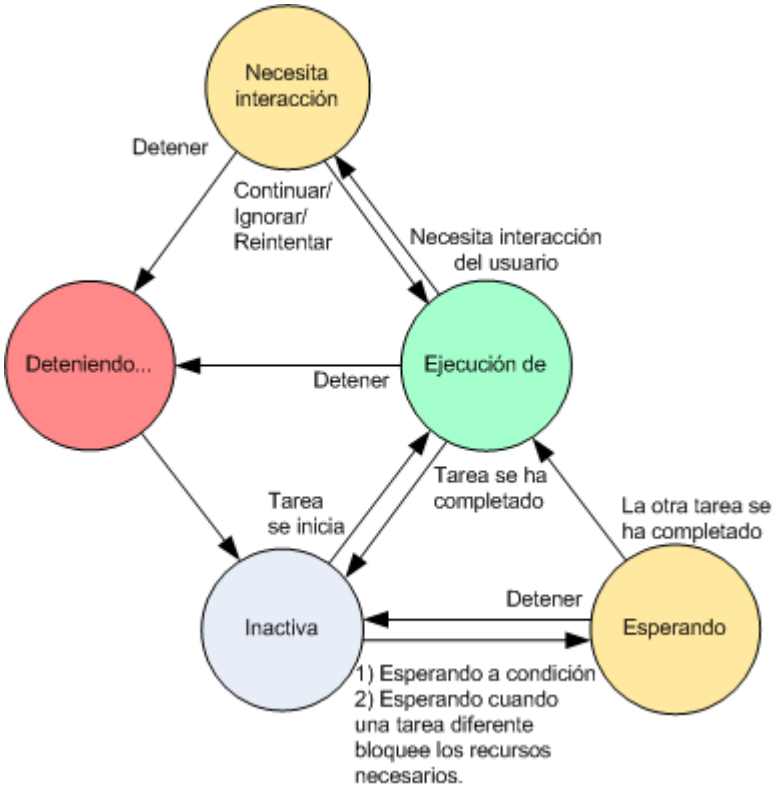
**Necesita interacción**

Cualquier tarea que esté ejecutándose puede pasar al estado **Necesita interacción** si necesita la interacción del usuario para, por ejemplo, cambiar un dispositivo o ignorar un error de lectura. El siguiente estado sería el de **Deteniendo** (si el usuario elige detener la tarea) o **Ejecutándose** (al seleccionar Ignorar/Reintentar u otra acción, tal como Reiniciar, que vuelva a cambiar la tarea al estado de **Ejecutando**).

**Deteniendo**

El usuario puede detener una tarea que se está ejecutando o una tarea que necesita interacción. Una tarea pasa del estado **Deteniendo** al estado **Inactiva**. También puede detenerse una tarea en espera. En este caso, ya que la tarea no está ejecutándose, "detener" significa eliminarla de la cola.

**Diagrama de estado de las tareas**




## Estatus de las tareas

Una tarea puede tener uno de los siguientes estatus: **Error**; **Advertencia**; **OK**.

El estatus de una tarea deriva del resultado de la última ejecución de la tarea.

| | Estado | Cómo se determina | Cómo afrontarlo |
|---|---|---|---|
| 1 | **Error** | El último resultado es "Fallido" | Identifique la tarea fallada -> Compruebe el registro de tareas para encontrar la causa del fallo, después lleve a cabo una o más de las siguientes tareas:<br>▪ Elimine la causa del fallo -> [opcionalmente] Inicie la tarea fallida manualmente<br>▪ Modifique la tarea fallida para prevenir su futuro fallo<br>▪ Modifique el plan local para prevenir su futuro fallo en caso de que un plan local haya fallado<br>▪ Modifique la política de copias de seguridad en el servidor de gestión en caso de que un plan centralizado haya fallado |
| 2 | **Advertencia** | El último resultado es "Completado correctamente con advertencias" | Vea el registro para leer las advertencias -> [opcionalmente] Realice las acciones para prevenir las advertencias o fallos futuros. |
| 3 | **OK** | El último resultado es "Completado correctamente", "- | No es necesario tomar ninguna medida.<br>El estado "-" significa que la tarea nunca se ha iniciado o |

| | | | |
|---|---|---|---|
| | | ", o "Detenido" | se ha iniciado, pero aún no se ha completado y, por lo tanto, su resultado no está disponible. |

## Trabajar con los planes y las tareas de copia de seguridad

### Acciones en los planes y tareas de copia de seguridad

A continuación se ofrece una guía para la realización de operaciones con planes y tareas de copia de seguridad.

| Operación | Procedimiento |
|---|---|
| Cree un plan de copia de seguridad nuevo o una tarea | Haga clic en **Nuevo** y luego seleccione una de las siguientes opciones:<br>▪ Plan de copia de seguridad (pág. 207)<br>▪ Tarea de recuperación<br>▪ Tarea de validación (pág. 255) |
| Ver los detalles de un plan o una tarea | **Plan de copia de seguridad**<br>Haga clic en **Ver detalles**.<br>En la ventana de **Detalles del plan** (pág. 203), revise los detalles del plan.<br>**Tarea**<br>Haga clic en **Ver detalles**.<br>En la ventana de **Detalles de la tarea** (pág. 201), revise los detalles de la tarea. |
| Ver el registro del plan o de la tarea | **Plan de copia de seguridad**<br>Haga clic en **Ver registro**.<br>Accederá a la sección de **Registro** (pág. 204), la cual incluye la lista de las entradas de registro relacionadas con el plan.<br>**Tarea**<br>Haga clic en **Ver registro**.<br>Accederá a la sección de **Registro** (pág. 204), la cual incluye la lista de las entradas de registro relacionadas con la tarea. |
| Ejecutar un plan o una tarea | **Plan de copia de seguridad**<br>Haga clic en **Ejecutar**.<br>En la ventana **Ejecutar plan de copia de seguridad** (pág. 201), seleccione la tarea que necesita que se ejecute.<br>La ejecución del plan de copia de seguridad inicia inmediatamente la tarea seleccionada de dicho plan, independientemente de la programación y de las condiciones.<br>*¿Por qué no puedo ejecutar el plan de copia de seguridad?*<br>▪ No tiene el privilegio adecuado<br>Un usuario no puede ejecutar planes de otros usuarios sin poseer los privilegios de Administrador.<br>**Tarea**<br>Haga clic en **Ejecutar**.<br>La tarea se ejecutará inmediatamente, independientemente de la programación y de las condiciones. |

| | |
|---|---|
| Detener un plan o una tarea | **Plan de copia de seguridad**<br><br>Haga clic en **Detener**.<br><br>Al detener el plan de copia de seguridad en ejecución se detendrán todas las tareas. Por lo tanto, se cancelarán todas las operaciones de tareas.<br><br>**Tarea**<br><br>Haga clic en **Detener**.<br><br>*¿Qué sucede si detengo la tarea?*<br><br>Por lo general, al detener la tarea se cancela su operación (copia de seguridad, recuperación, validación, exportación, conversión, migración). La tarea pasa en primer lugar al estado Deteniendo y después al estado Inactiva. La programación de la tarea, en caso de haberla creado, aún será válida. Para completar la operación, tendrá que ejecutar la tarea de nuevo.<br><br>▪ Tarea de recuperación (desde la copia de seguridad del disco): El volumen de destino se eliminará y el espacio quedará no asignado. También obtendrá el mismo resultado si la recuperación no se realiza correctamente. Para recuperar el volumen "perdido", deberá ejecutar la tarea una vez más.<br><br>▪ tarea de recuperación (desde la copia de seguridad de archivos): La operación cancelada puede ocasionar cambios en la carpeta de destino. Algunos archivos se podrían recuperar pero otros no, dependiendo del momento en el que se haya detenido la tarea. Para recuperar todos los archivos deberá ejecutar la tarea una vez más. |

| | |
|---|---|
| Editar un plan o una tarea | **Plan de copia de seguridad**<br><br>Haga clic en **Editar**.<br><br>La edición del plan de copia de seguridad se realiza de la misma manera que la creación (pág. 207), excepto por las siguientes **limitaciones**:<br><br>No siempre es posible utilizar todas las opciones de esquema cuando se edita un plan de copia de seguridad si el archivo comprimido creado no está vacío (es decir, contiene copias de seguridad).<br><br>1. No es posible cambiar el esquema a "abuelo-padre-hijo" o Torres de Hanói.<br>2. Si se utiliza el esquema de la Torres de Hanói, no es posible cambiar la cantidad de niveles.<br><br>En los demás casos, se puede cambiar el esquema, y debería continuar funcionando como si los archivos comprimidos existentes se hubieran creado bajo el nuevo esquema. En los archivos comprimidos vacíos es posible realizar cualquier tipo de cambio.<br><br>*¿Por qué no puedo editar el plan de copia de seguridad?*<br><br>▪ El plan de copia de seguridad se encuentra en ejecución en ese momento.<br><br>La edición del plan de copia de seguridad actualmente en ejecución no está permitida.<br><br>▪ No tiene el privilegio adecuado<br><br>Un usuario no puede editar planes de otros usuarios sin poseer los privilegios de Administrador.<br><br>▪ El plan de copia de seguridad posee un origen centralizado.<br><br>La edición directa de los planes de copia de seguridad centralizados no está permitida. Debe editar la política de copia de seguridad original.<br><br>**Tarea**<br><br>Haga clic en **Editar**.<br><br>*¿Por qué no puedo editar la tarea?*<br><br>▪ La tarea pertenece a un plan de copia de seguridad.<br><br>Solo las tareas que no pertenecen a un plan de copia de seguridad, tales como las tareas de recuperación, pueden modificarse mediante edición directa. Cuando deba modificar una tarea que pertenece a un plan de copia de seguridad local, edite el plan de copia de seguridad. Las tareas que pertenecen a un plan de copia de seguridad centralizado se pueden modificar al editar la política centralizada que generó el plan. Esto sólo lo puede hacer el administrador del servidor de gestión.<br><br>▪ No tiene el privilegio adecuado<br><br>Un usuario no puede modificar tareas de otros usuarios sin poseer los privilegios de Administrador. |

| | |
|---|---|
| Eliminar un plan o una tarea | **Plan de copia de seguridad**<br>Haga clic en **Eliminar**.<br>*¿Qué sucede si elimino el plan de copia de seguridad?*<br>Si se elimina el plan, se eliminarán todas sus tareas.<br>*¿Por qué no puedo eliminar el plan de copia de seguridad?*<br>▪ El plan de copia de seguridad se encuentra en el estado "En ejecución"<br>El plan de copia de seguridad no podrá eliminarse si al menos una de sus tareas se encuentra en ejecución.<br>▪ No tiene el privilegio adecuado<br>Un usuario no puede eliminar planes de otros usuarios sin poseer los privilegios de Administrador.<br>▪ El plan de copia de seguridad posee un origen centralizado.<br>El administrador del servidor de gestión puede eliminar un plan centralizado al revocar la política de copia de seguridad que dio origen al plan.<br>**Tarea**<br>Haga clic en **Eliminar**.<br>*¿Por qué no puedo eliminar la tarea?*<br>▪ La tarea pertenece a un plan de copia de seguridad.<br>La tarea que pertenece a un plan de copia de seguridad no puede eliminarse por separado del plan. Edite el plan para quitar la tarea o elimine el plan completo.<br>▪ No tiene el privilegio adecuado<br>Un usuario no puede eliminar tareas de otros usuarios sin poseer los privilegios de Administrador. |
| Actualizar la tabla | Haga clic en **Actualizar**.<br>La consola de gestión actualizará la lista de los planes y las tareas de copia de seguridad presentes en el equipo con la información más reciente. Si bien la lista se actualiza automáticamente en función de los eventos, es posible que los datos no se recuperen inmediatamente del equipo gestionado debido a un breve periodo de latencia. La actualización manual garantiza la visualización de los datos más recientes. |

## Filtrar y ordenar planes y tareas de copia de seguridad

| Para | Realizar |
|---|---|
| Ordenar planes y tareas de copia de seguridad por: nombre, estado, estatus, tipo, origen, etc. | Haga clic en el encabezado de la columna para ordenar los planes y las tareas de copia de seguridad por orden ascendente.<br>Haga clic de nuevo para ordenar los planes y las tareas de copia de seguridad por orden descendente. |
| Filtrar planes o tareas por nombre o propietario. | Escriba el nombre del plan o la tarea de copia de seguridad o el nombre del propietario en el campo situado debajo del encabezado de la columna respectiva.<br>Como consecuencia, verá la lista de las tareas cuyos nombres o nombres de propietario coinciden total o parcialmente con el valor introducido. |

| | |
|---|---|
| Filtrar planes y tareas por estado, estatus, tipo, origen, último resultado, programación. | En el campo situado debajo del encabezado de la columna respectiva, seleccione el valor que desee de la lista. |

### Configurar los planes de copias de seguridad y la tabla de tareas

De manera predeterminada, la tabla que se muestra se compone de seis columnas, las demás se encuentran ocultas. También puede ocultar las columnas innecesarias y mostrar las ocultas.

***Mostrar u ocultar columnas***

1. Haga clic con el botón derecho en el encabezado de cualquier columna para abrir el menú contextual. Los elementos del menú que no estén seleccionados corresponden a los encabezados de las columnas presentadas en la tabla.
2. Haga clic sobre los elementos que quiera mostrar/ocultar.

## Ejecutar el plan de copias de seguridad

Se considera que el plan de copias de seguridad se está ejecutando si por lo menos una de sus tareas se está ejecutando. La ventana **Ejecutar plan de copias de seguridad** le permite ejecutar la tarea del plan de copias de seguridad seleccionada manualmente, independientemente de su programación.

***Para ejecutar una tarea del plan de copias de seguridad seleccionado***

1. Seleccione la tarea del plan de copias de seguridad que necesita ejecutar. Para asegurarse de que su selección es la correcta, compruebe la información de la tarea contenida en las pestañas de la parte inferior de la ventana. Esta información también se duplica en la ventana **Detalles de tareas** (pág. 201).
2. Haga clic en **Aceptar**.

## Deshabilitar temporalmente un plan de copias de seguridad.

Es necesario deshabilitar temporalmente un plan de copias de seguridad cuando se mueven archivos comprimidos de una bóveda a otra por medio de un administrador de archivos de terceros.

Únicamente se aplica a los planes de copias de seguridad que usan esquemas de copia de seguridad personalizados.

***Deshabilitar un plan de copias de seguridad.***

1. Haga clic en **Editar**.
2. Entre en la opción de programación del esquema de copias de seguridad y deshabilite la programación para el periodo deseado al cambiar los parámetros de **Fecha de inicio** o **Fecha de finalización**.

## Detalles de la tarea

La ventana **Detalles de la tarea** (también aparece en el panel **Información**) incluye toda la información sobre la tarea seleccionada.

Cuando una tarea requiere la interacción del usuario, aparecerá un mensaje y botones de acción sobre las pestañas. El mensaje contiene una breve descripción del problema. Los botones le permiten reintentar o detener la tarea o el plan de copia de seguridad.

**Tipos de tareas**

La siguiente tabla resume todos los tipos de tareas que existen en Acronis Backup & Recovery 10. Los tipos de tareas a los que pueda acceder dependerán de la edición del producto y del componente del producto al que está conectada la consola.

| Nombre de la tarea | Descripción |
|---|---|
| Copia de seguridad (disco) | Copias de seguridad de discos y volúmenes |
| Copia de seguridad (archivo) | Copias de seguridad de archivos y carpetas |
| Copia de seguridad (máquina virtual) | Copias de seguridad de una máquina virtual completa o sus volúmenes |
| Recuperación (disco) | Recuperación de la copia de seguridad del disco |
| Recuperación (archivo) | Recuperación de archivos y carpetas |
| Recuperación (volumen) | Recuperación de volúmenes de una copia de seguridad del disco |
| Recuperación (MBR) | Recuperación del registro de inicio maestro |
| Recuperación (disco a VM existente) | Recuperación de una copia de seguridad del disco o volumen en una máquina virtual existente |
| Recuperación (disco a nueva VM) | Recuperación de una copia de seguridad del disco o volumen en una máquina virtual nueva |
| Recuperación (máquina virtual existente) | Recuperación de una copia de seguridad de una máquina virtual en una máquina virtual existente |
| Recuperación (máquina virtual nueva) | Recuperación de una copia de seguridad de una máquina virtual en una máquina virtual nueva |
| Validación (archivo comprimido) | Validación de un único archivo comprimido |
| Validación (copia de seguridad) | Validación de copias de seguridad |
| Validación (bóveda) | Validación de todos los archivos comprimidos almacenados en una bóveda |
| Limpieza | Eliminación de las copias de seguridad de un archivo de copia de seguridad de acuerdo con las reglas de retención |
| Creación de ASZ | Creación de Acronis Secure Zone |
| Gestión de ASZ | Modificación del tamaño, cambio de la contraseña, eliminación de Acronis Secure Zone |
| Gestión del disco | Operaciones de gestión del disco |
| Compactando | Tarea de servicio realizada en un nodo de almacenamiento |
| Indexando | La tarea de deduplicación realizada por el nodo de almacenamiento en la bóveda se completa luego de realizada la copia de seguridad |

Según el tipo de tarea y si se está ejecutando o no, aparecerá una combinación de las siguientes pestañas:

## Tarea

La pestaña **Tarea** es igual para todos los tipos de tareas. Proporciona información general sobre la tarea seleccionada.

### Archivo comprimido

La pestaña **Archivo comprimido** está disponible para las tareas de copia de seguridad, de validación del archivo comprimido y de limpieza.

Proporciona información sobre el archivo comprimido: nombre, tipo, tamaño, ubicación de almacenamiento, etc.

### Crear copia de seguridad

La pestaña **Copia de seguridad** está disponible para las tareas de recuperación, de validación de la copia de seguridad y de exportación.

Proporciona detalles sobre la copia de seguridad seleccionada: cuándo se creó, su tipo (completa, incremental, diferencial), información sobre el archivo comprimido y la bóveda en la que se encuentra la copia de seguridad.

### Configuraciones

La pestaña **Configuración** muestra información sobre la programación y las opciones cambiadas en comparación con los valores predeterminados.

### Progreso

La pestaña **Progreso** está disponible mientras se está ejecutando la tarea. Es igual para todos los tipos de tareas. Esta pestaña proporciona información sobre el progreso de la tarea, el tiempo transcurrido y otros parámetros.

## Detalles del plan de copias de seguridad

La ventana de **Detalles del plan de copias de seguridad** (también duplicada en el panel **Información**) reúne en cuatro pestañas toda la información del plan de copias de seguridad seleccionado.

El mensaje respectivo aparecerá en la parte superior de las pestañas si una de las tareas del plan necesita la interacción del usuario. Contiene una descripción breve del problema y de los botones de acción que le permiten seleccionar la acción adecuada o detener el plan.

### Plan de copias de seguridad

La pestaña del **plan de copias de seguridad** proporciona la siguiente información general sobre el plan seleccionado:

- **Nombre**, nombre del plan de copias de seguridad
- **Origen**, si el plan se ha creado en el equipo gestionado utilizando la gestión directa (origen local) o si ha aparecido en el equipo como resultado de la implementación de una política de copias de seguridad desde el servidor de gestión (origen centralizado).
- **Política** (para planes de copias de seguridad con origen centralizado), nombre de la política de plan de copias de seguridad, cuya implementación ha creado el plan de copias de seguridad.
- **Cuenta,** el nombre de la cuenta con la que se ejecuta el plan
- **Propietario**, el nombre del usuario que ha creado o modificado el plan la última vez
- **Estado**, estado de ejecución (pág. 193) del plan de copias de seguridad.
- **Estatus**, estatus (pág. 194) del plan de copias de seguridad.
- **Programación**, si la tarea es programada o se ha configurado para iniciarse manualmente.
- **Última copia de seguridad**, cuánto tiempo ha pasado desde la última copia de seguridad.
- **Creación**, fecha de creación del plan copia de seguridad.

- **Comentarios**, descripción del plan (si está disponible).

### Origen

La pestaña **Origen** brinda la siguiente información sobre los datos seleccionados para la copia de seguridad:

- **Tipo de origen**, el tipo de datos (pág. 210) seleccionados para la copia de seguridad.
- **Elementos a incluir en la copia de seguridad**, elementos seleccionados para incluir en la copia de seguridad y su tamaño.

### Destino

La pestaña **Destino** brinda la siguiente información:

- **Ubicación**, nombre de la bóveda o ruta que lleva hasta la carpeta en la que está almacenado el archivo comprimido.
- **Nombre del archivo comprimido**, nombre del archivo comprimido.
- **Comentarios del archivo comprimido**, comentarios sobre el archivo comprimido (si están disponibles).

### Ajustes

La pestaña **Ajustes** muestra la siguiente información:

- **Esquema de copia de seguridad**, el esquema de copia de seguridad seleccionado y todos sus ajustes y programaciones.
- **Validación** (si está seleccionado), eventos que se han llevado a cabo antes o después de la validación y de la programación de la validación.
- **Opciones de copia de seguridad**, opciones de copia de seguridad que se han modificado sin respetar los valores predeterminados.

## 6.1.3 Registro

El Registro almacena el historial de las operaciones realizadas por Acronis Backup & Recovery 10 o las acciones llevadas a cabo por el usuario en el equipo utilizando el programa. Por ejemplo, cuando un usuario edita una tarea, se añade la entrada respectiva al registro. Cuando el programa ejecuta una tarea, añade numerosas entradas. Con el registro, se pueden examinar las operaciones y los resultados de la ejecución de las tareas, incluyendo los motivos de cualquier fallo, en caso de producirse.

### Modo de trabajo con las entradas del registro

- Utilice los filtros para mostrar las entradas del registro que desee ver. También puede ocultar las columnas innecesarias y mostrar las ocultas. Para obtener más detalles, consulte la sección Filtrar y ordenar las entradas del registro (pág. 206).
- En la tabla del registro, seleccione la(s) entrada(s) del registro sobre la(s) que quiere llevar a cabo una acción. Para obtener más detalles, consulte la sección Acciones sobre las entradas del registro (pág. 205).
- Para revisar información detallada sobre la entrada del registro seleccionada, utilice el panel **Información**. De manera predeterminada, el panel se encuentra minimizado. Para expandir el panel, haga clic en la flecha tipo  . El contenido del panel también está duplicado en la ventana **Detalles de entrada del registro** (pág. 206).

### Abrir el Registro con las entradas prefiltradas del registro

Si ha seleccionado elementos en otras vistas de administración (**Tablero**, **Planes y tareas de copia de seguridad**), puede abrir la vista del **Registro** con entradas de registro prefiltradas para el elemento en cuestión. Así, no será necesario que configure los filtros en la tabla de registro.

| Vista | Acción |
|---|---|
| **Tablero** | En el calendario, haga clic con el botón derecho en cualquiera de las fechas resaltadas y después seleccione **Ver registro**. La vista **Registro** aparece con la lista de entradas del registro que ya se han filtrado por la fecha en cuestión. |
| **Planes y tareas de la copia de seguridad** | Seleccione un plan de copias de seguridad o una tarea y después haga clic en **Ver registro**. La vista Registro mostrará una lista de las entradas del registro relacionadas con el plan o tarea seleccionados. |

## Acciones en las entradas del registro

Todas las operaciones descritas a continuación se llevan a cabo haciendo clic en los elementos correspondientes en la **barra de herramientas** del registro. Todas estas operaciones se pueden llevar a cabo con el menú contextual (haciendo clic con el botón derecho en la entrada del registro), o con la barra **acciones del registro** (en el panel **Acciones y herramientas**).

A continuación se muestra una guía para llevar a cabo acciones en las entradas del registro.

| Operación | Procedimiento |
|---|---|
| Seleccionar una entrada del registro | Haga clic en ella. |
| Seleccionar varias entradas del registro | ▪ *no contiguas*: mantenga pulsada la tecla **CTRL** y haga clic en las entradas una a una<br>▪ *contiguas*: seleccione una entrada, mantenga pulsada la tecla **MAYÚSCULAS** y haga clic en otra entrada. Así se seleccionarán todas las entradas entre la primera y la última selección. |
| Ver información sobre las entradas del registro | 1. Seleccione una entrada del registro<br>2. Realice uno de los siguientes procedimientos:<br>▪ Haga clic en **Ver detalles**. Los detalles de las entradas del registro se mostrarán en una ventana diferente.<br>▪ Expanda el Panel de información haciendo clic en la flecha tipo. |
| Guardar las entradas del registro seleccionadas en un archivo comprimido. | 1. Seleccione una o varias entradas del registro.<br>2. Haga clic en **Guardar la selección en archivo**.<br>3. En la ventana abierta, especifique la ruta y un nombre para el archivo. |
| Guardar todas las entradas del registro a un archivo. | 1. Asegúrese de que no se han configurado filtros.<br>2. Haga clic en **Guardar todo en archivo**.<br>3. En la ventana abierta, especifique la ruta y un nombre para el archivo. |
| Guardar todas las entradas filtradas del registro en un archivo comprimido. | 1. Configure los filtros para obtener una lista de las entradas del registro que satisfagan los criterios.<br>2. Haga clic en **Guardar todo en archivo**.<br>3. En la ventana abierta, especifique la ruta y un nombre para el archivo. |

| | |
|---|---|
| | Como consecuencia, se guardarán las entradas del registro de la lista. |
| Eliminar todas las entradas del registro. | Haga clic en **Limpiar registro**.<br>Todas las entradas del registro se eliminarán del mismo y se creará una nueva entrada. Esta contendrá información relacionada con quién eliminó las entradas y cuándo. |

## Filtrado y clasificación de entradas del registro

A continuación se muestra una guía para filtrar y ordenar las entradas del registro.

| Operación | Procedimiento |
|---|---|
| Mostrar las entradas del registro para un periodo de tiempo determinado | 1. En el campo **De**, seleccione la fecha a partir de la cual se mostrarán las entradas del registro.<br>2. En el campo **A**, seleccione la fecha hasta la cual se mostrarán las entradas del registro. |
| Filtrar las entradas del registro por tipo | Active o desactive los siguientes botones de la barra de herramientas:<br>para filtrar mensajes de error<br>para filtrar mensajes de advertencia<br>para filtrar mensajes de información |
| Filtrar entradas del registro por tipo de plan de copia de seguridad original o entidad gestionada. | En el encabezado de la columna **Plan de copia de seguridad** (o **Tipo de entidad gestionada**), seleccione el plan de copia de seguridad o el tipo de entidad gestionada de la lista. |
| Filtrar entradas del registro por tarea, entidad gestionada, equipo, código o propietario. | Escriba el valor requerido (nombre de la tarea, del equipo, del propietario, etc.) en el campo situado debajo del encabezado de la columna respectiva.<br>Como consecuencia, verá la lista de las entradas del registro que coinciden total o parcialmente con el valor introducido. |
| Ordenar las entradas del glosario por fecha y hora | Haga clic en el encabezado de la columna para ordenar las entradas del registro por orden ascendente. Haga clic de nuevo para ordenar las entradas del registro por orden descendente. |

### Configurar la tabla del registro

De manera predeterminada, la tabla muestra siete columnas, las otras están ocultas. Si fuera necesario, puede ocultar las columnas visibles y mostrar las ocultas.

#### *Mostrar u ocultar columnas*

1. Haga clic con el botón derecho en el encabezado de cualquier columna para abrir el menú contextual. Los elementos del menú que no estén seleccionados corresponden a los encabezados de las columnas presentadas en la tabla.
2. Haga clic sobre los elementos que quiera mostrar/ocultar.

## Detalles de la entrada del registro

Muestra información detallada de la entrada del registro seleccionada y permite copiarla al portapapeles.

Para copiar los detalles, haga clic en el botón **Copiar al portapapeles**.

Campos de datos de entrada del registro.

Una entrada del registro local contiene los siguientes campos de datos:

- **Tipo**: tipo de evento (Error; Advertencia; Información)
- **Fecha**: fecha y hora en la que ocurre el evento
- **Plan de copias de seguridad**: el plan de copias de seguridad con el que se relaciona el evento (si hubiera)
- **Tarea**: tarea con la que se relaciona el evento (si hubiera)
- **Código**: el código de programa del evento. Cada tipo de evento del programa tiene su propio código. El código se compone de un número entero que puede utilizar el servicio de asistencia de Acronis para solucionar el problema.
- **Módulo**: número del módulo del programa en el que tuvo lugar el evento. Se trata de un número entero que puede utilizar el servicio de asistencia de Acronis para solucionar el problema.
- **Propietario**: nombre de usuario del propietario del plan de copias de seguridad (solo para el sistema operativo)
- **Mensaje**: una descripción textual del evento.

La información de la entrada del registro que se copiará tendrá el siguiente aspecto:

```
--------------------------Detalles de entrada del registro--------------------
-------
Tipo:                           Información
Fecha y hora:                   DD.MM.AAAA HH:MM:SS
Plan de copias de seguridad:    Nombre del plan de copias de seguridad
Tarea:                          Nombre de la tarea
Mensaje:                        Descripción de la operación
Código:                         12(3x45678A)
Módulo:                         Nombre del módulo
Propietario:                    Propietario del plan
------------------------------------------------------------------------
```

La presentación de la fecha y la hora depende de su ajuste local.

## 6.2 Crear un plan de copias de seguridad

Antes de crear su primer plan de copia de seguridad (pág. 411), familiarícese con los conceptos básicos (pág. 27) utilizados en Acronis Backup & Recovery 10.

***Para crear un plan de copias de seguridad, siga los siguientes pasos.***

### General

**Nombre del plan**

[Opcional] Introduzca un solo nombre para el plan de copias de seguridad. Un nombre lógico le permitirá identificar este plan de entre otros.

**Credenciales del plan** (pág. 210)

[Opcional] El plan de copias de seguridad se ejecutará en nombre del usuario que haya creado el plan. Si es necesario, es posible cambiar las credenciales de las cuentas del plan. Para acceder a esta opción, seleccione la casilla de verificación **Vista avanzada**.

**Comentarios**

[Opcional] Escriba una descripción del plan de copias de seguridad. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

**Etiqueta**

[Opcional] Marque una etiqueta de texto para el equipo al que va a realizar la copia de seguridad. La etiqueta puede usarse para identificar el equipo en diversos escenarios. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

## Qué incluir en la copia de seguridad

**Tipo de fuente** (pág. 210)

Seleccione el tipo de datos para incluir en la copia de seguridad. El tipo de datos depende de los agentes instalados en el equipo.

**Elementos para incluir en la copia de seguridad** (pág. 211)

Especifique los elementos de datos que incluirá en la copia de seguridad. La lista de elementos para incluir en la copia de seguridad depende del tipo de datos especificados con anterioridad.

**Credenciales de acceso** (pág. 212)

[Opcional] Proporcione credenciales para los datos de origen si las cuentas del plan no tienen permisos de acceso a los datos. Para acceder a esta opción, seleccione la casilla de verificación **Vista avanzada**.

**Exclusiones** (pág. 213)

[Opcional] Establezca exclusiones para los tipos de archivos específicos de los cuales no desea realizar una copia de seguridad. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

## Dónde realizar copias de seguridad

**Archivo comprimido** (pág. 214)

Especifique la ruta en la que los archivos comprimidos de la copia de seguridad se almacenarán, así como el nombre del archivo comprimido. Se recomienda que el nombre del archivo comprimido sea único dentro de la ubicación. El nombre de archivo comprimido predeterminado es Archivo(N), donde N es el número de secuencia del archivo comprimido en la ubicación que se ha seleccionado.

**Nombre los archivos de copia de seguridad utilizando el nombre del archivo comprimido tal como Acronis True Image Echo, en vez de utilizar nombres generados automáticamente**

*No disponible al hacer la copia de seguridad en una bóveda gestionada, cinta Acronis Secure Zone o Acronis Online Backup Storage.*

[Opcional] Seleccione esta casilla de verificación si desea utilizar nombres de archivos comprimidos simplificados para los archivos comprimidos de la copia de seguridad.

**Credenciales de acceso** (pág. 221)

[Opcional] Proporcione credenciales para la ubicación si la cuenta del plan no tiene permisos de acceso a la ubicación. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

**Comentarios de archivo comprimido**

[Opcional] Introduzca comentarios en el archivo comprimido. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

## ¿Cómo crear copias de seguridad?

**Esquema de copias de seguridad** (pág. 221)

Especifique dónde y con qué frecuencia realizar copias de seguridad de sus datos, establezca durante cuánto tiempo mantener los archivos comprimidos de la copia de seguridad en la ubicación seleccionada y configure una programación para el procedimiento de limpieza del

archivo comprimido. Utilice esquemas de copia de seguridad optimizados y reconocidos como Abuelo-Padre-Hijo (GFS) o Torres de Hanoi y cree un esquema de copia de seguridad personalizado, o realice copias de seguridad solo una vez.

### Validación de archivos comprimidos

**Cuándo validar** (pág. 232)

[Opcional] Defina cuándo y cada cuánto tiempo realizará la validación y si se desea validar todo el archivo comprimido o la última copia de seguridad del archivo.

### Opciones de la copia de seguridad

**Configuraciones**

[Opcional] Configure los parámetros de la operación de copia de seguridad, como los comandos pre/post copia de seguridad, el ancho de banda de red máximo asignado para el flujo de copia de seguridad o el nivel de compresión del archivo de copia de seguridad. Si no hace nada en esta sección, se usarán los valores predeterminados (pág. 96).

Después de que se modifique cualquiera de las configuraciones con respecto al valor predeterminado, aparecerá una nueva línea que mostrará el valor recientemente establecido. El estado de la configuración cambia de **Predeterminada** a **Personalizada**. Si modifica nuevamente la configuración, la línea mostrará el nuevo valor, a menos que el nuevo valor sea el predeterminado. Cuando se fija un valor predeterminado, la línea desaparece. Por lo tanto, solo son visibles los valores que son diferentes a los valores predeterminados en esta sección de la página **Crear plan de copias de seguridad**.

Para restablecer toda la configuración a los valores predeterminados, haga clic en **Restablecer a los valores predeterminados**.

### Conversión a VM

Se aplica a: Copias de seguridad de **disco/volumen**, copias de seguridad de **Equipos virtuales completos** o **Volúmenes de un equipo virtual**

No disponible en equipos cuyo sistema operativo es de Linux

Al configurar una conversión normal, se obtiene una copia del servidor o estación de trabajo en un equipo virtual que puede encenderse fácilmente si el equipo original falla. El mismo agente que realiza la copia de seguridad o un agente instalado en otro equipo pueden realizar la conversión. Si opta por la segunda opción, debe almacenar el archivo comprimido en una ubicación compartida, como una carpeta de red o una bóveda gestionada, para que el otro equipo tenga acceso al mismo.

**Cuándo convertir** (pág. 232)

[Opcional] Especifique si deben convertirse todas las copias de seguridad completas, incrementales o diferenciales o la última copia de seguridad que se creó según la programación. Si es necesario, especifique la programación de la conversión.

**Servidor** (pág. 233)

Especifique el equipo que realizará la conversión. El equipo debe tener instalado Acronis Backup & Recovery 10 Agent para Windows, Agent para ESX/ESXi o Agent para Hyper-V.

**Servidor de virtualización** (pág. 233)

Aquí debe seleccionar el tipo y la ubicación del equipo virtual resultante. Las opciones disponibles dependerán del servidor que haya seleccionado en el paso anterior.

**Almacenamiento** (pág. 233)

Escoja el almacenamiento en el servidor de virtualización o la carpeta en la que deben colocarse los archivos del equipo virtual.

**VMs resultante**

Especifique el nombre del equipo virtual.

Tras realizar todos los pasos necesarios, haga clic en **Aceptar** para crear el plan de copias de seguridad.

Después, es posible que se le pida introducir una contraseña (pág. 210).

El plan que ha creado podrá examinarse y gestionarse en la vista **Planes y tareas de la copia de seguridad** (pág. 192).

### 6.2.1 ¿Por qué este programa me pide la contraseña?

Una tarea programada o pospuesta debe ejecutarse sin importar si los usuarios están conectados al sistema. En caso de que no haya especificado explícitamente las credenciales bajo las cuales se ejecutarán las tareas, el programa propone utilizar su cuenta. Introduzca su contraseña, especifique otra cuenta o cambie el inicio programado a manual.

### 6.2.2 Credenciales del plan de copias de seguridad

Proporcione credenciales para la cuenta con la que se ejecutarán las tareas del plan.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Ejecutar bajo el usuario actual**

     Las tareas se ejecutarán bajo las credenciales de la cuenta con las que el usuario que inicia las tareas haya iniciado la sesión. Si alguna de las tareas debe ejecutarse según la programación, se le solicitará la contraseña de usuario actual al finalizar la creación de la tarea.
   - **Utilizar las siguientes credenciales**

     Las tareas se ejecutarán siempre con las credenciales que especifique, ya sea que se inicie manualmente o según la programación.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña para la cuenta.
2. Haga clic en **Aceptar**.

Para obtener más información sobre las operaciones disponibles según los privilegios del usuario, consulte la sección Privilegios de usuario en un equipo gestionado (pág. 33).

### 6.2.3 Tipo de fuente

Seleccione el tipo de datos del que desea que haya una copia de seguridad en el equipo gestionado. La lista de tipos de datos disponible depende de los agentes ejecutándose en la máquina:

**Archivos**

Disponible si Acronis Backup & Recovery 10 Agent para Windows (o para Linux) está instalado.

Seleccione esta opción para realizar la copia de seguridad de archivos y carpetas específicas.

Si no le preocupa la recuperación del sistema operativo con todos los ajustes y las aplicaciones instalados, pero planea mantener seguros solo algunos datos (el proyecto en curso, por ejemplo), seleccione la copia de seguridad de archivo. Esto reducirá el tamaño del archivo comprimido, ahorrando así espacio de almacenamiento.

**Discos/volúmenes**

Disponible si el Acronis Backup & Recovery 10 Agent para Windows (o para Linux) está instalado.

Seleccione esta opción para realizar la copia de seguridad de discos y/o volúmenes. Para poder realizar la copia de seguridad de discos o volúmenes, debe tener privilegios de Administrador o de operador de copias de seguridad.

Realizar la copia de seguridad de discos y volúmenes le permite recuperar el sistema completo en caso de que suceda un fallo en el hardware o daño grave de los datos. El procedimiento de copia de seguridad es mucho más rápido que la copia de archivos y puede acelerar considerablemente el proceso de copia de seguridad cuando es necesario asegurar grandes volúmenes de datos.

***Nota para los usuario de Linux:*** *Le recomendamos que desmonte los volúmenes que no contengan sistemas de archivos no diarios, como el sistema de archivos ext2, antes de realizar una copia de seguridad de los mismos. De lo contrario, estos volúmenes pueden contener archivos dañados tras la recuperación. Es posible que la recuperación de estos volúmenes falle.*

### 6.2.4 Elementos para incluir en la copia de seguridad

Los elementos para incluir en la copia de seguridad dependen del tipo de origen (pág. 210) seleccionado con anterioridad.

#### Seleccionar discos y volúmenes

***Especificar los discos o volúmenes para incluir en la copia de seguridad***

1. Seleccione las casillas de verificación para los discos o volúmenes para incluir en la copia de seguridad. Puede seleccionar un conjunto aleatorio de discos y particiones.

   *Si su sistema operativo y su cargador residen en diferentes volúmenes, debe incluir siempre ambas particiones en la imagen. Los volúmenes debe recuperarse juntos, de otro modo existe el riesgo de que no inicie el sistema operativo.*

   En Linux, los volúmenes lógicos y los dispositivos MD se muestran como **GPT y dinámicos**. Para obtener más información acerca de cómo hacer la copia de seguridad de dichos volúmenes y dispositivos, vaya a "Realización de copias de seguridad de volúmenes LVM y dispositivos MD (Linux)".
2. [Opcional] Para crear una copia exacta de un disco o volumen en un nivel físico, seleccione la casilla de verificación **Copia de seguridad sector por sector** . La copia de seguridad resultante tendrá el mismo tamaño que el disco objeto de la copia de seguridad (si la opción de **Nivel de compresión** está establecida como **Ninguna**). Utilice la copia de seguridad sector por sector para realizar copias de seguridad de unidades con sistemas de archivos no reconocidos o incompatibles, o formatos de datos de terceros.
3. Haga clic en **Aceptar**.

### ¿Qué almacena una copia de seguridad de un disco o volumen?

Para sistemas de archivo compatibles, con la opción de sector por sector desactivada, una copia de seguridad de un disco o volumen almacena únicamente aquellos sectores que contienen datos. Esto reduce el tamaño de la copia de seguridad resultante y acelera las operaciones de copia de seguridad y recuperación.

**Windows**

Las copias de seguridad no incluyen el archivo de intercambio (pagefile.sys) ni el archivo que mantiene el contenido de la memoria RAM cuando el equipo está en estado de hibernación (hiberfil.sys). Después de la recuperación, los archivos se pueden volver a crear en el lugar apropiado con el tamaño cero.

Una copia de seguridad de volúmenes almacena todos los archivos y las carpetas del volumen seleccionado, independientemente de sus atributos (incluidos los archivos ocultos y del sistema), el registro de inicio, la tabla de asignación de archivos (FAT) si existe, la raíz y el registro cero del disco duro con el registro de inicio maestro (MBR). El código de inicio de los volúmenes GPT no se incluye en la copia de seguridad.

Un copia de seguridad del disco almacena todos los volúmenes del disco seleccionado (incluidos volúmenes ocultos como las particiones de mantenimiento del proveedor) y el registro cero con el registro de inicio maestro.

**Linux**

Una copia de seguridad de volúmenes almacena todos los archivos y las carpetas del volumen seleccionado, independientemente de sus atributos, un registro de inicio y el superbloque del sistema de archivos.

Una copia de seguridad del disco almacena todos los volúmenes del disco y también el registro cero junto con el registro de inicio maestro.

### Seleccionar archivos y carpetas

***Seleccionar los archivos o carpetas para incluir en la copia de seguridad***

1. Expanda el árbol de las carpetas locales para poder ver las carpetas anidadas y sus archivos.
2. Seleccione un elemento al activar la casilla de verificación correspondiente en el árbol. Seleccionar una casilla de verificación para una carpeta significa que todo su contenido (archivos y carpetas) formará parte de la copia de seguridad. Ocurrirá lo mismo para el caso de los nuevos archivos nuevos que aparezcan en el futuro.

   *Una copia de seguridad basada en archivos no es suficiente para recuperar el sistema operativo. Para recuperar el sistema operativo, debe realizar una copia de seguridad del disco.*

   Utilice la tabla de la parte derecha de la ventana para explorar y seleccionar los elementos anidados. Al activar la casilla de verificación al lado del encabezado de la columna **Nombre**, automáticamente se seleccionan todos los elementos de la tabla. Al desactivar esta casilla de verificación, se anula automáticamente la selección de todos los elementos.
3. Haga clic en **Aceptar**.

## 6.2.5 Credenciales de acceso a los datos de origen

Especifique las credenciales que se necesitarán para el acceso a los datos que va a incluir en la copia de seguridad.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:

- **Usar las credenciales del plan**

  El programa accederá a los datos de origen mediante las credenciales del plan de copias de seguridad especificado en la sección General.

- **Utilice las siguientes credenciales.**

  El programa accederá a los datos de origen mediante las credenciales que especifique.Utilice esta opción si la cuenta del plan no dispone de permisos de acceso a los datos.

  Especifique:

  - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
  - **Contraseña**. La contraseña de la cuenta.

2. Haga clic en **Aceptar**.

### 6.2.6 Exclusiones

[Opcional] Configure exclusiones para tipos de archivo específicos para los cuales no desea realizar copias de seguridad. Por ejemplo, quizá desee que los archivos y carpetas ocultos y del sistema, así como los archivos con extensiones específicas, no se almacenen en el archivo comprimido.

***Para especificar los archivos y carpetas que desea excluir:***

Configure alguno de los siguientes parámetros:

- **Excluir todos los archivos y carpetas ocultos**

  Esta opción está vigente sólo para sistemas de archivos compatibles con Windows. Seleccione esta casilla de verificación para omitir archivos y carpetas con el atributo **Oculto**. Si una carpeta está **Oculta**, se excluirán todos sus contenidos, incluso los archivos que no se encuentran **Ocultos**.

- **Excluir todos los archivos y carpetas del sistema**

  Esta opción está vigente sólo para sistemas de archivos compatibles con Windows. Seleccione esta casilla de verificación para omitir archivos y carpetas con el atributo **Sistema**. Si una carpeta tiene el atributo **Sistema**, se excluirán todos sus contenidos, incluso los archivos que no tengan el atributo **Sistema**.

*Puede ver los atributos del archivo o de la carpeta en las propiedades del archivo/carpeta o mediante el comando **atrib**. Para obtener más información, consulte el Centro de Servicio Técnico y Ayuda de Windows.*

- **Excluir los archivos que coincidan con los siguientes criterios**

  Seleccione esta casilla de verificación para omitir los archivos y las carpetas cuyos nombres en la lista coincidan con alguno de los criterios, llamados máscaras del archivo; utilice los botones **Agregar**, **Editar**, **Eliminar** y **Eliminar todos** para crear la lista de máscaras del archivo.

  Puede utilizar uno o más caracteres comodín * y ? en una máscara de archivo:

  El asterisco (*) sustituye de cero a más caracteres del nombre del archivo; por ejemplo, la máscara de archivo Doc*.txt genera archivos Doc.txt y Document.txt

  El signo de interrogación (?) substituye a un único carácter; por ejemplo, la máscara de archivo Doc?.txt genera archivos Doc1.txt y Docs.txt, pero, por el contrario, no general archivos Doc.txt o Doc11.txt

Para excluir una carpeta especificada por una ruta que contiene la letra de unidad, agregue una barra invertida (\) al nombre de carpeta en el criterio; por ejemplo: C:\Finance\

**Ejemplos de exclusión**

| Criterio | Ejemplo | Descripción |
|---|---|---|
| **Windows y Linux** | | |
| Por nombre | F.log<br>F | Excluye todos los archivos denominados "F.log"<br>Excluye todas las carpetas denominadas "F" |
| Por máscara (*) | *.log<br>F* | Excluye todos los archivos con la extensión .log<br>Excluye todos los archivos y carpetas cuyos nombres comiencen con "F" (como carpetas F, F1 y archivos F.log, F1.log) |
| Por máscara (?) | F???.log | Excluye todos los archivos .log cuyos nombres contengan cuatro símbolos y comiencen con "F" |
| **Windows** | | |
| Por ruta de archivo | C:\Finance\F.log | Excluye el archivo denominado "F.log" ubicado en la carpeta C:\Finance |
| Por ruta de carpeta | C:\Finance\F\ | Excluye la carpeta C:\Finance\F (asegúrese de especificar la ruta completa, comenzando por la letra de unidad) |
| **Linux** | | |
| Por ruta de archivo | /home/user/Finance/F.log | Excluye el archivo denominado "F.log", ubicado en la carpeta /home/user/Finance |
| Por ruta de carpeta | /home/user/Finance/ | Excluye la carpeta /home/user/Finance |

## 6.2.7 Archivo comprimido

Especifique dónde se almacenará el archivo comprimido y el nombre del archivo comprimido.

### 1. Seleccionar el destino

Introduzca la ruta de destino completa en el campo **Ruta** o seleccione el destino deseado en el árbol de carpetas.

- Para hacer una copia de seguridad de datos en Acronis Online Backup Storage, haga clic en **Iniciar sesión** y especifique las credenciales de acceso al almacenamiento en línea. Después, expanda el grupo **Almacenamiento de copia de seguridad en línea** y seleccione la cuenta.

  Antes de hacer una copia de seguridad del almacenamiento en línea, necesitará comprar una suscripción para el servicio de almacenamiento en línea y activar la suscripción en el(los) equipo(s) de los que desea realizar una copia de seguridad. La opción de copia de seguridad en línea no está disponible en Linux ni bajo dispositivo de inicio.

  *Acronis Backup & Recovery 10 Online es posible que no esté disponible en su región. Para obtener más información, haga clic aquí: http://www.acronis.es/my/backup-recovery-online/.*

- Para realizar copias de seguridad de datos en una bóveda centralizada, amplíe el grupo **Centralizado** y haga clic en la bóveda.
- Para realizar copias de seguridad de datos en una bóveda personal, amplíe el grupo **Personalizado** y haga clic en la bóveda.
- Para realizar copias de seguridad de datos en una carpeta local del equipo, amplíe el grupo **Carpetas locales** y haga clic en la carpeta correspondiente.

- Para realizar copias de seguridad en una red compartida, amplíe el grupo **Carpetas de red**, seleccione el equipo en red correspondiente y después haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

  ***Nota para los usuario de Linux:*** *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como* ***/mnt/share****, seleccione este punto de montaje en lugar de la propia red compartida.*

- Para realizar copias de seguridad de datos en un servidor **FTP** o **SFTP**, escriba el nombre o dirección del servidor en el campo **Ruta** de la siguiente manera:

  **ftp://ftp_server:port _number** o **sftp://sftp_server:port number**

  Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

  Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

  Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

  *Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

- Para realizar copias de seguridad de datos en un dispositivo de cinta conectado a nivel local, amplíe el grupo **Unidades de cinta** y haga clic en el dispositivo correspondiente.

### 2. Uso de la tabla de archivos comprimidos

Para asistirle en la elección del destino correcto, la tabla muestra los nombres de los archivos comprimidos contenidos en cada una de las ubicaciones que seleccione. Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.

### 3. Nombrar un archivo comprimido nuevo

Una vez que seleccione el destino del archivo comprimido, el programa genera un nombre para el nuevo archivo comprimido y lo muestra en el campo **Nombre**. El nombre aparece normalmente como Archivo(1). El nombre generado es único dentro de la ubicación seleccionada. Si está satisfecho con el nombre generado automáticamente, haga clic en **Aceptar**. De lo contrario, introduzca otro nombre único y haga clic en **Aceptar**.

### Realizar una copia de seguridad en un archivo comprimido existente

Puede configurar el plan de copia de seguridad para realizar una copia de seguridad a un archivo comprimido existente. Para hacerlo, seleccione el archivo comprimido en la tabla de archivos comprimidos o escriba el nombre del archivo comprimido en el campo **Nombre**. Si el archivo comprimido está protegido con una contraseña, el programa le pedirá que la introduzca en una ventana emergente.

Al seleccionar un archivo comprimido existente, se está entrometiendo en el área de otro plan de copia de seguridad que utiliza el archivo comprimido. Esto no será un problema si el otro plan se ha interrumpido, pero en general debería seguir la regla: "un plan de copia de seguridad - un archivo comprimido". Lo contrario no provocará que el programa deje de funcionar pero no es práctico ni eficiente, a excepción de algunos casos específicos.

**Por qué dos o más planes no deberían realizar copias de seguridad del mismo archivo comprimido**

1. Realizar copias de seguridad de orígenes diferentes en el mismo archivo comprimido dificulta la utilización del archivo comprimido desde el punto de vista de la funcionalidad. Cuando se trata de recuperación, cada segundo es valioso, pero puede perderse en el contenido del archivo comprimido.

   Los planes de copias de seguridad que funcionan con el mismo archivo comprimido deberían realizar copias de seguridad de los mismos elementos de datos (por ejemplo, ambos planes realizan una copia de seguridad del volumen C).
2. Aplicar múltiples reglas de retención a un archivo comprimido hace que el contenido del mismo sea impredecible en cierta medida. Como cada una de las reglas se aplicarán al archivo comprimido completo, las copias de seguridad correspondientes a un plan de copias de seguridad se pueden borrar con facilidad junto con las copias de seguridad correspondientes al otro. Particularmente, no debe esperar el comportamiento clásico de los esquemas de copia de seguridad GFS y Torres de Hanói.

   Por lo general, cada plan de copias de seguridad complejo debe realizar la copia de seguridad de su propio archivo comprimido.

### 6.2.8 Asignación simplificada de nombre a los archivos de copia de seguridad

Si selecciona la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...**:

- El nombre de archivo de la primera copia de seguridad completa consistirá en el nombre del archivo comprimido; por ejemplo: **MyData.tib.** Los nombres de los archivos de posteriores copias de seguridad (incrementales o diferenciales) tendrán un índice; por ejemplo: **MyData2.tib**, **MyData3.tib**y así sucesivamente.

  Este sencillo esquema de nombres le permite crear una imagen portátil de un equipo en un medio extraíble o mover las copias de seguridad a una ubicación diferente utilizando un comando.
- Antes de crear una nueva copia de seguridad completa, el software eliminará el archivo comprimido entero e iniciará uno nuevo.

  Este comportamiento es muy útil cuando rote discos duros USB y cuando quiere que cada disco mantenga una sola copia de seguridad completa (pág. 218) o todas las copias de seguridad creadas a lo largo de una semana (pág. 219). Pero puede acabar sin ninguna copia de seguridad en el caso de que falle una copia de seguridad completa de una sola unidad.

  Este comportamiento puede ser eliminado si agrega la [Date] variable (pág. 220) al nombre de archivo comprimido.

Si *no* selecciona la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...**:

- Cada copia de seguridad tendrá un único nombre de archivo con el sello de tiempo exacto y el tipo de copia de seguridad; por ejemplo: **MyData_2010_03_26_17_01_38_960D.tib**. Esta forma estándar de nombre archivos permite una gama más amplia de destinos de copias de seguridad y de esquemas de copias de seguridad.

**Restricciones**

Al utilizar la simplificación de nombre de archivos, la siguiente funcionalidad deja de estar disponible:

- Configuración de copias de seguridad completas, incrementales y diferenciales dentro de un único plan de copias de seguridad. Necesita crear planes de copias de seguridad separados para cada tipo de copia de seguridad.
- Copia de seguridad de una bóveda gestionada, cinta Acronis Secure Zone o Acronis almacenamiento de copias de seguridad en línea
- Configuración de reglas de retención
- Configuración de una conversión regular de copias de seguridad a una máquina virtual
- Utilización de numerales al final del nombre del archivo comprimido

***Consejo.*** *Los sistemas de archivos FAT16, FAT32 y NTFS no permiten los siguientes caracteres en el nombre de archivo: barra invertida (\), barra (/), dos puntos (:), asterisco (*), signo de interrogación (?), comillas ("), signo menos que (<), signo más que (>), y barra vertical (|).*

## Ejemplos de uso

Esta sección proporciona ejemplos de cómo puede usar la simplificación de nombres de archivos.

### Ejemplo 1. Realice una copia de seguridad diaria reemplazando el antiguo

Considere el siguiente escenario:

- Desea realizar una copia de seguridad diaria completa de su equipo.
- Desea almacenar la copia de seguridad de forma local en el archivo **MyMachine.tib**.
- Desea que cada copia de seguridad nueva reemplace a la antigua.

En este escenario, cree un plan de copia de seguridad con una programación diaria. Al crear el plan de copias de seguridad, especifique **MiEquipo** como el nombre del archivo comprimido, seleccione la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...** y seleccione **Completa** como el tipo de copia de seguridad.

**Resultado.** El archivo comprimido consiste en un único archivo: MyMachine.tib. Este archivo se eliminará antes de crear una nueva copia de seguridad.

### Ejemplo 2. Copias de seguridad completas diarias con sello de fecha.

Considere el siguiente escenario:

- Desea realizar una copia de seguridad diaria completa de su equipo.
- Desea mover las copias de seguridad más antiguas a una ubicación remota utilizando un comando.

En este escenario, cree un plan de copia de seguridad con una programación diaria. Al crear el plan de copias de seguridad, especifique **MiEquipo-[DATE]** como el nombre del archivo comprimido, seleccione la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...** y seleccione **Completa** como el tipo de copia de seguridad.

**Resultado:**

- Las copias de seguridad de el 1 de enero de 2011, 2 de enero de 2011 y así sucesivamente, son almacenadas respectivamente en MyMachine-1.1.2011.tib, MyMachine-1.2.2011.tib y así sucesivamente.

- Su comando puede mover las copias de seguridad más antiguas basadas en el sello de la fecha.

Vea también “La variable [Date]” (pág. 220).

## Ejemplo 3. Copias de seguridad a la hora en un día.

Considere el siguiente escenario:

- Desea realizar copias de seguridad cada hora de sus archivos críticos todos los días.
- Desea que la primera copia de seguridad de cada día sea completa y se ejecute a medianoche; y que las posteriores copias de seguridad del día sean diferenciales y se ejecuten a la 01.00, a las 02.00 y así sucesivamente.
- Desea mantener las copias de seguridad más antiguas en el archivo comprimido.

En este escenario, cree un plan de copia de seguridad con una programación diaria. Al crear el plan de copia de seguridad, especifique **ServerFiles([Date])** como nombre del archivo comprimido; seleccione la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido**..., especifique **Diferencial** como el tipo de copia de seguridad y programe las copias de seguridad para que se ejecuten cada hora desde la medianoche.

**Resultado:**

- Las 24 copias de seguridad de el 1 de enero de 2011, se almacenarán como ServerFiles(1.1.2011).tib, ServerFiles(1.1.2011)2.tib y así sucesivamente hasta ServerFiles(1.1.2011)24.tib.
- Al día siguiente, las copias de seguridad comenzarán con la copia de seguridad completa de ServerFiles(1.2.2011).tib.

Vea también “La variable [Date]” (pág. 220).

## Ejemplo 4. Copias de seguridad completas diarias con intercambios de unidad

Considere el siguiente escenario:

- Desea realizar copias de seguridad completas diarias de su equipo al archivo **MyMachine.tib** en una unidad de disco duro externa.
- Tiene las dos unidades. Cualquiera de ellas tiene la letra de unidad **D** cuando está adjuntada al equipo.
- Desea intercambiar las unidades antes de cada copia de seguridad, de forma que una unidad contenga la copia de seguridad de hoy y la otra unidad la copia de seguridad de ayer.
- Desea que cada nueva copia de seguridad reemplace a la copia de seguridad de la unidad adjuntada actualmente.

En este escenario, cree un plan de copia de seguridad con una programación diaria. Al crear el plan de copias de seguridad, especifique **MiEquipo** como el nombre del archivo comprimido y **D:** como la ubicación del archivo comprimido, seleccione la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...** y seleccione **Completa** como el tipo de copia de seguridad.

**Resultado.** Cada unidad de disco duro contendrá una copia de seguridad completa. Mientras una de las unidades está adjuntada al equipo, puede mantener la otra unidad de forma externa para obtener una mayor protección de datos.

## Ejemplo 5. Copias de seguridad diarias con intercambios de unidad semanales

Considere el siguiente escenario:

- Desea realizar copias de seguridad diarias de su equipo: una copia de seguridad completa cada lunes y copias de seguridad incrementales del martes al domingo.
- Desea hacer una copia de seguridad del archivo comprimido **MyMachine** en la unidad de disco duro externa.
- Tiene las dos unidades. Cualquiera de ellas tiene la letra de unidad **D** en el sistema operativo cuando está adjuntada al equipo.
- Desea intercambiar las unidades cada lunes, de forma que una unidad contenga copias de seguridad de la actual semana (de lunes a domingo) y que la otra unidad contenga las de la semana anterior.

En este escenario, necesita crear dos planes de copia de seguridad de la siguiente manera:

a) Al crear el primer plan de copia de seguridad especifique **MiEquipo** como el nombre de archivo comprimido y **D:** como la ubicación del archivo comprimido; seleccione la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...**, seleccione **Completa** como el tipo de copia de seguridad y programa las copias de seguridad para que se ejecuten el lunes de cada semana.

b) Al crear el segundo plan de copia de seguridad, especifique las mismas configuraciones que en el primer plan de copia de seguridad, pero seleccione **Incremental** como el tipo de copia de seguridad y programe las copias de seguridad para que se ejecuten cada semana de martes a domingo.

**Resultado:**

- Antes de crear una copia de seguridad de lunes, con el primer plan de copia de seguridad, todas las copias de seguridad quedarán eliminadas de la unidad adjuntada actualmente.
- Mientras una de las unidades está adjuntada al equipo, puede mantener la otra unidad de forma externa para obtener una mayor protección de datos.

## Ejemplo 6. Copias de seguridad en horas de trabajo.

Considere el siguiente escenario:

- Desea realizar copias de seguridad de los archivos críticos de su servidor todos los días.
- Desea que la primera copia de seguridad de cada día sea completa y se ejecute a la 01:00.
- Desea que las copias de seguridad durante las horas de trabajo sean diferenciales y se ejecuten cada hora desde las 08:00 hasta las 17:00.
- Desea incluir una fecha de creación en el nombre de cada archivo de copia de seguridad.

En este escenario, necesita crear dos planes de copia de seguridad de la siguiente manera:

a) Al crear la primera copia de seguridad especifique **ServerFiles([DATE])** como el nombre del archivo comprimido; seleccione la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...**; seleccione **Completa** como el tipo de copia de seguridad y programa las copias de seguridad para que se ejecuten cada día a la 01:00.

b) Al crear el segundo plan de copia de seguridad, especifique las mismas configuraciones que en el primer plan de copia de seguridad, pero seleccione **Diferencial** como el tipo de copia de seguridad y programe las copias de seguridad como se explica a continuación:

   - **Ejecute la tarea**: **Diariamente**

- **Cada**: **1 Hora(s)**
- **Desde las**: **08:00:00**
- **Hasta las**: **17:01:00**

**Resultado:**

- La copia de seguridad completa del 31 de enero de 2011, se almacenará como ServerFiles(1.31.2011).tib.
- Las 10 copias de seguridad diferenciales del 31 de enero de 2011, se almacenarán como ServerFiles(1.31.2011)2.tib, ServerFiles(1.31.2011)3.tib y así sucesivamente hasta ServerFiles(1.31.2011)11.tib.
- Al día siguiente, el 1 de febrero, las copias de seguridad comenzarán con la copia de seguridad completa de ServerFiles(2.1.2011).tib. Las copias de seguridad diferenciales comenzarán con ServerFiles(2.1.2011)2.tib.

Vea también “La variable [Date]” (pág. 220).

## La variable [DATE]

Si especifica la variable **[DATE]** en el nombre del archivo comprimido, el nombre del archivo de cada copia de seguridad incluirá la fecha de creación de esa copia de seguridad.

Al utilizar esta variable, la primera copia de seguridad de cada día será una copia de seguridad completa. Antes de crear la siguiente copia de seguridad completa, el software elimina todas las copias de seguridad realizadas más pronto ese día. Se mantienen las copias de seguridad realizadas antes de ese día. Esto significa que puede almacenar múltiples copias de seguridad completas con o sin las incrementales, pero no más de una copia de seguridad completa por día. Puede clasificar las copias de seguridad por día; copiar, mover y/o eliminar copias de seguridad de forma manual o bien utilizando un comando.

El formato de fecha es *mes**.**día**.**año*. Por ejemplo, para enero es el 1.31.2011 31, 2011. (Nota: ausencia de ceros).

Puede colocar esta variable en cualquier lugar del nombre del archivo comprimido. Puede usar letras tanto minúsculas como mayúsculas en esta variable.

### Ejemplos

**Ejemplo 1.** Suponga que realiza copias de seguridad incrementales dos veces al día (a medianoche y al mediodía) durante dos días empezando el 31 de enero de 2011. Si el nombre del archivo comprimido es **MyArchive-[DATE]-**, a continuación la lista de archivos de copias de seguridad después del día dos:

**MyArchive-1.31.2011-.tib** (full, created on January 31 at midnight)
**MyArchive-1.31.2011-2.tib** (incremental, created on January 31 at noon)
**MyArchive-2.1.2011-.tib** (full, created on February 1 at midnight)
**MyArchive-2.1.2011-2.tib** (incremental, created on February 1 at noon)

**Ejemplo 2.** Suponga que realiza copias de seguridad completas, con la misma programación y nombre de archivo comprimido, siguiendo el ejemplo anterior. Así, la lista de archivos de copias de seguridad después del día dos es la que viene a continuación:

**MyArchive-1.31.2011-.tib** (completa, creada el 31 de enero a medianoche)
**MyArchive-2.1.2011-.tib** (completa, creada el 1 de febrero a medianoche)

Esto es porque las copias de seguridad completas creadas a medianoche fueron reemplazadas por copias de seguridad completas del mismo día.

### Simplificación de nombre de archivos y división de copias de seguridad

Cuando se divide una copia de seguridad de acuerdo con las configuraciones de División de copias de seguridad (pág. 112), se utiliza la misma indexación para nombrar también las partes de la copia de seguridad. El nombre de archivo de la siguiente copia de seguridad tendrá el siguiente índice disponible.

Por ejemplo, suponga que la primera copia de seguridad del archivo comprimido **MyData** ha sido dividido en dos partes. Entonces los nombres de los archivos para esta copia de seguridad serán **MyData1.tib** y **MyData2.tib**. El nombre de la segunda copia de seguridad, suponiendo que no está dividida, será **MyData3.tib**.

## 6.2.9 Credenciales de acceso para la ubicación del archivo comprimido

Especifique las credenciales que se necesitarán para el acceso a la ubicación donde se almacenará el archivo comprimido de la copia de seguridad. El usuario cuyo nombre se especifique se considerará el propietario del archivo comprimido.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Usar las credenciales del plan**

     El programa accederá a los datos de origen mediante las credenciales del plan de copias de seguridad especificado en la sección General.
   - **Utilice las siguientes credenciales.**

     El programa accederá a los datos de origen mediante las credenciales que especifique.Utilice esta opción si la cuenta del plan no dispone de permisos de acceso a la ubicación. Quizás necesite atribuir credenciales especiales para una red compartida o para una bóveda de nodo de almacenamiento.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

***Advertencia:*** *Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

## 6.2.10 Esquemas de copia de seguridad

Elija uno de los esquemas de copia de seguridad disponibles:

- **Copia de seguridad ahora** – para crear una tarea de copia de seguridad para un inicio manual y ejecutar la tarea inmediatamente después de crearla.
- **Copia de seguridad más tarde** – para crear una tarea de copia de seguridad para un inicio manual O programar que la tarea se ejecute más tarde una vez.
- **Simple** – para programar cuándo y con qué frecuencia realizar copias de seguridad de los datos y especificar reglas de retención.

- **Abuelo-Padre-Hijo** – para utilizar el esquema de copia de seguridad Abuelo-Padre-Hijo. Este esquema sólo permite realizar copias de seguridad de los datos una vez al día.. Puede configurar los días de la semana en los que se llevará a cabo la copia de seguridad y seleccionar de entre esos días, la fecha para la copia de seguridad semanal o mensual. Después, debe ajustar los periodos de retención para las copias de seguridad diarias (llamadas "hijos"), semanales (llamadas "padres") y mensuales (llamadas "abuelos"). Las copias de seguridad caducadas se borrarán automáticamente.
- **Torre de Hanoi** – para utilizar el esquema de copia de seguridad Torre de Hanoi, en el que se programa cuándo y con qué frecuencia realizar copias de seguridad (sesiones) y se selecciona el número de niveles de copia de seguridad (hasta 16). Con este esquema, se puede realizar más de una copia de seguridad de los datos al día. Al configurar el calendario de copia de seguridad y seleccionar los niveles de copia de seguridad, se obtiene automáticamente el periodo de recuperación, es decir, el número garantizado de sesiones que se pueden a las que se puede volver en cualquier momento. El mecanismo de limpieza automático mantiene el periodo de recuperación necesario, borrando las copias de seguridad caducadas y conservando las copias de seguridad más recientes de cada nivel.
- **Personalizada** – para crear una copia de seguridad personalizada, en la que se puede configurar libremente la estrategia que mejor convenga a las necesidades de su empresa: especificar diferentes programaciones para diferentes tipos de copias de seguridad, añadir condiciones y especificar las reglas de retención.
- **Inserción inicial** - para guardar localmente una copia de seguridad completa cuyo destino final es Acronis Online Backup Storage.

## Esquema Copia de seguridad ahora

Con el esquema **Copia de seguridad ahora**, la copia de seguridad se llevará a cabo inmediatamente después de que haga clic en el botón **Aceptar** en la parte inferior de la página.

En el campo **Tipo de copia de seguridad**, seleccione si desea crear una copia de seguridad completa, incremental o diferencial (pág. 31).

## Esquema Copia de seguridad más tarde

Con el esquema Copia de seguridad más tarde, la copia de seguridad se llevará a cabo una sola vez, en la fecha y hora que especifique.

Especifique los ajustes adecuados de la siguiente manera

| | |
|---|---|
| **Tipo de copia de seguridad** | Seleccione el tipo de copia de seguridad: completo, incremental o diferencial. Si no existe una copia de seguridad completa en el archivo comprimido, se creará una independientemente de su elección. |
| **Fecha y hora** | Especifique cuándo desea iniciar la copia de seguridad. |
| **La tarea se iniciará manualmente** | Seleccione esta casilla de verificación si no necesita colocar la tarea de copia de seguridad en una programación y desea iniciarla manualmente más tarde. |

## Esquema simple

Con el esquema simple de copia de seguridad, simplemente debe programar cuándo y con qué frecuencia realizar copias de seguridad de los datos y configurar la regla de retención. La primera vez se creará una copia de seguridad completa. Las siguientes copias de seguridad serán incrementales.

Para configurar el esquema simple de copia de seguridad, especifique los ajustes apropiados de la siguiente manera.

| | |
|---|---|
| **Crear copia de seguridad** | Configure la programación de la copia de seguridad: cuándo y con qué frecuencia realizar copias de seguridad de los datos.<br>Para obtener más información sobre cómo configurar el calendario, consulte la sección Programación (pág. 173). |
| **Regla de retención** | Con el esquema simple, solo se dispone de una regla de retención (pág. 42). Configure el periodo de retención para las copias de seguridad. |

## Esquema Abuelo-padre-hijo

### De un vistazo

- Copias de seguridad incrementales diarias, diferenciales semanales y completas mensuales
- Día personalizado para las copias de seguridad semanales y mensuales
- Periodos de retención personalizados para las copias de seguridad de cada tipo

### Descripción

Supongamos que queremos configurar un plan de copias de seguridad que produzca una serie de copias de seguridad regulares diarias (D), semanales (S) y mensuales (M). Este es el modo más normal para hacerlo: la siguiente tabla muestra un ejemplo de un periodo de dos meses para dicho plan.

| | Lu | Ma | Mi | Ju | Vi | Sa | Do |
|---|---|---|---|---|---|---|---|
| 1 Ene—7 Ene | D | D | D | D | S | - | - |
| 8 Ene—14 Ene | D | D | D | D | S | - | - |
| 15 Ene—21 Ene | D | D | D | D | S | - | - |
| 22 Ene—28 Ene | D | D | D | D | M | - | - |
| 29 Ene—4 Feb | D | D | D | D | S | - | - |
| 5 Feb—11 Feb | D | D | D | D | S | - | - |
| 12 Feb—18 Feb | D | D | D | D | S | - | - |
| 19 Feb—25 Feb | D | D | D | D | M | - | - |
| 26 Feb—4 Mar | D | D | D | D | S | - | - |

Las copias de seguridad diarias se ejecutan todos los días laborables excepto los viernes, que se reservan para las copias de seguridad semanales y mensuales. Las copias de seguridad mensuales se llevan a cabo el cuarto viernes de cada mes y las semanales, los demás viernes del mes.

- Las copias de seguridad mensuales ("Abuelo") son completas;
- Las copias de seguridad semanales ("Padre") son diferenciales;
- Las copias de seguridad diarias ("Hijo") son incrementales.

### Parámetros

Puede configurar los siguientes parámetros de un esquema Abuelo-Padre-Hijo (GFS).

| | |
|---|---|
| **Comienzo de la copia de seguridad en:** | Especifica cuándo se inicia una copia de seguridad. El valor predeterminado son las 12:00. |
| **Copia de seguridad en:** | Especifica los días en los que se lleva a cabo la copia de seguridad. El valor predeterminado es el viernes. |
| **Semanalmente/mensualmente:** | Especifica cuál de los días elegidos en el campo **Realizar copias de seguridad el** desea reservar para las copias de seguridad semanales y mensuales. El cuarto día especificado del mes se llevará a cabo una copia de seguridad mensual. El valor predeterminado es el viernes. |
| **Mantener copias de seguridad:** | Especifica durante cuánto tiempo desea que se almacenen las copias de seguridad en el archivo comprimido. Se puede configurar en horas, días, semanas, meses o años. Para copias de seguridad mensuales, puede seleccionar también **Mantener indefinidamente** si desea que se almacenen para siempre.<br><br>Los valores predeterminados para cada tipo de copia de seguridad son los siguientes.<br><br>Diariamente: 7 días (mínimo recomendado)<br><br>Semanalmente: 4 semanas<br><br>Mensualmente: indefinidamente<br><br>El periodo de retención para las copias de seguridad semanales debe ser mayor al establecido para las diarias. Del mismo modo, el periodo de retención para las copias de seguridad mensuales debe ser mayor al de las copias semanales.<br><br>Le recomendamos configurar un periodo de retención de al menos una semana para las copias de seguridad diarias. |

*Nunca se elimina una copia de seguridad hasta que todas las copias de seguridad que dependen directamente de ella se puedan eliminar. Por esta razón, puede que observe que una copia de seguridad semanal o mensual permanece en el archivo comprimido incluso unos días después de la fecha de caducidad esperada.*

*Si la programación comienza con una copia de seguridad diaria o semanal, en su lugar se crea una copia de seguridad completa.*

### Ejemplos

#### Cada día de la semana pasada, cada semana del mes pasado

Permítanos sugerir un esquema de copia de seguridad GFS que podría encontrar útil.

- Realizar copias de seguridad cada día, fines de semana incluidos
- Tener la posibilidad de recuperar los archivos de cualquier fecha dentro de los últimos siete días
- Tener acceso a las copias de seguridad semanales del mes anterior.
- Mantener copias de seguridad mensuales indefinidamente.

Los parámetros del esquema de copia de seguridad se pueden configurar de la siguiente manera.

- Comienzo de la copia de seguridad en: **23:00**
- Copia de seguridad en: **Todos los días**
- Semanalmente/mensualmente: **Sábado** (por ejemplo)
- Mantener copias de seguridad:
  - Diariamente: **1 semana**
  - Semanalmente: **1 mes**
  - Mensualmente: **indefinidamente**

Por lo tanto, se creará un archivo comprimido de copias de seguridad diarias, semanales y mensuales. Las copias de seguridad diarias estarán disponibles durante siete días a partir de la fecha de creación. Por ejemplo, una copia de seguridad diaria con fecha de domingo, 1 de enero, permanecerá disponible hasta el próximo domingo, 8 de enero; la primera copia de seguridad semanal, con fecha de sábado, 7 de enero, se almacenará en el sistema hasta el 7 de febrero. Las copias de seguridad mensuales no se eliminarán nunca.

### Almacenamiento limitado

Si no desea fijar una gran cantidad de espacio para almacenar un archivo comprimido muy grande, debería configurar un esquema GFS para limitar la vida media de sus copias de seguridad, a la vez que garantiza que su información pueda recuperarse en caso de una pérdida de datos accidental.

Suponga que necesita:

- Realizar copias de seguridad al final de cada día laborable
- Tener la posibilidad de recuperar un archivo modificado o eliminado de manera accidental si se ha detectado relativamente pronto
- Tener acceso a una copia de seguridad semanal durante 10 días después de su creación.
- Conservar copias de seguridad mensuales durante 6 meses.

Los parámetros del esquema de copia de seguridad se pueden configurar de la siguiente manera.

- Comienzo de la copia de seguridad a las: **18:00**
- Copia de seguridad el: **Días hábiles**
- Semanalmente/mensualmente: **Viernes**
- Mantener copias de seguridad:
  - Diaria: **1 semana**
  - Semanal: **10 días**
  - Mensual: **6 meses**

Con este esquema, dispondrá de una semana para recuperar una versión anterior de un archivo dañado a partir de una copia de seguridad diaria, así como de 10 días de acceso a las copias de seguridad semanales. Las copias de seguridad completas mensuales estarán disponible durante 6 meses a partir de la fecha de creación.

### Programación laboral

Supongamos que es consultor financiero y trabaja media jornada en una empresa los martes y jueves. Durante estos días, por lo general, realiza cambios en documentos financieros y declaraciones, y actualiza hojas de cálculo, etc. en su portátil. Para realizar copias de seguridad de estos datos, es conveniente que:

- Rastree los cambios en las declaraciones financieras, hojas de cálculo, etc. realizados los martes y jueves (copia de seguridad incremental diaria).
- Tenga un resumen semanal de los cambios en los archivos desde el mes pasado (copia de seguridad diferencial semanal).
- Tenga una copia de seguridad completa mensual de todos los archivos.

Además, supongamos que desea mantener el acceso a todas las copias de seguridad, incluidas las diarias, durante al menos seis meses.

El siguiente esquema GFS cumple estos fines:

- Iniciar copia de seguridad a las: **23:30.**
- Realizar copias de seguridad el: **Martes, Jueves, Viernes**
- Semanalmente/mensualmente: **Viernes**
- Mantener copias de seguridad:
  - Diariamente: **6 meses**
  - Semanalmente: **6 meses**
  - Mensualmente: **5 años**

Aquí, las copias de seguridad incrementales diarias se crearán los martes y jueves, con copias de seguridad semanales y mensuales que se realizarán los viernes. Tenga en cuenta que, para elegir **Viernes** en el campo **Semanalmente/mensualmente**, deberá seleccionarlo primero en el campo **Realizar copias de seguridad el**.

Ese archivo comprimido le permitirá comparar los documentos financieros a partir del primer y último día hábil, y tener un historial de cinco años de todos los documentos, etc.

### Sin copias de seguridad diarias

Considere un esquema GFS diferente:

- Iniciar copia de seguridad a las: **12:00.**
- Realizar copias de seguridad el: **Viernes**
- Semanalmente/mensualmente: **Viernes**
- Mantener copias de seguridad:
  - Diariamente: **1 semana**
  - Semanalmente: **1 mes**
  - Mensualmente: **indefinidamente**

La copia de seguridad, por lo tanto, se realiza solo los viernes. Esto hace que el viernes sea la única opción para realizar copias de seguridad semanales y mensuales, sin que haya otra fecha para las copias de seguridad diarias. El archivo comprimido “Abuelo-padre” resultante, por lo tanto, consistirá solo de copias de seguridad diferenciales semanales y completas mensuales.

Si bien se puede utilizar el esquema GFS para crear dicho archivo comprimido, el esquema personalizado es más flexible para esta situación.

## Esquema Torres de Hanói

### De un vistazo

- Hasta 16 niveles de copias de seguridad completas, diferenciales e incrementales
- La frecuencia de las copias de seguridad del nivel siguiente es exactamente la mitad de la de las copias de seguridad de los niveles anteriores.
- Solo se almacena una copia de seguridad de cada nivel al mismo tiempo
- La cantidad de copias de seguridad recientes es mayor que la de las antiguas.

### Parámetros

Puede configurar los siguientes parámetros de un esquema Torres de Hanói.

| | |
|---|---|
| **Programación** | Configurar una programación diaria (pág. 174), semanal (pág. 176) o mensual (pág. 178). Se pueden crear programaciones simples al configurar los parámetros de la programación (ejemplo de una programación simple diaria: se realizará una tarea de copia de seguridad cada día 1 a las 10:00), así como programaciones más complejas (ejemplo de una programación compleja diaria: se realizará una tarea cada 3 días, comenzando a partir del 15 de enero. En los días especificados, la tarea se repetirá cada 2 horas desde las 10 hasta las 22 horas). De este modo, las programaciones complejas especifican las sesiones en las que el esquema debería ejecutarse. En los comentarios siguientes, se puede reemplazar por "sesiones programadas". |
| **Número de niveles** | Seleccione los niveles de copia de seguridad entre 2 a 16. Para obtener más información, consulte el siguiente ejemplo. |
| **Periodo de recuperación** | El número garantizado de sesiones a las que se puede volver en el archivo comprimido en cualquier momento. Se calcula automáticamente, dependiendo de los parámetros de programación y de los niveles que seleccione. Para obtener más información, consulte el siguiente ejemplo. |

### Ejemplo

Los parámetros de **Programación** se configuran de la siguiente manera

- Repetir: Cada día
- Frecuencia: Por primera vez a las 18:00

**Número de niveles**: 4

Para los 14 días siguientes (o 14 sesiones), este esquema de programación se verá de la siguiente manera: Los números sombreados indican los niveles de copia de seguridad.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 1 | 3 | 1 | 2 | 1 | 4 | 1 | 2 | 1 | 3 | 1 |

Las copias de seguridad de niveles diferentes son de diferentes tipos:

- Las copias de seguridad de *último nivel* (en este caso, nivel 4) son completas;
- Las copias de seguridad de *niveles intermedios* (2, 3) son diferenciales;
- Las copias de seguridad de *primer nivel* (1) son incrementales.

Un mecanismo de limpieza garantiza que solo se mantienen las copias de seguridad más recientes de cada nivel. Este es el aspecto del archivo comprimido en el día 8, un día antes de crear una nueva copia de seguridad completa.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|

| 4 | 1 | 2 | 1 | 3 | 1 | 2 | 1 |
|---|---|---|---|---|---|---|---|

El esquema permite un almacenamiento eficiente de los datos: Se acumulan más copias de seguridad cuanto más cerca nos encontramos de la fecha actual. Con 4 copias de seguridad, se pueden recuperar datos de hoy, de ayer, de media semana o de una semana atrás.

### Periodo de recuperación

El número de días a los que se puede volver en el archivo comprimido es diferente en función del día. El número mínimo de días garantizados se llama periodo de recuperación.

La siguiente tabla muestra los periodos de copia de seguridad completos y los periodos de recuperación para esquemas de diferentes niveles.

| **Número de niveles** | **Copia de seguridad completa cada** | **En días diferentes, puede volver atrás** | **Periodo de recuperación** |
|---|---|---|---|
| 2 | 2 días | De 1 a 2 días | 1 día |
| 3 | 4 días | De 2 a 5 días | 2 días |
| 4 | 8 días | De 4 a 11 días | 4 días |
| 5 | 16 días | De 8 a 23 días | 8 días |
| 6 | 32 días | De 16 a 47 días | 16 días |

Al aumentar un nivel, la duración de los periodos de copia de seguridad completa y de recuperación se multiplican por dos.

Para ver por qué varía el número de los días de recuperación, consulte el ejemplo siguiente.

A continuación se encuentran las copias de seguridad que tenemos en el día 12 (los números en gris indican las copias de seguridad eliminadas).

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 1 | 3 | 1 | 2 | 1 | 4 | 1 | 2 | 1 |

Todavía no se ha creado una copia de seguridad diferencial de nivel 3, por lo que la copia de seguridad del día 5 aún se encuentra almacenada. Esta copia de seguridad sigue estando disponible ya que depende de la copia de seguridad completa del día 1. Esto nos permite retroceder hasta 11 días, lo cual constituye el mejor de los casos posibles.

El día siguiente, sin embargo, se crea una nueva copia de seguridad diferencial de nivel 3 y se elimina la copia de seguridad completa antigua.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 1 | 3 | 1 | 2 | 1 | 4 | 1 | 2 | 1 | 3 |

Esto nos proporciona solo un intervalo de recuperación de 4 días, lo que representa la peor situación posible.

En el día 14, el intervalo es de 5 días. En los días siguientes, este intervalo va aumentando hasta volver a reducirse, sucesivamente.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 1 | 3 | 1 | 2 | 1 | 4 | 1 | 2 | 1 | 3 | 1 |

El periodo de recuperación muestra el número de días que están garantizados incluso en el peor de los casos. Para un esquema de cuatro niveles, es de 4 días.

## Esquema personalizado de copia de seguridad

### De un vistazo

- Programación personalizada y condiciones de copia de seguridad de cada tipo
- Programación personalizada y reglas de retención

### Parámetros

| Parámetro | Significado |
|---|---|
| **Copia de seguridad completa** | Especifica con qué programación y bajo qué condiciones realizar una copia de seguridad completa.<br>Por ejemplo, la copia de seguridad completa puede configurarse para que se ejecute cada domingo a la 01:00, tan pronto como todos los usuarios hayan cerrado sus sesiones. |
| **Incremental** | Especifica con qué programación y bajo qué condiciones realizar una copia de seguridad incremental.<br>Si el archivo comprimido no contiene copias de seguridad cuando se ejecute la tarea, se llevará a cabo una copia de seguridad completa en lugar de una incremental. |
| **Diferencial** | Especifica con qué programación y bajo qué condiciones realizar una copia de seguridad diferencial.<br>Si el archivo comprimido no contiene copias de seguridad cuando se ejecute la tarea, se llevará a cabo una copia de seguridad completa en lugar de una diferencial. |
| **Limpie el archivo comprimido** | Especifica cómo eliminar copias de seguridad antiguas: ya sea aplicando reglas de retención (pág. 42) regularmente o limpiando el archivo durante la realización de una copia de seguridad cuando la ubicación de destino se queda sin espacio.<br>De manera predeterminada, las reglas de retención no se especifican, lo cual significa que las copias de seguridad más antiguas no se eliminarán de forma automática.<br>**Utilización de reglas de retención**<br>Especifique las reglas de retención y cuándo aplicarlas.<br>Se recomienda esta configuración para destinos de copias de seguridad como carpetas compartidas o bóvedas centralizadas.<br>**Cuando no hay espacio suficiente mientras se realiza la copia de seguridad**<br>El archivo comprimido se limpiará únicamente durante la realización de la copia de seguridad y sólo si no hay espacio suficiente para crear una copia de seguridad nueva. En este caso, el programa actuará de la siguiente manera:<br>▪ Eliminará la copia de seguridad más antigua y todas las copias de seguridad incrementales/diferenciales dependientes.<br>▪ Si queda sólo una copia de seguridad completa y otra está en progreso, eliminará la última copia de seguridad completa y todas las copias de seguridad incrementales/diferenciales dependientes<br>▪ Si queda sólo una copia de seguridad completa y hay una copia de seguridad incremental o diferencial en progreso, se producirá un error que le indicará que no hay espacio disponible<br>Se recomienda esta configuración para realizar copias de seguridad en una unidad USB o Acronis Secure Zone. Esta configuración no se aplica a bóvedas gestionadas. |

| | |
|---|---|
| | Esta configuración permite la eliminación de la última copia de seguridad en el archivo comprimido, en caso de que su dispositivo de almacenamiento no pueda incluir más de una copia de seguridad. Sin embargo, si por alguna razón el programa no puede crear la copia de seguridad nueva, podría quedarse sin copias de seguridad. |
| **Aplicar las reglas**<br>(solo si las reglas de retención están configuradas) | Especifica cuándo aplicar las reglas de retención (pág. 42).<br>Por ejemplo, el procedimiento de limpieza puede configurarse para que se ejecute después de cada copia de seguridad y según la programación.<br>Esta opción estará disponible únicamente si ha configurado al menos una regla de retención en **Reglas de retención**. |
| **Programación de limpieza**<br>(solo si la opción **Según programación** está seleccionada) | Especifica una programación para la limpieza del archivo comprimido.<br>Por ejemplo, la limpieza puede programarse para que comience el último día de cada mes.<br>Esta opción estará disponible únicamente si ha seleccionado **Según programación** en **Aplicar las reglas**. |

## Ejemplos

### Copia de seguridad completa semanal

El siguiente esquema genera una copia de seguridad completa que se realiza todos los viernes por la noche.

**Copia de seguridad completa**: **Programación: Semanalmente**, todos los **viernes**, a las **22:00.**

Aquí, todos los parámetros de **Copia de seguridad completa** quedan vacíos, excepto **Programar**. Todas las copias de seguridad se conservan indefinidamente en el archivo comprimido (no se realizan limpiezas del archivo).

### Copia de seguridad incremental y completa más limpieza

Con el siguiente esquema, el archivo comprimido constará de copias de seguridad completas semanales e incrementales diarias. Más allá de eso, necesitamos que una copia de seguridad completa tenga lugar únicamente una vez que todos los usuarios hayan cerrado sesión.

**Copia de seguridad completa: Programación: Semanal**, cada **viernes** a las **22:00**

**Copia de seguridad completa: Condiciones: El usuario ha cerrado sesión**

**Incremental: Programación: Semanal, cada día laborable** a las **21:00**

Permita también que todas las copias de seguridad que tengan más de un año se eliminen del archivo comprimido, así como la realización de una limpieza que finalice con la creación de una nueva copia de seguridad.

**Reglas de retención:** Eliminar las copias de seguridad que tengas más de **12 meses**

**Aplicar las reglas: Después de realizar la copia de seguridad**

De manera predeterminada, no se eliminará una copia de seguridad completa a menos que se eliminen todas las copias de seguridad incrementales que dependen de ella. Para obtener más información, consulte Reglas de retención (pág. 42).

### Copias de seguridad mensuales completas, semanales diferenciales y diarias incrementales más limpieza

Este ejemplo demuestra el uso de todas las opciones disponibles en el esquema personalizado.

Supongamos que necesitamos un esquema para generar copias de seguridad completas mensuales, diferenciales semanales e incrementales diarias. La programación de copia de seguridad podría ser la siguiente:

Copia de seguridad completa: **Programación: Mensualmente**, todos los **últimos domingos** del mes, a las **21:00.**

**Incremental: Programación: Diariamente**, todos los **días hábiles**, a las **19:00.**

**Diferencial: Programación: Semanalmente**, todos los **sábados**, a las **20:00.**

Además, queremos añadir condiciones que deben cumplirse para que se inicie una tarea de copia de seguridad. Estas opciones se establecen en los campos **Condiciones** de cada tipo de copia de seguridad.

**Copia de seguridad completa**: **Condiciones**: **Ubicación disponible**

**Incremental**: **Condiciones**: **El usuario cerró la sesión**

**Diferencial**: **Condiciones**: **El usuario está inactivo**

Por ese motivo, la copia de seguridad completa. originalmente programada para las 21:00, podría comenzar más tarde: en cuanto la ubicación de la copia de seguridad esté disponible. Del mismo modo, las tareas de copia de seguridad para copias incrementales y diferenciales no se iniciarán hasta que todos los usuarios hayan cerrado sesión y estén inactivos, respectivamente.

Por último, creamos reglas de retención para el archivo comprimido: que se conserven solo las copias de seguridad que tengan menos de seis meses y que se realice una limpieza después de cada tarea de copia de seguridad y también el último día de cada mes.

**Reglas de retención**: Eliminar las copias de seguridad con más de **6 meses**

**Aplicar las reglas**: **Después de realizar la copia de seguridad**, **Según la programación**

**Programación de limpieza**: **Mensualmente**, el **Último día** de **Todos los meses**, a las **22:00.**

De manera predeterminada, una copia de seguridad no se eliminará siempre que tenga otras copias dependientes que deban conservarse. Por ejemplo: si una copia de seguridad completa puede eliminarse, pero hay otras copias incrementales o diferenciales que dependen de ella, la eliminación se pospone hasta que también se puedan eliminar todas las copias de seguridad dependientes.

Para obtener más información, consulte Reglas de retención (pág. 42).

### Tareas resultantes

Todos los esquemas personalizados originan siempre tres tareas de la copia de seguridad y, en caso de que se especifiquen las reglas de retención, una tarea de limpieza. Cada tarea se detalla en la lista de tareas como **Programada** (si se ha configurado la programación) o como **Manual** (si no se ha configurado la programación).

Puede ejecutar cualquier tarea de copia de seguridad o limpieza en cualquier momento, sin importar si se encuentra programada.

En el primero de los ejemplos anteriores, configuramos una programación únicamente para copias de seguridad completas. Sin embargo, el esquema seguirá originando tres tareas de copia de seguridad, permitiéndole así realizar manualmente una copia de seguridad de cualquier tipo:

- Copia de seguridad completa, se ejecuta cada viernes a las 22:00
- Copia de seguridad incremental, se ejecuta manualmente
- Copia de seguridad diferencial, se ejecuta manualmente

Puede ejecutar cualquiera de estas tareas de copia de seguridad al seleccionarlas en la lista de tareas en la sección **Planes y tareas de la copia de seguridad** situada en el panel izquierdo.

Si también ha especificado las reglas de retención en su esquema de copia de seguridad, el esquema originará cuatro tareas: tres tareas de copia de seguridad y una tarea de limpieza.

## 6.2.11 Validación de archivos comprimidos

Configure la validación de la tarea para comprobar si los datos de la copia de seguridad pueden recuperarse. Si la copia de seguridad no finaliza la validación correctamente, la tarea de validación falla y el plan de copias de seguridad establecerá su estado en Error.

Para configurar la validación, especifique los siguientes parámetros

1. **Cuándo validar**: seleccione cuándo realizar la validación. Ya que la validación es una operación que utiliza muchos recursos, puede ser conveniente **programar** la validación en el periodo de menor actividad del equipo gestionado. Por otro lado, si la validación es uno de los elementos clave de su estrategia de protección de datos y prefiere que se le notifique inmediatamente en el caso de que los datos de la copia de seguridad no estén dañado y puedan recuperarse correctamente, considere la posibilidad de comenzar la validación inmediatamente después de la creación de la copia de seguridad.
2. **Qué validar**: seleccione validar el archivo comprimido al completo o su última copia de seguridad en el archivo comprimido. La validación de la copia de seguridad de un archivo simula la recuperación de todos los archivos de la copia de seguridad a un destino ficticio La validación de la copia de seguridad del volumen calcula la suma de comprobación para cada bloque de datos guardados en la copia de seguridad. La validación del archivo comprimido validará todas las copias de seguridad de los archivos comprimidos y podría llevar un tiempo considerable y agotar muchos recursos.
3. **Programación de la validación** (aparece únicamente si ha seleccionado según programación en el paso 1): configure la programación de la validación. Para obtener más información, consulte la sección Programación (pág. 173).

## 6.2.12 Configuración de una conversión normal a una máquina virtual

Cuando se crea un plan de copias de seguridad (pág. 207), puede configurar la conversión normal de la copia de seguridad de un disco o volumen a una máquina virtual. Esta sección proporciona información que le ayudará a realizar los ajustes adecuados.

### Configuración de una programación de conversión

Una copia de seguridad del disco (pág. 404) creada mientra se ejecuta un plan de copias de seguridad se puede convertir en una máquina virtual inmediatamente, con una programación o se pueden combinar ambos métodos.

La tarea de conversión se creará en el equipo del que se está realizando la copia de seguridad y se utilizará la fecha y la hora de ese equipo.

Como resultado de esta primera conversión, se creará una nueva máquina virtual. Todas las conversiones posteriores recrearán este equipo de cero. En primer lugar, se creará una nueva máquina virtual (temporal). Si esta operación se realiza correctamente, se sustituirá el equipo anterior. Si se produce un error durante la creación del equipo temporal, este se eliminará. De esta manera, la tarea siempre finaliza con un único equipo, pero durante la conversión se necesita espacio de almacenamiento extra para mantener el equipo temporal.

La máquina virtual anterior debe estar apagada durante la conversión, ya que de lo contrario no se podrá eliminar y la tarea de conversión fallará. Si ocurre esto, puede reiniciar la tarea de conversión manualmente tras haber apagado el equipo. Se sobrescribirán todos los cambios realizados cuando el equipo estaba encendido.

## Selección de un servidor que realizará la conversión

Especifique el equipo que realizará la conversión. El equipo debe tener instalado Acronis Backup & Recovery 10 Agent para Windows, Agent para ESX/ESXi o Agent para Hyper-V.

Tenga en cuenta las siguientes consideraciones.

### ¿Qué agente se instala en el servidor?

El tipo y la ubicación de la máquina virtual resultante dependen del agente que resida en el servidor seleccionado.

- El **agente para Windows** está instalado en el servidor

  Puede optar entre varios tipos de máquinas virtuales: VMware Workstation, Microsoft Virtual PC o Parallels Workstation. Los archivos de la nueva máquina virtual se colocarán en la carpeta que seleccione.
- El **agente para ESX/ESXi** está instalado en el servidor

  Se creará una máquina virtual VMware en el servidor ESX/ESXi.

  Se supone que a las máquinas virtuales generadas de la copia de seguridad no se les realiza una copia de seguridad y, por lo tanto, no aparecen en el servidor de gestión, a menos que se haya habilitado su integración con VMware vCenter Server. Si la integración se ha habilitado, esos equipos aparecen como no gestionables. No se les puede aplicar una política de copia de seguridad.
- El **agente para Hyper-V** está instalado en el servidor

  Puede escoger entre crear una máquina virtual en el servidor Hyper-V o crear un equipo VMware Workstation, Microsoft Virtual PC o Parallels Workstation en la carpeta que seleccione.

  Las máquinas virtuales creadas en el servidor Hyper-V como el resultado de una copia de seguridad no aparecerán en el servidor de gestión porque se supone que a esos equipos no se les realiza la copia de seguridad.

### ¿Qué es la potencia de procesamiento del servidor?

La tarea de conversión se creará en el equipo del que se está realizando la copia de seguridad y se utilizará la fecha y la hora de ese equipo. De hecho, el servidor ejecutará la tarea que usted seleccione y tomará los recursos de la CPU de ese servidor. Si varios planes de copia de seguridad utilizan el mismo servidor, habrá en cola de espera varias tareas de conversión en ese servidor y completarlas podrá llevarle un tiempo considerable.

### ¿Qué almacenamiento se utilizará en las máquinas virtuales?

#### Uso de la red

A diferencia de las copias de seguridad normales (archivos TIB), los archivos de las máquinas virtuales se transfieren sin comprimir a través de la red. Por tanto, utilizar un SAN o un almacenamiento local con respecto a un servidor que realiza las conversiones es la mejor elección desde el punto del vista de uso de la red. Un disco local no es un opción, aunque la conversión la realice el mismo equipo en el que se realiza la copia de seguridad. Utilizar un NAS también es una buena opción.

#### Espacio de disco

En VMware ESX/ESXi, los nuevos equipos se crean con discos previamente asignados. Esto significa que el tamaño del disco virtual siempre es igual a la capacidad original del disco. Si suponemos que el tamaño del disco original es de 100 GB, el disco virtual correspondiente ocupará 100 GB, incluso si el disco almacena 10 GB de datos.

Las máquinas virtuales creadas en un servidor Hyper-V o en equipos de tipo estación de trabajo (VMware Workstation, Microsoft Virtual PC o Parallels Workstation) utilizan tanto espacio del disco como los datos originales. Debido a que el espacio en el disco no se asigna previamente, el disco físico en el que se ejecutará el disco virtual se prevé que cuente con el espacio suficiente para que el disco virtual aumente de tamaño.

## 6.3 Recuperación de datos

En cuanto a la recuperación de datos, en primer lugar deberá considerar el método más funcional: conecte la consola al **equipo gestionado que ejecuta el sistema operativo** y cree la tarea de recuperación.

Si el **sistema operativo del equipo gestionado no se puede iniciar** o necesita **recuperar datos desde cero**, inicie el equipo desde el dispositivo de inicio (pág. 410)o utilizando Acronis Startup Recovery Manager (pág. 51). Después, cree una tarea de recuperación.

Acronis Universal Restore (pág. 52) le permite recuperar e iniciar **Windows en hardware diferentes** o en una máquina virtual.

**Un sistema Windows se puede poner en línea en segundos** mientras todavía se está recuperando. Mediante el uso de la tecnología propia de Acronis Active Restore (pág. 53), Acronis Backup & Recovery 10 iniciará el equipo en el sistema operativo encontrado en la copia de seguridad, como si el sistema estuviera presente en el disco físico. El sistema se vuelve funcional y listo para proporcionar los servicios necesarios. Por lo tanto, el tiempo de inactividad del sistema será mínimo.

Un **volumen dinámico** se puede recuperar sobre un volumen existente, en un espacio no asignado de un grupo de discos o en un espacio no asignado de un disco básico. Para obtener más información sobre la recuperación de volúmenes dinámicos, consulte la sección LDM de Microsoft (Volúmenes dinámicos) (pág. 44).

Acronis Backup & Recovery 10 Agent para Windows tiene la habilidad de recuperar una copia de seguridad de disco (volumen) a una máquina virtual nueva de uno de los siguientes tipos: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) o Red Hat KVM. El dispositivo virtual puede ser importado de XenServer. El equipo VMware Workstation puede convertirse al formato de virtualización abierta (OVF) con la herramienta VMware OVF. Con Acronis Backup & Recovery 10 Agent para Hyper-V o Agent para ESX/ESXi, puede crear una máquina virtual nueva en el respectivo servidor de virtualización.

Es posible que tenga que preparar discos de destino antes de la recuperación. Acronis Backup & Recovery 10 incluye una utilidad de gestión de disco muy útil que le permite crear o eliminar volúmenes, cambiar el estilo de partición de disco, crear un grupo de discos y realizar otras operaciones de gestión de disco en el hardware de destino, tanto en sistemas operativos como desde cero. Para obtener más información sobre Acronis Disk Director LV, consulte la sección Gestión de disco (pág. 294).

***Para crear una tarea de recuperación, realice los siguientes pasos***

## General

**Nombre de la tarea**

[Opcional] Introduzca un nombre único para la tarea de recuperación. Un nombre pensado deliberadamente le permite identificar de manera rápida una tarea entre las demás.

**Credenciales de la tarea** (pág. 237)

[Opcional] La tarea se ejecutará en nombre del usuario que cree la tarea. De ser necesario, podrá cambiar las credenciales de la cuenta de la tarea. Para acceder a esta opción, seleccione la casilla de verificación **Vista avanzada**.

## Qué recuperar

**Archivo comprimido** (pág. 237)

Seleccione el archivo comprimido del que desea recuperar datos.

**Tipo de datos** (pág. 238)

*Se aplica a: recuperación de discos*

Elija el tipo de datos que necesita recuperar de la copia de seguridad del disco seleccionada.

**Contenido** (pág. 238)

Seleccione la copia de seguridad y el contenido que desea recuperar.

**Credenciales de acceso** (pág. 239)

[Opcional] Proporcione las credenciales para la ubicación del archivo comprimido si la cuenta de la tarea no tiene derecho para acceder a ésta. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

## Dónde recuperar:

Esta sección aparece después de seleccionar la copia de seguridad necesaria y definir el tipo de datos que se desea recuperar. Los parámetros que especifique aquí dependerán del tipo de datos que se recuperen.

**Discos**

**Volúmenes**

**Acronis Active Restore**

[OPCIONAL] La casilla de verificación de **Acronis Active Restore** está disponible para la recuperación de Windows desde Windows 2000. Acronis Active Restore pone en línea un sistema inmediatamente después de que se inicia la recuperación. El sistema operativo se inicia desde la imagen de la copia de seguridad, y el equipo queda funcional y listo para proporcionar los servicios necesarios. Se recuperan los datos que se utilizarán para las solicitudes entrantes con la más alta prioridad; todo lo demás se recupera en segundo plano.

Consulte Acronis Active Restore (pág. 53) para obtener más información.

**Archivos** (pág. 246)

Es posible que tenga que especificar las credenciales para el destino. Omita este paso cuando opere en un equipo iniciado con un dispositivo de inicio.

**Credenciales de acceso** (pág. 247)

[Opcional] Proporcione las credenciales para el destino si las credenciales de la tarea no permiten recuperar los datos seleccionados. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

### Cuándo recuperar

**Recuperar** (pág. 248)

Seleccione cuándo desea iniciar la recuperación. La tarea puede iniciarse inmediatamente después de su creación, programarse para una determinada fecha y hora en el futuro o simplemente guardarse para su ejecución manual.

### [Opcional] Acronis Universal Restore

*Se aplica a: recuperación de sistema operativo y volumen del sistema Windows*

**Universal Restore** (pág. 248)

Utilice Acronis Universal Restore cuando necesite recuperar e iniciar Windows en hardware diferente.

**Búsqueda automática de controladores**

Especifique el lugar donde el programa debe buscar los controladores de HAL, almacenamiento masivo y adaptadores de red. Acronis Universal Restore instalará los controladores que mejor se adecuen al hardware de destino.

**Instalar de todas maneras los controladores de los dispositivos de almacenamiento masivo**

[Opcional] Especifique manualmente los controladores de almacenamiento masivo si la búsqueda automática de controladores no encontró los controladores apropiados. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

### Opciones de recuperación

**Configuraciones**

[Opcional] Para personalizar la operación de recuperación, configure las opciones de recuperación, como los comandos pre/post recuperación, la prioridad de recuperación, el manejo de errores o las opciones de notificación. Si no hace nada en esta sección, se usarán los valores predeterminados (pág. 121).

Después de que se modifique cualquiera de las configuraciones con respecto al valor predeterminado, aparecerá una nueva línea que mostrará el valor recientemente establecido. El estado de la configuración cambia de **Predeterminada** a **Personalizada**. Si modifica nuevamente la configuración, la línea mostrará el nuevo valor, a menos que el nuevo valor sea el predeterminado. Cuando se establece el valor predeterminado, la línea desaparece, de modo que siempre verá sólo la configuración que difiere de los valores predeterminados en la sección **Configuración**.

Al hacer clic en **Restablecer a los valores predeterminados**, se restablece la configuración a los valores predeterminados.

Una vez que haya completado todos los pasos necesarios, haga clic en **Aceptar** para ejecutar la creación de la tarea de recuperación.

## 6.3.1 Credenciales de la tarea

Proporcione las credenciales para la cuenta con la que se ejecutará la tarea.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Ejecutar con el usuario actual**

     La tarea se ejecutará con las credenciales de la cuenta con la que el usuario que inicia las tareas haya iniciado la sesión. Si la tarea debe ejecutarse según la programación, se le solicitará la contraseña del usuario actual al finalizar la creación de la tarea.
   - **Utilizar las siguientes credenciales**

     La tarea se ejecutará siempre con las credenciales que especifique, ya sea que se inicie manualmente o según la programación.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

Para obtener más información sobre cómo utilizar las credenciales para Acronis Backup & Recovery 10, consulte la sección Propietarios y credenciales (pág. 33).

Para obtener más información sobre las operaciones disponibles según los privilegios del usuario, consulte la sección Privilegios de usuario en un equipo gestionado (pág. 33).

## 6.3.2 Selección de archivos comprimidos

### Selección del archivo comprimido

1. Introduzca la ruta completa a la ubicación en el campo **Ruta** o seleccione la carpeta deseada en el árbol de carpetas.
   - Si el archivo comprimido se almacena en Acronis Online Backup Storage, haga clic en **Iniciar sesión** y especifique las credenciales de acceso al almacenamiento en línea. Después, expanda el grupo **Almacenamiento de copia de seguridad en línea** y seleccione la cuenta.

   *Las copias de seguridad almacenadas en Acronis Online Backup Storage no son aptas para la exportación ni el montaje.*
   - Si el archivo comprimido está almacenado en una bóveda centralizada, expanda el grupo **Centralizada** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una bóveda personal, expanda el grupo **Personal** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una carpeta local en el equipo, expanda en grupo **Carpetas locales** y haga clic en la carpeta correspondiente.

   *Si el archivo comprimido se encuentra en un medio extraíble como, por ejemplo, un DVD, introduzca primero el último DVD y, a continuación, los discos en orden comenzando por el primero cuando el programa le pregunte.*
   - Si el archivo comprimido se encuentra en una red compartida, expanda el grupo **Carpetas de red** y, a continuación, seleccione el equipo en red correspondiente y haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

***Nota para los usuario de Linux:*** *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como /mnt/share, seleccione este punto de montaje en lugar de la propia red compartida.*

- Si el archivo comprimido se encuentra en un servidor **FTP** o **SFTP**, escriba el nombre o la dirección del servidor en el campo **Ruta** tal y como se indica a continuación:

  **ftp://ftp_server:port _number o sftp://sftp_server:port number**

  Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

  Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

  Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

*Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

- Si el archivo comprimido se encuentra en un dispositivo de cinta conectado localmente, expanda el grupo **Dispositivos de cinta** y haga clic en el dispositivo correspondiente.

Cuando opere en un equipo iniciado con un dispositivo de inicio:

- Para acceder a la bóveda gestionada, escriba la siguiente cadena en el campo **Ruta**:

  **bsp://dirección_nodo/nombre_bóveda/**

- Para acceder a una bóveda centralizada sin gestionar, escriba la ruta completa de la carpeta de la bóveda.

2. En la tabla ubicada a la derecha del árbol, seleccione el archivo comprimido. La tabla muestra los nombres de los archivos comprimidos contenidos en cada una de las bóvedas/carpetas que seleccione.

   Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.
3. Haga clic en **Aceptar**.

## 6.3.3 Tipo de datos

Elija el tipo de datos para recuperar de la copia de seguridad del disco seleccionada.

- **Discos**: para recuperar discos
- **Volúmenes**: para recuperar volúmenes
- **Archivos**: para recuperar archivos y carpetas específicos

## 6.3.4 Selección del contenido

La representación de esta ventana depende del tipo de datos almacenados en el archivo comprimido.

### Selección de discos/volúmenes

***Para seleccionar una copia de seguridad y los discos/volúmenes para recuperar:***

1. Seleccione una de las copias de seguridad sucesivas según su fecha y hora de creación. De este modo, puede revertir los datos del disco a un momento determinado.

Especifique los elementos para recuperar. De manera predeterminada, se seleccionarán todos los elementos de la copia de seguridad seleccionada. Si no desea recuperar determinados elementos, simplemente desmárquelos.
Para obtener información sobre un disco/volumen, haga clic con el botón secundario sobre éste y después haga clic en **Información**.

2. Haga clic en **Aceptar**.

#### Selección de un MBR

Por lo general, seleccionará el MBR del disco si:

- El sistema operativo no puede iniciarse.
- El disco es nuevo y no cuenta con un MBR.
- Desea recuperar cargadores de inicio personalizados o que no sean de Windows (como LILO y GRUB).
- La geometría del disco es diferente de la almacenada en la copia de seguridad.

Es probable que haya otros casos en que necesite recuperar el MBR, pero los anteriores son los más comunes.

Al recuperar el MBR de un disco en otro, Acronis Backup & Recovery 10 recupera la pista 0, que no afecta la tabla de partición ni la distribución de la partición del disco de destino. Acronis Backup & Recovery 10 actualiza automáticamente los cargadores de Windows después de la recuperación, de modo que no es necesario recuperar el MBR y la pista 0 para los sistemas Windows, a menos que el MBR esté dañado.

### Selección de archivos

***Para seleccionar una copia de seguridad y los archivos que se van a recuperar:***

1. Seleccione una de las copias de seguridad sucesivas según su fecha/hora de creación. De esta manera, puede revertir los archivos/carpetas a un momento determinado.
2. Especifique los archivos y carpetas para recuperar al seleccionar las casillas de verificación correspondientes en el árbol de archivos comprimidos.

   Al seleccionar una carpeta, automáticamente se selecciona la totalidad de sus carpetas y archivos anidados.

   Utilice la tabla ubicada a la derecha del árbol de archivos comprimidos para seleccionar los elementos anidados. Al seleccionar la casilla de verificación del encabezado de la columna **Nombre**, se seleccionan automáticamente todos los elementos de la tabla. Al desmarcar esta casilla de verificación, se anula automáticamente la selección de todos los elementos.
3. Haga clic en **Aceptar**.

## 6.3.5 Credenciales de acceso para la ubicación

Especifique las credenciales necesarias para acceder a la ubicación donde está almacenado el archivo de copia de seguridad.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Utilizar las credenciales de la tarea**

     El programa accederá a la ubicación utilizando las credenciales de la cuenta de la tarea especificada en la sección General.
   - **Utilizar las siguientes credenciales**

El programa accederá a la ubicación utilizando las credenciales que especifique. Utilice esta opción si la cuenta de la tarea no dispone de permisos de acceso a la ubicación. Quizás necesite atribuir credenciales especiales para una red compartida o para una bóveda de nodo de almacenamiento.

Especifique:

- **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
- **Contraseña**. La contraseña de la cuenta.

2. Haga clic en **Aceptar**.

*Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

## 6.3.6 Selección del destino

Especifique el destino en el cual se recuperarán los datos seleccionados.

### Discos

La disponibilidad de los destinos de discos depende de los agentes que funcionan en el equipo.

**Recuperar a:**

**Equipo físico**

*Disponible cuando está instalado Acronis Backup & Recovery 10 Agent para Windows o Agent para Linux.*

Los discos seleccionados se recuperarán en los discos físicos del equipo al que esté conectada la consola. Al seleccionar esta opción, continuará con el procedimiento regular de asignación de discos que se describe a continuación.

**Máquina virtual nueva** (pág. 245)

*Si está instalado Acronis Backup & Recovery 10 Agent para Windows.*

Los discos seleccionados se recuperarán en un equipo virtual nuevo de cualquiera de los siguientes tipos: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) o Red Hat KVM. Los archivos del equipo virtual se guardarán en el destino que especifique.

*Si está instalado Acronis Backup & Recovery 10 Agent para Hyper-V o Agent para ESX/ESXi.*

Estos agentes permiten crear un equipo virtual nuevo en el servidor de virtualización que especifique.

El equipo virtual nuevo se configurará automáticamente, y la configuración del equipo de origen se copiará cuando sea posible. La configuración se muestra en la sección **Configuración del equipo virtual** (pág. 245). Verifique la configuración y realice los cambios correspondientes.

Después, continuará con el procedimiento regular de asignación de discos que se describe a continuación.

**Máquina virtual existente**

*Disponible cuando está instalado Acronis Backup & Recovery 10 Agent para Hyper-V o Agent para ESX/ESXi.*

Al seleccionar esta opción, se especifica el servidor de virtualización y el equipo virtual de destino. Después, continuará con el procedimiento regular de asignación de discos que se describe a continuación.

*Tenga en cuenta que el equipo de destino se apagará de manera automática antes de la recuperación. Si prefiere apagarlo manualmente, modifique la opción de administración de energía de VM.*

**N.° de disco:**

**N.° de disco (MODELO)** (pág. 243)

Seleccione el disco de destino para cada uno de los discos de origen.

**Firma NT** (pág. 241)

Seleccione el modo en que se gestionará la firma del disco recuperado. La firma del disco es utilizada por Windows, y por la versión 2.6 y versiones posteriores del kernel de Linux.

## Destino del disco

***Para especificar un disco de destino:***

1. Seleccione el disco donde desea recuperar el disco seleccionado. El espacio del disco de destino debe tener al menos el mismo tamaño que los datos de la imagen sin comprimir.
2. Haga clic en **Aceptar**.

*Todos los datos almacenados en el disco de destino se reemplazarán con los datos incluidos en la copia de seguridad; por lo tanto, tenga cuidado y controle si tiene datos sin copia de seguridad que pueda necesitar.*

## Firma NT

Cuando se selecciona el MBR junto con la copia de seguridad del disco, debe retener la capacidad de inicio del sistema operativo en el volumen del disco de destino. El sistema operativo debe tener la información de volumen del sistema (p. ej., la letra del volumen) coincidente con la firma NT del disco que se mantiene en el registro del disco MBR. Pero dos discos con la misma firma NT no pueden funcionar de manera correcta en un sistema operativo.

*Si hay dos discos que tienen la misma firma NT e incluyen un volumen del sistema en un equipo, al inicio el sistema operativo se ejecuta desde el primer disco, descubre la misma firma en el segundo, genera de manera automática una nueva firma NT única y se la asigna al segundo disco. Como resultado, todos los volúmenes del segundo disco perderán sus letras, todas las rutas serán inválidas en el disco y los programas no encontrarán sus archivos. El sistema operativo de ese disco no se iniciará.*

***Para retener la capacidad de inicio del sistema en el volumen del disco de destino, elija una de las siguientes opciones:***

- **Seleccione automáticamente**

  Se creará una nueva firma NT sólo si la existente difiere de la que se encuentra en la copia de seguridad. De lo contrario, se mantendrá la firma NT existente.

- **Crear nuevo**

  El programa generará una nueva firma NT para la unidad de disco duro de destino.

- **Recuperar a partir de la copia de seguridad**

  El programa reemplazará la firma NT del disco duro de destino por una de la copia de seguridad del disco.

Puede que desee recuperar la firma del disco por las siguientes razones:

- Acronis Backup & Recovery 10 crea tareas programadas usando la firma del disco duro de origen. Si recupera la misma firma del disco, no necesita volver a crear o editar las tareas que creó anteriormente.
- Algunas aplicaciones instaladas utilizan la firma del disco para fines de licencias y otros fines.
- Permite conservar todos los puntos de restauración de Windows en el disco recuperado.
- Para recuperar las instantáneas del VSS que utiliza la función "Versiones anteriores" de Windows Vista

- **Mantener los existentes**

  El programa dejará la firma NT existente del disco duro de destino tal como está.

## Volúmenes

La disponibilidad de los destinos de volúmenes depende de los agentes que funcionan en el equipo.

### Recuperar a:

**Equipo físico**

*Disponible cuando está instalado Acronis Backup & Recovery 10 Agent para Windows o Agent para Linux.*

Los volúmenes seleccionados se recuperarán en los discos físicos del equipo al que esté conectada la consola. Al seleccionar esta opción, continuará con el procedimiento regular de asignación de volúmenes que se describe a continuación.

**Máquina virtual nueva** (pág. 245)

*Si está instalado Acronis Backup & Recovery 10 Agent para Windows.*

Los volúmenes seleccionados se recuperarán en un equipo virtual nuevo de cualquiera de los siguientes tipos: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) o Red Hat KVM. Los archivos del equipo virtual se guardarán en el destino que especifique.

*Si está instalado Acronis Backup & Recovery 10 Agent para Hyper-V o Agent para ESX/ESXi.*

Estos agentes permiten crear un equipo virtual nuevo en el servidor de virtualización que especifique.

El equipo virtual nuevo se configurará automáticamente, y la configuración del equipo de origen se copiará cuando sea posible. La configuración se muestra en la sección **Configuración del equipo virtual** (pág. 245). Verifique la configuración y realice los cambios correspondientes.

Después, continuará con el procedimiento regular de asignación de volúmenes que se describe a continuación.

**Máquina virtual existente**

*Disponible cuando está instalado Acronis Backup & Recovery 10 Agent para Hyper-V o Agent para ESX/ESXi.*

Al seleccionar esta opción, se especifica el servidor de virtualización y el equipo virtual de destino. Después, continuará con el procedimiento regular de asignación de volúmenes que se describe a continuación.

*Tenga en cuenta que el equipo de destino se apagará de manera automática antes de la recuperación. Si prefiere apagarlo manualmente, modifique la opción de administración de energía de VM.*

**Recuperar [Nº de disco] MBR en: [Si se selecciona el Registro de inicio maestro (MBR) para la recuperación]**

**N° de disco:** (pág. 243)

Escoja el disco donde recuperar el Registro de inicio maestro (MBR).

**Firma NT:** (pág. 241)

Seleccione la forma en la que se gestionará la firma del disco que se encuentra en el MBR. La firma del disco es utilizada por Windows, y por la versión 2.6 y versiones posteriores del kernel de Linux.

**Recuperar [Volumen] [Letra] en:**

**N.° de disco/Volumen** (pág. 243)

Asigne de manera secuencial cada uno de los volúmenes de origen a un volumen o espacio no asignado del disco de destino.

**Tamaño**:

[Opcional] Cambie el tamaño, la ubicación y otras propiedades del volumen recuperado.

## Destino MBR

***Para especificar un disco de destino:***

1. Seleccione el disco en el que desea recuperar el MBR.
2. Haga clic en **Aceptar**.

## Destino del volumen

***Para especificar un volumen de destino:***

1. Seleccione un volumen o espacio no asignado donde desee que se recupere el volumen seleccionado. El volumen/espacio no asignado de destino deberá tener al menos el mismo tamaño que los datos de la imagen sin comprimir.
2. Haga clic en **Aceptar**.

*Todos los datos almacenados en el volumen de destino se reemplazarán con los datos incluidos en la copia de seguridad; por lo tanto, tenga cuidado y controle si tiene datos sin copia de seguridad que pueda necesitar.*

### Cuando utilice un dispositivo de inicio

Las letras de los discos que se ven en los dispositivos de inicio de estilo Windows pueden diferir de la manera en que Windows identifica las unidades. Por ejemplo, la unidad D: de la utilidad de rescate puede corresponder a la unidad E: de Windows.

*¡Cuidado! Para estar seguro, se aconseja asignar nombres únicos a los volúmenes.*

Los dispositivos de inicio de estilo Linux muestran los discos y volúmenes locales como desmontados (sda1, sda2...).

## Propiedades del volumen

### Cambios de tamaño y ubicación

Al recuperar un volumen en un disco MBR básico, puede cambiar el tamaño y la ubicación del volumen al arrastrarlo o arrastrar sus bordes con el ratón, o al introducir los valores correspondientes en los campos apropiados. Al utilizar esta función, puede redistribuir el espacio de

disco entre los volúmenes que se están recuperando. En este caso, deberá recuperar primero el volumen que se reducirá.

***Consejo:*** *El tamaño de un volumen no puede modificarse cuando se recupera desde una copia de seguridad dividida en múltiples DVD o cintas. Para poder modificar el tamaño de un volumen, copie todas las partes de la copia de seguridad en una ubicación única en un disco duro.*

### Propiedades

#### Tipo

Un disco MBR básico puede contener hasta cuatro volúmenes primarios o hasta tres volúmenes primarios, y varias unidades lógicas. De manera predeterminada, el programa selecciona el tipo del volumen original. Si fuera necesario, puede cambiar esta configuración.

- **Primarios**. La información sobre los volúmenes primarios está incluida en la tabla de partición del MBR. La mayoría de los sistemas operativos puede iniciarse solo desde el volumen primario del primer disco duro, pero la cantidad de volúmenes primarios es limitada.

  Si desea recuperar un volumen del sistema en un disco MBR básico, seleccione la casilla de verificación Activo. El volumen activo se usa para cargar un sistema operativo. Elegir la opción Activo para un volumen sin un sistema operativo instalado puede impedir el inicio del equipo. No puede establecer una unidad lógica o un volumen dinámico como activos.
- **Lógicos**. La información sobre los volúmenes lógicos no se encuentra en el MBR, sino en la tabla de partición extendida. La cantidad de volúmenes lógicos de un disco es ilimitada. Un volumen lógico no puede establecerse como activo. Si recupera un volumen del sistema en otro disco duro con sus propios volúmenes y sistema operativo, probablemente solo necesitará los datos. En este caso, puede recuperar el volumen como lógico para acceder únicamente a los datos.

#### Sistema de archivos

Si fuera necesario, cambie el sistema de archivos del volumen. De manera predeterminada, el programa selecciona el sistema de archivos del volumen original. Acronis Backup & Recovery 10 puede realizar las siguientes conversiones de sistemas de archivos: FAT 16 -> FAT 32 y Ext2 -> Ext3. Para volúmenes con otros sistemas de archivos nativos, esta opción no está disponible.

Supongamos que desea recuperar el volumen de un disco FAT16 antiguo y de poca capacidad en un disco más nuevo. FAT16 no sería efectivo y podría incluso ser imposible configurar en el disco duro de alta capacidad. Esto sucede porque FAT16 es compatible con volúmenes de hasta 4 GB, de manera que no podrá recuperar un volumen FAT16 de 4 GB en un volumen que exceda ese límite sin cambiar el sistema de archivos. En este caso, sería necesario cambiar el sistema de archivos de FAT16 a FAT32.

Los sistemas operativos más antiguos (MS-DOS, Windows 95 y Windows NT 3.x, 4.x) no son compatibles con FAT32 y no funcionarán después de recuperar un volumen y cambiar su sistema de archivos. Normalmente, estos sistemas solamente pueden recuperarse en un volumen FAT16.

#### Letra de unidad lógica (únicamente para Windows)

Asigne una letra al volumen recuperado. Seleccione la letra que desee de una lista desplegable.

- Con la selección AUTOMÁTICA predeterminada, la primera letra que no esté en uso será asignada al volumen.
- Si selecciona NO, no se asignará ninguna letra al volumen recuperado y se lo ocultará del sistema operativo. No debe asignar letras a volúmenes inaccesibles para Windows, como las que no son FAT o NTFS.

## Selección del tipo de equipo virtual / servidor de virtualización

El equipo virtual nuevo puede crearse en un servidor de virtualización (esto requiere la instalación de Acronis Backup & Recovery 10 Agent para Hyper-V o Agent para ESX/ESXi) o en cualquier carpeta local o en red accesible.

***Para seleccionar el servidor de virtualización en el que se creará el equipo virtual nuevo***

1. Elija la opción **Colocar en el servidor de virtualización que seleccione**.
2. En la parte izquierda de la ventana, seleccione el servidor de virtualización. Utilice la parte derecha de la ventana para revisar los detalles del servidor seleccionado.
3. Haga clic en **Aceptar** para volver a la página **Recuperación de datos**.

***Para seleccionar el tipo de equipo virtual***

1. Elija la opción **Guardar como archivos del tipo de equipo virtual que seleccione en la carpeta que especifique**.
2. En la parte izquierda de la ventana, seleccione el tipo de equipo virtual. Utilice la parte derecha de la ventana para revisar los detalles del tipo de equipo virtual seleccionado.
3. Haga clic en **Aceptar** para volver a la página **Recuperación de datos**.

## Configuración del equipo virtual

Se puede establecer la siguiente configuración del equipo virtual.

### Almacenamiento

**Configuración inicial:** el almacenamiento predeterminado del servidor de virtualización si el nuevo equipo se crea en el servidor de virtualización. De lo contrario, la carpeta de documentos del usuario actual.

Se trata del lugar donde se creará el nuevo equipo virtual. El hecho de que pueda o no cambiar el almacenamiento del servidor de virtualización dependerá de la marca y la configuración del producto de virtualización. VMware ESX puede tener varios almacenamientos. Un servidor Microsoft Hyper-V permite crear un equipo virtual nuevo en cualquier carpeta local.

### Memoria

**Configuración inicial:** si no está incluida en la copia de seguridad, la configuración predeterminada del servidor de virtualización.

Se trata de la cantidad de memoria asignada al equipo virtual nuevo. Los valores de ajuste de la memoria dependen del hardware del host, el sistema operativo del host y la configuración del producto de virtualización. Por ejemplo, es posible que los equipos virtuales no puedan utilizar más del 30% de la memoria.

### Discos

**Configuración inicial:** la cantidad y el tamaño de los discos del equipo de origen.

La cantidad de discos suele ser igual a la del equipo de origen, pero podría ser diferente si el programa tiene que añadir más discos para incluir los volúmenes del equipo de origen debido a las limitaciones establecidas por el producto de virtualización. Puede añadir discos virtuales a la configuración del equipo o, en algunos casos, eliminar los discos propuestos.

*La implementación de equipos Xen se basa en Microsoft Virtual PC y presenta sus mismas limitaciones: hasta 3 discos IDE y 1procesador. los discos SCSI no son compatibles.*

### Procesadores

**Configuración inicial:** si no está incluida en la copia de seguridad o si la configuración en copia de seguridad no es compatible con el servidor de virtualización, la configuración del servidor predeterminado.

Se trata de la cantidad de procesadores del equipo virtual nuevo. En la mayoría de los casos se establece en uno. No se garantiza que se asigne más de un procesador al equipo. La cantidad de procesadores virtuales puede estar limitada por la configuración de la CPU del host, el producto de virtualización y el sistema operativo invitado. Por lo general, varios procesadores virtuales están disponibles en servidores con múltiples procesadores. Una CPU de servidor con varios núcleos o la tecnología de varios hilos (hyperthreading) pueden permitir varios procesadores virtuales en un servidor con procesador único.

## Destino del archivo

***Para especificar un destino:***

1. Seleccione una ubicación en la que se recuperarán los archivos incluidos en la copia de seguridad:
   - **Ubicación original:** los archivos y carpetas se recuperarán con la(s) misma(s) ruta(s) que tenían en la copia de seguridad. Por ejemplo, si realizó una copia de seguridad de todos los archivos y carpetas en C:\Documentos\Finanzas\Informes\, los archivos se recuperarán con la misma ruta. Si la carpeta no existe, se creará automáticamente.
   - **Nueva ubicación**: los archivos se recuperarán en la ubicación que especifique en el árbol. Los archivos y carpetas se recuperarán sin volver a crear una ruta completa, a menos que desmarque la casilla de verificación **Recuperar sin la ruta completa**.
2. Haga clic en **Aceptar**.

## Exclusiones de la recuperación

Configure exclusiones para los archivos específicos que no desea recuperar.

Utilice los botones **Agregar**, **Editar**, **Eliminar** y **Eliminar todo** para crear la lista de máscaras de archivos. Durante la recuperación, se pasarán por alto los archivos cuyos nombres coincidan con alguna de las máscaras.

Puede utilizar uno o más caracteres comodín * y ? en una máscara de archivo:

- El asterisco (*) sustituye de cero a más caracteres del nombre del archivo; por ejemplo, la máscara de archivo Doc*.txt genera archivos Doc.txt y Document.txt
- El signo de interrogación (?) substituye a un único carácter; por ejemplo, la máscara de archivo Doc?.txt genera archivos Doc1.txt y Docs.txt, pero, por el contrario, no general archivos Doc.txt o Doc11.txt

**Ejemplos de exclusión**

| Criterio | Ejemplo | Descripción |
|---|---|---|
| **Windows y Linux** | | |
| Por nombre | F.log<br>F | Excluye todos los archivos denominados "F.log"<br>Excluye todas las carpetas denominadas "F" |
| Por máscara (*) | *.log<br>F* | Excluye todos los archivos con la extensión .log<br>Excluye todos los archivos y carpetas cuyos nombres comiencen con "F" (como carpetas F, F1 y archivos F.log, F1.log) |
| Por máscara (?) | F???.log | Excluye todos los archivos .log cuyos nombres contengan cuatro símbolos y comiencen con "F" |
| **Windows** | | |
| Por ruta de archivo | Finance\F.log | Excluye los archivos denominados "F.log" de todas las carpetas con el nombre "Finance" |
| Por ruta de carpeta | Finance\F\ o Finance\F | Excluye las carpetas denominadas "F" de todas las carpetas con el nombre "Finance" |
| **Linux** | | |
| Por ruta de archivo | /home/user/Finance/F.log | Excluye el archivo denominado "F.log", ubicado en la carpeta /home/user/Finance |

Las configuraciones anteriores no se realizarán para los archivos o carpetas que se seleccionaron explícitamente para la recuperación. Por ejemplo, supongamos que seleccionó la carpeta MiCarpeta y el archivo MiArchivo.tmp fuera de esa carpeta, y seleccionó la opción de omitir todos los archivos .tmp. En este caso, todos los archivos .tmp de la carpeta MiCarpeta serán omitidos durante el proceso de recuperación, pero no se omitirá el archivo MiArchivo.tmp.

## Sobrescritura

Elija qué hacer si el programa encuentra un archivo en la carpeta de destino que tenga el mismo nombre que el que se encuentra en el archivo comprimido:

- **Sobrescribir el archivo existente**: esto le dará prioridad al archivo de la copia de seguridad sobre el archivo del disco duro
- **Sobrescribir el archivo existente en caso de que sea anterior**: esto le dará prioridad a la modificación más reciente del archivo, ya sea que se haya realizado en la copia de seguridad o en el disco.
- **No sobrescribir el archivo existente**: esto le dará prioridad al archivo del disco duro sobre el archivo de la copia de seguridad.

Si permite que los archivos se sobrescriban, aún tiene la opción de evitar la sobrescritura de archivos específicos excluyéndolos (pág. 246) de la operación de recuperación.

### 6.3.7 Credenciales de acceso para el destino

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Utilizar las credenciales de la tarea**

     El programa accederá al destino utilizando las credenciales de la cuenta de la tarea especificada en la sección General.
   - **Utilice las siguientes credenciales.**

     El programa accederá al destino utilizando las credenciales que usted especifique. Utilice esta opción si la cuenta de la tarea no tiene permisos de acceso para el destino.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

### 6.3.8 Cuándo recuperar

Seleccione cuándo desea iniciar la tarea de recuperación:

- **Recuperar ahora**: la tarea de recuperación se iniciará inmediatamente después de que haga clic en **Aceptar**, en el paso final.
- **Recuperar más tarde**: la tarea de recuperación se iniciará en la fecha y hora que especifique.

Si no necesita programar la tarea y desea iniciarla manualmente después, seleccione la casilla de verificación **La tarea se iniciará manualmente (no programe la tarea)**.

### 6.3.9 Universal Restore

Utilice Acronis Backup & Recovery 10 Universal Restore cuando necesite recuperar e iniciar Windows en hardware diferentes. Universal Restore controla las diferencias en los dispositivos que son críticos para el inicio del sistema operativo, como controladores de almacenamiento, placa madre o conjunto de chips.

Para obtener más información sobre la tecnología Universal Restore, consulte la sección Universal Restore (pág. 52).

#### Acronis Backup & Recovery 10 Universal Restore no está disponible cuando:

- un equipo se inicia con Acronis Startup Recovery Manager (utilizando F11)
- la imagen de copia de seguridad está ubicada en Acronis Secure Zone
- ha optado por utilizar Acronis Active Restore (pág. 400)

debido a que estas funciones fueron especialmente diseñadas para la recuperación instantánea de datos en el mismo equipo.

#### Preparación

Antes de recuperar Windows en hardware diferentes, asegúrese de tener los controladores para el nuevo controlador de disco duro y el conjunto de chips. Estos controladores son críticos para iniciar

el sistema operativo. Utilice el CD o DVD suministrado por el proveedor del hardware o descargue los controladores del sitio web del proveedor. Los archivos de controlador deben tener las extensiones *.inf, *.sys o *.oem. Si descarga los controladores en el formato *.exe, *.cab o *.zip, extráigalos usando la aplicación de un tercero, como WinRAR (http://www.rarlab.com/) o Universal Extractor (http://legroom.net/software/uniextract).

Se recomienda almacenar los controladores para todo el hardware utilizado en su organización en un mismo depósito, ordenados según el tipo de dispositivo o las configuraciones de hardware. Puede conservar una copia del depósito en un DVD o una unidad de memoria flash; elija algunos controladores y añádalos al dispositivo de inicio; cree un dispositivo de inicio personalizado con los controladores necesarios (y la configuración de red necesaria) para cada uno de sus servidores. O bien, simplemente especifique la ruta al depósito cada vez que utilice Universal Restore.

Asegúrese de tener acceso al dispositivo con controladores cuando trabaje con el dispositivo de inicio. Incluso si configura la recuperación del disco de sistema en un entorno de Windows, el equipo se reiniciará y la recuperación continuará en el entorno basado en Linux. Utilice el dispositivo basado en WinPE si el dispositivo está disponible en Windows, pero el dispositivo basado en Linux no lo detecta.

### Configuración de Universal Restore

#### Búsqueda automática de controladores

Especifique el lugar donde el programa debe buscar los controladores de la capa de abstracción del hardware (HAL), el controlador de disco duro y los adaptadores de red:

- Si los controladores se encuentran en el disco de un proveedor u otro medio extraíble, active la opción **Buscar en medios extraíbles**.

- Si los controladores se encuentran en una carpeta en red o en el dispositivo de inicio, especifique la ruta a la carpeta en el campo **Buscar en carpeta**.

Durante la recuperación, Universal Restore ejecutará la búsqueda repetitiva en todas las subcarpetas de la carpeta especificada, encontrará los controladores de HAL y del controlador de disco duro más apropiados entre todos los que estén disponibles, y los instalará en el sistema recuperado. Universal Restore también busca el controlador de adaptadores de red; luego, Universal Restore transmite al sistema operativo la ruta al controlador encontrado. Si el hardware cuenta con varias tarjetas de interfaz de red, Universal Restore intentará configurar los controladores de todas las tarjetas. En caso de que Universal Restore no pueda encontrar un controlador compatible en las ubicaciones especificadas, indicará el dispositivo con problema y solicitará un disco o una ruta de red al controlador.

Una vez que Windows se inicie, ejecutará el procedimiento estándar para instalar un nuevo hardware. El controlador de adaptadores de red se instalará silenciosamente si el controlador tiene la firma de Microsoft Windows. De lo contrario, Windows solicitará confirmación para instalar el controlador sin firma.

Después, podrá configurar la conexión de red y especificar los controladores para el adaptador de vídeo, USB y otros dispositivos.

#### Instalar de todas maneras los controladores de los dispositivos de almacenamiento masivo

Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Si el hardware de destino tiene un controlador de almacenamiento masivo específico, como RAID (especialmente, NVIDIA RAID) o un adaptador de canal de fibra, especifique los controladores apropiados en el campo **Controladores**.

Los controladores definidos aquí tendrán prioridad. Estos controladores se instalarán, con las advertencias correspondientes, incluso si el programa encuentra un controlador mejor.

Utilice esta opción solo si la opción de búsqueda automática de controladores no ayuda a iniciar el sistema.

### Controladores para un equipo virtual

Al recuperar un sistema en un equipo virtual nuevo, la tecnología Universal Restore se aplica en segundo plano, dado que el programa sabe qué controladores son necesarios para los equipos virtuales compatibles.

Al recuperar el sistema en un equipo virtual existente que utiliza el controlador de disco duro SCSI, asegúrese de especificar los controladores SCSI para el entorno virtual, en el paso **Instalar de todas maneras los controladores de almacenamiento masivo**. Utilice los controladores incluidos en el software de su equipo virtual o descargue las últimas versiones de los controladores del sitio web del fabricante de software.

## 6.3.10 Cómo convertir una copia de seguridad del disco en un equipo virtual

En vez de convertir un archivo TIB a un archivo de disco virtual, que necesita operaciones adicionales para que el disco virtual pueda utilizarse, Acronis Backup & Recovery 10 realiza la conversión al recuperar una copia de seguridad del disco a una nueva máquina virtual completamente configurada y operativa. Tiene la capacidad de adaptar la configuración de la máquina virtual a sus necesidades cuando configura la operación de recuperación.

Con el **Acronis Backup & Recovery 10 Agent para Windows** puede recuperar la copia de seguridad de un disco (volumen) en un equipo virtual nuevo de uno de los siguientes tipos: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) o Red Hat KVM.

Los archivos de la nueva máquina virtual se colocarán en la carpeta que seleccione. Puede iniciar el equipo con el correspondiente software de virtualización o preparar los archivos del equipo para otros usos. El Citrix XenServer Open Virtual Appliance (OVA) puede ser importado a XenServer utilizando Citrix XenCenter. El equipo VMware Workstation puede convertirse al formato de virtualización abierta (OVF) con la herramienta VMware OVF.

Con **Acronis Backup & Recovery 10 Agent para Hyper-V** o **Agent para ESX/ESXi** puede recuperar una copia de seguridad del disco (volumen) a una nueva máquina virtual en el servidor de virtualización respectivo.

***Consejo.*** *Microsoft Virtual PC no es compatible con discos de más de127 GB. Acronis le permite crear máquinas Virtual PC con discos más grandes de forma que pueda adjuntar el disco a una máquina virtual Microsoft Hyper-V.*

***Para convertir una copia de seguridad del disco en un equipo virtual:***

1. Conecte la consola a un equipo en donde esté instalado Agente para Windows, Agente para Hyper-V o Agente para ESX/ESXi.
2. Realice uno de los siguientes:
   - Haga clic en **Recuperar** para abrir la página de **Recuperar datos**. Inicie la creación de una tarea de recuperación como se describe en "Recuperación de datos". Seleccione el archivo comprimido y después seleccione la copia de seguridad de disco o volumen que desea convertir.
   - Utilice el panel de **Navegación** para navegar hasta la bóveda en donde está almacenado el archivo comprimido. Seleccione el archivo comprimido y después seleccione la copia de

seguridad de disco o volumen que desea convertir. Haga clic en **Recuperar como máquina virtual**. La página **Recuperar datos** se abre con la copia de seguridad preseleccionada.

3. En **Tipo de datos**, seleccione **Discos** o **Volúmenes** dependiendo de lo que necesite convertir.
4. En **Contenido**, seleccione los discos para convertir o los volúmenes con el registro de inicio maestro (MBR) de los discos correspondientes.
5. En **Recuperar a**, seleccione **Nueva máquina virtual**.
6. En **Servidor VM**, seleccione el tipo de la nueva máquina virtual que se creará *o* en qué servidor de virtualización se creará el equipo.
7. En **Nombre de VM**, introduzca el nombre del nuevo equipo virtual.
8. [Opcional] Revise las **Configuraciones de la máquina virtual (pág. 245)** y realice los cambios necesarios. Aquí puede especificar la ruta a la nueva máquina virtual.

   *No se puede crear el mismo tipo de equipo con el mismo nombre en la misma carpeta. Cambie el nombre de la VM o la ruta si obtiene un mensaje de error generado por nombres idénticos.*

9. Seleccione el disco de destino para cada uno de los discos de origen o los volúmenes de origen y los MBR.

   *En un PC virtual de Microsoft, asegúrese de recuperar el disco o volumen donde reside el cargador del sistema operativo en el disco duro 1. De lo contrario, el sistema operativo no arrancará. Esto no se puede arreglar cambiando el orden del dispositivo de inicio en la BIOS, ya que un PC virtual ignora esos ajustes.*

10. En **Cuándo recuperar**, debe especificar el momento en que comenzará la tarea.
11. [Opcional] Revise las **Opciones de recuperación** y cambie la configuración predeterminada, si fuera necesario. Puede especificar en **Opciones de recuperación > Administración de energía VM** si quiere iniciar de forma automática la nueva máquina virtual después de que la recuperación haya sido completada. Esta opción está disponible solo cuando el nuevo equipo se crea en un servidor de virtualización.
12. Haga clic en **Aceptar**. Si la tarea de recuperación está programada para el futuro, especifique las credenciales con las que se ejecutará la tarea.

Pasará a la vista **Planes y tareas de copia de seguridad** en donde podrá examinar el estado y progreso de la tarea de recuperación.

### Operaciones postconversión

El equipo resultante siempre tiene una interfaz de disco SCSI y volúmenes MBR básicos. Si el equipo utiliza un cargador de inicio personalizado, puede que deba configurar el cargador para que apunte a nuevos dispositivos y reactivarlo. La configuración GRUB se describe en "Cómo reactivar GRUB y modificar su configuración (pág. 253)".

***Consejo.*** *Si desea conservar los volúmenes lógicos (LVM) en un equipo con Linux, considere el método alternativo de conversión. Cree una nueva máquina virtual, iníciela mediante un dispositivo de inicio y lleve a cabo la recuperación como en un equipo físico. La estructura LVM puede recrearse automáticamente (pág. 289) durante la recuperación si se ha guardado en la copia de seguridad.*

## 6.3.11 Solución de problemas de capacidad de inicio

Si un sistema era inicializable al momento de realizar una copia de seguridad, se espera que se inicie después de la recuperación. Sin embargo, la información que el sistema operativo almacena y utiliza para el inicio puede desactualizarse durante la recuperación, especialmente si cambia los tamaños de volúmenes, las ubicaciones o las unidades de destino. Acronis Backup & Recovery 10 actualiza de manera automática los cargadores de Windows después de la recuperación. También puede haber

otros cargadores que sean fijos, pero en algunos casos es necesario reactivar los cargadores. Específicamente al recuperar volúmenes de Linux, se necesita a veces efectuar reparaciones o realizar cambios en el inicio para que Linux se pueda iniciar y cargar correctamente.

A continuación, encontrará un resumen de las situaciones típicas que requieren acciones adicionales por parte del usuario.

### Por qué un sistema operativo recuperado no se inicia

- **El BIOS del equipo está configurado para iniciarse desde otro disco duro.**

  **Solución**: configure el BIOS para que se inicie desde el disco duro donde reside el sistema operativo.

- **El sistema se recuperó en un hardware diferente y el nuevo hardware es incompatible con la mayoría de los controladores más críticos incluidos en la copia de seguridad.**

  **Solución para Windows**: vuelva a recuperar el volumen. Al configurar la recuperación, opte por usar Acronis Universal Restore y especifique los controladores de HAL y almacenamiento masivo apropiados.

- **Windows se recuperó en un volumen dinámico que no puede iniciarse**

  **Solución**: recupere Windows en un volumen básico, simple o replicado.

- **Un volumen del sistema se recuperó en un disco que no tiene un MBR**

  Cuando configure la recuperación de un volumen del sistema en un disco que no tenga un MBR, el programa le preguntará si desea recuperar el MBR junto con el volumen del sistema. Opte por no recuperarlo, solo si no desea que el sistema sea inicializable.

  **Solución**: vuelva a recuperar el volumen junto con el MBR del disco correspondiente.

- **El sistema utiliza Acronis OS Selector**

  Como el registro de inicio maestro (MBR) puede cambiarse durante la recuperación del sistema, es posible que Acronis OS Selector, que utiliza el MBR, deje de funcionar. Si esto sucede, reactive Acronis OS Selector de la siguiente manera.

  **Solución**: inicie el equipo desde el dispositivo de inicio de Acronis Disk Director y seleccione en el menú **Herramientas -> Activar OS Selector**.

- **El sistema utiliza el cargador de inicio GRUB y se recuperó a partir de una copia de seguridad normal (no una copia sin procesar, es decir, sector por sector)**

  Una parte del cargador GRUB reside en los primeros sectores del disco o en los primeros sectores del volumen. El resto se encuentra en el sistema de archivos de uno de los volúmenes. La capacidad de inicio del sistema puede recuperarse automáticamente solo cuando el GRUB reside en los primeros sectores del disco y en el sistema de archivos al cual es posible tener acceso directo. En otros casos, el usuario debe reactivar el cargador de inicio manualmente.

  **Solución**: reactive nuevamente el cargador de inicio. También es posible que tenga que reparar el archivo de configuración.

- **El sistema utiliza el cargador de Linux (LILO) y se recuperó a partir de una copia de seguridad normal (no una copia sin procesar, es decir, sector por sector)**

  LILO contiene numerosas referencias a números de sectores absolutos; por lo tanto, no puede repararse automáticamente, excepto cuando todos los datos se recuperan en los sectores que tienen los mismos números absolutos que el disco de origen.

  **Solución**: reactive nuevamente el cargador de inicio. También es posible que tenga que reparar el archivo de configuración del cargador por el motivo descrito en el punto anterior.

- **El cargador del sistema apunta al volumen equivocado**

  Esto puede suceder cuando los volúmenes del sistema o de inicio no se recuperan en su ubicación original.

  **Solución**:

  La modificación de los archivos boot.ini o boot\bcd permite reparar este problema para los cargadores de Windows. Acronis Backup & Recovery 10 hace esto de forma automática; por lo tanto, es poco probable que tenga este problema.

  Para los cargadores GRUB y LILO, deberá corregir los archivos de configuración del GRUB. Si el número de la partición raíz de Linux cambió, también se recomienda cambiar /etc/fstab para poder acceder correctamente al volumen SWAP.

- **Linux se recuperó a partir de la copia de seguridad de un volumen LVM en un disco MBR básico**

  Este sistema no puede iniciarse porque su kernel intenta montar el sistema de archivos raíz en el volumen LVM.

  **Solución**: cambie la configuración del cargador y /etc/fstab para que LVM no se utilice, y active el cargador de inicio.

## Cómo reactivar GRUB y cambiar su configuración

Por lo general, debe consultar las páginas del manual correspondientes a cargadores de inicio para conocer el procedimiento apropiado. También se encuentra el artículo correspondiente en la Base de Conocimientos en el sitio Web de Acronis.

El siguiente es un ejemplo de cómo reactivar GRUB en caso que el disco del sistema (volumen) sea recuperado en un hardware idéntico.

1. Inicie Linux o cárguelo desde el medio iniciable, y luego presione CTRL+ALT+F2.
2. Monte el sistema que está recuperando:

```
mkdir /mnt/system/
mount -t ext3 /dev/sda2 /mnt/system/ # root particion
mount -t ext3 /dev/sda1 /mnt/system/boot/ # boot particion
```

3. Corra los sistemas de archivo **proc** y **dev** para el sistema que está recuperando:

```
mount -t proc none /mnt/system/proc/
mount -o bind /dev/ /mnt/system/dev/
```

4. Guarde una copia del archivo de menú GRUB, ejecutando uno de los siguientes comandos:

```
cp /mnt/system/boot/grub/menu.lst /mnt/system/boot/grub/menu.lst.backup
```

   o

```
cp /mnt/system/boot/grub/grub.conf /mnt/system/boot/grub/grub.conf.backup
```

5. Edite el archivo **/mnt/system/boot/grub/menu.lst** (para las distribuciones Debian, Ubuntu, y SUSE Linux) o el archivo **/mnt/system/boot/grub/grub.conf** (para las distribuciones Fedora y Linux Enterprise Red Hat), por ejemplo, como figura a continuación:

```
vi /mnt/system/boot/grub/menu.lst
```

6. En el archivo **menu.lst** (respectivamente **grub.conf**), encuentre el elemento del menú que corresponde al sistema que está recuperando. Los elementos de este menú tienen la siguiente forma:

```
title Red Hat Enterprise Linux Server(2.6.24.4)
      root (hd0,0)
      kernel /vmlinuz-2.6.24.4 ro root=/dev/sda2 rhgb quiet
      initrd /initrd-2.6.24.4.img
```

Las líneas que comienzan con **título**, **raíz,kernel e initrd** determinan respectivamente:

- El título del elemento del menú.
- El dispositivo en el cual el núcleo Linux se encuentra: típicamente, la partición de inicio o la partición de raíz, como la **raíz (hd0,0)** en este ejemplo.
- La ruta al núcleo en ese dispositivo y la partición de raíz: en este ejemplo, la ruta es **/vmlinuz-2.6.24.4** y la partición de raíz es **/dev/sda2**. Puede especificar la partición de raíz por etiqueta (como **root=LABEL=/**), identificador (en la forma **root=UUID=***some_uuid*), o nombre de dispositivo (como **root=/dev/sda2**).
- La ruta al servicio **initrd** en dicho dispositivo.

7. Edite el archivo **/mnt/system/etc/fstab** para corregir los nombres de cualquier dispositivo que haya cambiado como resultado de la recuperación.
8. Inicie la shell de GRUB ejecutando uno de los siguientes comandos:

   ```
   chroot /mnt/system/ /sbin/grub
   ```

   o

   ```
   chroot /mnt/system/ /sbin/grub
   ```

9. Especifique el disco en el cual se ubica GRUB: generalmente, la partición de inicio o de raíz:

   ```
   root (hd0,0)
   ```

10. Instalar GRUB. Por ejemplo, para GRUB en el registro de inicio maestro (MBR) del primer disco, ejecute el siguiente comando:

    ```
    setup (hd0)
    ```

11. Salir del shell de GRUB:

    ```
    quit
    ```

12. Desmontar los sistemas de archivos montados y luego reiniciar:

    ```
    umount /mnt/system/dev/
    umount /mnt/system/proc/
    umount /mnt/system/boot/
    umount /mnt/system/
    reboot
    ```

13. Reconfigurar el cargador de arranque utilizando las herramientas y documentación de distribución Linux que usa. Por ejemplo, en Debian y Ubuntu, puede precisar editar algunas líneas comentadas en el archivo **/boot/grub/menu.lst** y luego ejecutar el script **update-grub**; caso contrario, los cambios pueden no resultar efectivos.

## Acerca de los cargadores de Windows

### Windows NT/2000/XP/2003

Una parte del cargador reside en el sector de inicio de la partición y el resto se encuentra en los archivos ntldr, boot.ini, ntdetect.com, ntbootdd.sys. El archivo boot.ini es un archivo de texto que contiene la configuración del cargador. Ejemplo:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
/noexecute=optin /fastdetect
```

**Windows Vista/2008**

Una parte del cargador reside en el sector de inicio de la partición y el resto se encuentra en los archivos bootmgr, boot\bcd. Al iniciar Windows, boot\bcd se monta a la clave de registro HKLM \BCD00000000.

### 6.3.12 Recuperación del nodo de almacenamiento

Además de realizar copias de seguridad de datos a bóvedas centralizadas por Nódulo de Almacenamiento Acronis Backup & Recovery 10, puede realizar una copia de seguridad del disco de la máquina donde el nódulo de almacenamiento está instalado.

Esta sección describe cómo recuperar el nodo de almacenamiento en el servidor de gestión en caso de que el nódulo de almacenamiento y el servidor de gestión estén instalados en máquinas diferentes (si están instalados en la misma máquina, simplemente recupere la máquina).

Considere el siguiente escenario:

- Tiene una máquina con el servidor de gestión y una máquina con un nodo de almacenamiento..
- El nodo de almacenamiento está registrado en el servidor de gestión.
- Realizó la copia de seguridad de la máquina con el nodo de almacenamiento en otro momento, y lo acaba de recuperar, en la misma máquina o en otra diferente.

Antes de utilizar el nodo de almacenamiento recuperado, realice lo siguiente:

- Si ha recuperado del nodo de almacenamiento en la misma máquina y no se han añadido o quitado bóvedas centralizadas administradas por el nodo de almacenamiento entre la copia de seguridad y recuperación, no haga nada.
- Caso contrario, haga lo siguiente:
  1. Conéctese al servidor de gestión y remueva el nodo de almacenamiento.

  ***Nota:*** *Todas las bóvedas administradas por el nodo de almacenamiento serán eliminadas del servidor de gestión. No se perderán archivos.*

  2. Añada el nodo de almacenamiento al servidor de gestión nuevamente, especificando la máquina en la cual el nodo de almacenamiento está instalado.
  3. Vuelva a crear las bóvedas de gestión necesarias.

## 6.4 Validar bóvedas, archivos comprimidos y copias de seguridad

La validación es una operación que verifica la posibilidad de recuperación de datos en una copia de seguridad.

La validación de la copia de seguridad de un archivo imita la recuperación de todos los archivos de la copia de seguridad a un destino simulado. La validación de la copia de seguridad de un disco o volumen calcula la suma de comprobación por cada bloque de datos guardados en la copia de seguridad. Ambos procedimientos utilizan muchos recursos.

La validación de un archivo comprimido validará las copias de seguridad del archivo comprimido. La validación de una bóveda (o una ubicación) validará todos los archivos comprimidos almacenados en esta bóveda (ubicación).

Si bien una validación satisfactoria implica una gran probabilidad de recuperación exitosa, no verifica todos los factores que tienen influencia sobre el proceso de recuperación. Si realiza una copia de seguridad del sistema operativo, solo se podrá garantizar una recuperación exitosa con una recuperación de prueba en el entorno de inicio a una unidad de disco duro libre. Al menos, asegúrese de que la copia de seguridad pueda validarse correctamente utilizando el dispositivo de inicio.

### Diferentes formas de crear una tarea de validación

La forma más general de crear una tarea de validación consiste en usar la página Validación. En esa página puede validar inmediatamente o establecer una programación de validación para cualquier copia de seguridad, archivo comprimido o ubicación a la cual tenga permitido acceder.

La validación de un archivo comprimido o de la copia de seguridad más reciente del archivo comprimido puede programarse como parte del plan de copia de seguridad. Para obtener más información, consulte la sección Creación de un plan de copia de seguridad (pág. 207).

Puede acceder a la página **Validación** desde la vista **Bóvedas** (pág. 130). Haga clic con el botón secundario en el objeto que desee validar (archivo comprimido, copia de seguridad o bóveda), y seleccione **Validar** del menú contextual. La página Validación se abrirá con el objeto preseleccionado como origen. Solo tiene que seleccionar cuándo debe realizarse la validación y (opcionalmente) proporcionar un nombre para la tarea.

**Para crear una tarea de validación, realice los siguientes pasos.**

#### General

**Nombre de la tarea**

[Opcional] Introduzca un nombre único para la tarea de validación. Un nombre pensado deliberadamente le permite identificar de manera rápida una tarea entre las demás.

**Credenciales** (pág. 257)

[Opcional] La tarea de validación se ejecutará en nombre del usuario que cree la tarea. De ser necesario, podrá cambiar las credenciales de la tarea. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

#### Qué validar

**Validar**

Elija un objeto para validar:

**Archivo comprimido** (pág. 257): en ese caso, es necesario que especifique el archivo comprimido.

**Copia de seguridad** (pág. 258): especifique primero el archivo y después seleccione la copia de seguridad deseada en este archivo comprimido.

**Bóveda** (pág. 259): seleccione la bóveda (u otra ubicación) cuyos archivos comprimidos desee validar.

**Credenciales de acceso** (pág. 259)

[Opcional] Proporcione las credenciales para acceder al origen si la cuenta de la tarea no tiene suficientes privilegios para acceder a este. Para acceder a esta opción, seleccione la casilla de verificación **Vista avanzada**.

#### Cuándo validar

**Validar** (pág. 260)

Especifique cuándo y con qué frecuencia debe realizarse la validación.

Una vez que haya establecido la configuración necesaria, haga clic en **Aceptar** para crear la tarea de validación.

### 6.4.1 Credenciales de la tarea

Proporcione las credenciales para la cuenta con la que se ejecutará la tarea.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Ejecutar con el usuario actual**

     La tarea se ejecutará con las credenciales de la cuenta con la que el usuario que inicia las tareas haya iniciado la sesión. Si la tarea debe ejecutarse según la programación, se le solicitará la contraseña del usuario actual al finalizar la creación de la tarea.
   - **Utilizar las siguientes credenciales**

     La tarea se ejecutará siempre con las credenciales que especifique, ya sea que se inicie manualmente o según la programación.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

Para obtener más información sobre cómo utilizar las credenciales para Acronis Backup & Recovery 10, consulte la sección Propietarios y credenciales (pág. 33).

Para obtener más información sobre las operaciones disponibles según los privilegios del usuario, consulte la sección Privilegios de usuario en un equipo gestionado (pág. 33).

### 6.4.2 Selección de archivos comprimidos

**Selección del archivo comprimido**

1. Introduzca la ruta completa a la ubicación en el campo **Ruta** o seleccione la carpeta deseada en el árbol de carpetas.
   - Si el archivo comprimido se almacena en Acronis Online Backup Storage, haga clic en **Iniciar sesión** y especifique las credenciales de acceso al almacenamiento en línea. Después, expanda el grupo **Almacenamiento de copia de seguridad en línea** y seleccione la cuenta.

   *Las copias de seguridad almacenadas en Acronis Online Backup Storage no son aptas para la exportación ni el montaje.*
   - Si el archivo comprimido está almacenado en una bóveda centralizada, expanda el grupo **Centralizada** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una bóveda personal, expanda el grupo **Personal** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una carpeta local en el equipo, expanda en grupo **Carpetas locales** y haga clic en la carpeta correspondiente.

   *Si el archivo comprimido se encuentra en un medio extraíble como, por ejemplo, un DVD, introduzca primero el último DVD y, a continuación, los discos en orden comenzando por el primero cuando el programa le pregunte.*

- Si el archivo comprimido se encuentra en una red compartida, expanda el grupo **Carpetas de red** y, a continuación, seleccione el equipo en red correspondiente y haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

***Nota para los usuario de Linux:*** *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como /mnt/share, seleccione este punto de montaje en lugar de la propia red compartida.*

- Si el archivo comprimido se encuentra en un servidor **FTP** o **SFTP**, escriba el nombre o la dirección del servidor en el campo **Ruta** tal y como se indica a continuación:

  **ftp://ftp_server:port _number o sftp://sftp_server:port number**

  Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

  Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

  Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

*Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

- Si el archivo comprimido se encuentra en un dispositivo de cinta conectado localmente, expanda el grupo **Dispositivos de cinta** y haga clic en el dispositivo correspondiente.

Cuando opere en un equipo iniciado con un dispositivo de inicio:

- Para acceder a la bóveda gestionada, escriba la siguiente cadena en el campo **Ruta**:

  **bsp://dirección_nodo/nombre_bóveda/**

- Para acceder a una bóveda centralizada sin gestionar, escriba la ruta completa de la carpeta de la bóveda.

2. En la tabla ubicada a la derecha del árbol, seleccione el archivo comprimido. La tabla muestra los nombres de los archivos comprimidos contenidos en cada una de las bóvedas/carpetas que seleccione.

   Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.
3. Haga clic en **Aceptar**.

### 6.4.3 Selección de la copia de seguridad

***Para especificar una copia de seguridad para validar***

1. En el panel superior, seleccione una copia de seguridad por su fecha/hora de creación.

   La parte inferior de la ventana muestra el contenido de la copia de seguridad seleccionada, lo cual le ayuda a encontrar la copia de seguridad correcta.
2. Haga clic en **Aceptar**.

### 6.4.4 Selección de la ubicación

***Para seleccionar una ubicación***

Introduzca la ruta completa a la ubicación en el campo **Ruta** o seleccione la ubicación deseada en el **árbol de carpetas**.

- Para seleccionar una bóveda centralizada, expanda el grupo **Centralizada** y haga clic en la bóveda.
- Para seleccionar una bóveda personal, expanda el grupo **Personal** y haga clic en la bóveda.
- Para seleccionar la carpeta local (unidad de CD/DVD, o dispositivo de cintas adjunto local), expanda el grupo de **Carpetas locales** y haga clic en la carpeta que precisa.
- Para seleccionar una red compartida, amplíe el grupo **Carpetas de red**, seleccione el equipo en red correspondiente y después haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.
- Para seleccionar un servidor **FTP** o **SFTP**, amplíe el grupo correspondiente y haga clic en la carpeta correspondiente del servidor.

Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

#### Uso de la tabla de archivos comprimidos

Para ayudarle a elegir la ubicación correcta, la tabla muestra los nombres de los archivos comprimidos incluidos en cada ubicación que seleccione. Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.

### 6.4.5 Credenciales de acceso para el origen

Especifique las credenciales necesarias para acceder a la ubicación donde está almacenado el archivo de copia de seguridad.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Utilizar las credenciales de la tarea**

     El programa accederá a la ubicación utilizando las credenciales de la cuenta de la tarea especificada en la sección General.
   - **Utilizar las siguientes credenciales**

     El programa accederá a la ubicación utilizando las credenciales que especifique. Utilice esta opción si la cuenta de la tarea no dispone de permisos de acceso a la ubicación. Quizás necesite atribuir credenciales especiales para una red compartida o para una bóveda de nodo de almacenamiento.

     Especifique:

     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.

2. Haga clic en **Aceptar**.

*Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

### 6.4.6 Cuándo validar

Como la validación es una operación que utiliza muchos recursos, es conveniente programar la validación para el período de menor actividad del equipo gestionado. Por otro lado, si prefiere que le informen de inmediato si los datos no están dañados y pueden recuperarse correctamente, considere la opción de iniciar la validación de inmediato después de la creación de la tarea.

***Elija una de las siguientes opciones:***

- **Ahora**: para iniciar la tarea de validación inmediatamente después de su creación, es decir, después de hacer clic en Aceptar en la página Validación.
- **Más tarde**: para iniciar la tarea de validación solo una vez en la fecha y hora que especifique.

  Especifique los parámetros apropiados de la siguiente manera:
  - **Fecha y hora**: la fecha y hora en que debe comenzar la tarea.
  - **La tarea se iniciará manualmente (no programe la tarea)**: seleccione esta casilla de verificación si desea iniciar la tarea manualmente más tarde.
- **Según programación**: para programar la tarea. Para obtener más información sobre cómo configurar los parámetros de programación, consulte la sección Programación (pág. 173).

## 6.5 Montaje de una imagen

El montaje de volúmenes a partir de una copia de seguridad del disco (imagen) le permite acceder a los volúmenes como si se tratara de discos físicos. Se pueden montar varios volúmenes incluidos en la misma copia de seguridad dentro de una única operación de montaje. La operación de montaje está disponible cuando la consola está conectada a un equipo gestionado que ejecuta Windows o Linux.

El montaje de volúmenes en el modo de lectura-grabación le permite modificar el contenido de la copia de seguridad, es decir, guardar, mover, crear o eliminar archivos o carpetas, y ejecutar ejecutables que consten de un archivo.

***Limitación:*** *No es posible realizar el montaje de copias de seguridad del volumen en el nodo de almacenamiento de Acronis Backup & Recovery 10.*

**Escenarios de uso:**

- **Compartir**: las imágenes montadas pueden compartirse fácilmente con los usuarios en red.
- **Solución de recuperación de base de datos "Band aid"**: monte una imagen que contenga una base de datos SQL desde una máquina que falló recientemente. Esto dará acceso a la base de datos hasta que se recupere la máquina que falló.
- **Limpieza de virus fuera de línea**: Si una máquina es atacada, el administrador la cierra, la reinicia con medios reiniciables y crea una imagen. Luego, el administrador configura esta imagen en modo de lectura/escritura, la escanea y limpia con un programa antivirus, y finalmente recupera la máquina.

- **Comprobación de errores**: si falla la recuperación debido a un error de disco, monte la imagen en el modo lectura/escritura. Luego, compruebe el disco en búsqueda de errores por medio del comando **chkdsk /r**.

***Para montar una imagen, realice los siguientes pasos.***

**Origen**

**Archivo comprimido** (pág. 261)

Especifique la ruta a la ubicación del archivo comprimido y seleccione el archivo comprimido que contenga copias de seguridad del disco.

**Crear copia de seguridad** (pág. 262)

Seleccione la copia de seguridad.

**Credenciales de acceso** (pág. 262)

[Opcional] Proporcione las credenciales para la ubicación del archivo comprimido. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

**Configuración del montaje**

**Volúmenes** (pág. 263)

Seleccione los volúmenes para montar y establezca la configuración del montaje para cada volumen: asigne una letra o introduzca el punto de montaje, elija el modo de acceso de lectura/grabación o de sólo lectura.

Cuando haya completado todos los pasos obligatorios, haga clic en **Aceptar** para montar los volúmenes.

## 6.5.1 Selección de archivos comprimidos

**Selección del archivo comprimido**

1. Introduzca la ruta completa a la ubicación en el campo **Ruta** o seleccione la carpeta deseada en el árbol de carpetas.
   - Si el archivo comprimido se almacena en Acronis Online Backup Storage, haga clic en **Iniciar sesión** y especifique las credenciales de acceso al almacenamiento en línea. Después, expanda el grupo **Almacenamiento de copia de seguridad en línea** y seleccione la cuenta.

   *Las copias de seguridad almacenadas en Acronis Online Backup Storage no son aptas para la exportación ni el montaje.*

   - Si el archivo comprimido está almacenado en una bóveda centralizada, expanda el grupo **Centralizada** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una bóveda personal, expanda el grupo **Personal** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una carpeta local en el equipo, expanda en grupo **Carpetas locales** y haga clic en la carpeta correspondiente.

   *Si el archivo comprimido se encuentra en un medio extraíble como, por ejemplo, un DVD, introduzca primero el último DVD y, a continuación, los discos en orden comenzando por el primero cuando el programa le pregunte.*

   - Si el archivo comprimido se encuentra en una red compartida, expanda el grupo **Carpetas de red** y, a continuación, seleccione el equipo en red correspondiente y haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

***Nota para los usuario de Linux:*** *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como /mnt/share, seleccione este punto de montaje en lugar de la propia red compartida.*

- Si el archivo comprimido se encuentra en un servidor **FTP** o **SFTP**, escriba el nombre o la dirección del servidor en el campo **Ruta** tal y como se indica a continuación:

  **ftp://ftp_server:port _number o sftp://sftp_server:port number**

  Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

  Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

  Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

*Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

- Si el archivo comprimido se encuentra en un dispositivo de cinta conectado localmente, expanda el grupo **Dispositivos de cinta** y haga clic en el dispositivo correspondiente.

Cuando opere en un equipo iniciado con un dispositivo de inicio:

- Para acceder a la bóveda gestionada, escriba la siguiente cadena en el campo **Ruta**:

  **bsp://dirección_nodo/nombre_bóveda/**

- Para acceder a una bóveda centralizada sin gestionar, escriba la ruta completa de la carpeta de la bóveda.

2. En la tabla ubicada a la derecha del árbol, seleccione el archivo comprimido. La tabla muestra los nombres de los archivos comprimidos contenidos en cada una de las bóvedas/carpetas que seleccione.

   Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.
3. Haga clic en **Aceptar**.

## 6.5.2 Selección de la copia de seguridad

***Para seleccionar una copia de seguridad:***

1. Seleccione una de las copias de seguridad por su fecha/hora de creación.
2. Para ayudarle a elegir la copia de seguridad correcta, la tabla de la parte inferior muestra los volúmenes incluidos en la copia de seguridad seleccionada.

   Para obtener información sobre un volumen, haga clic con el botón secundario sobre este y después haga clic en **Información**.
3. Haga clic en **Aceptar**.

## 6.5.3 Credenciales de acceso

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:

   - **Utilizar las credenciales actuales de usuario**

     El programa accederá a la ubicación utilizando las credenciales del usuario actual.

- **Utilice las siguientes credenciales.**

  El programa accederá a la ubicación mediante las credenciales que especifique. Utilice esta opción si la cuenta del usuario actual no tiene permisos de acceso para la ubicación. Es posible que tenga que proporcionar credenciales especiales para una red compartida o una bóveda del nodo de almacenamiento.

  Especifique:

  - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
  - **Contraseña**. La contraseña de la cuenta.

2. Haga clic en **Aceptar**.

*Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

### 6.5.4 Selección de volúmenes

Seleccione los volúmenes para montar y configure los parámetros de montaje para cada uno de los volúmenes seleccionados de la siguiente manera:

1. Seleccione la casilla de verificación para cada volumen que necesite montar.
2. Haga clic en el volumen seleccionado para establecer sus parámetros de montaje.
   - **Modo de acceso**: elija el modo en que desea montar el volumen:
     - **Sólo lectura**: permite explorar y abrir archivos dentro de la copia de seguridad sin ejecutar ningún cambio.
     - **Lectura/grabación**: con este modo, el programa asume que se modificará el contenido de la copia de seguridad, y crea una copia de seguridad incremental para capturar los cambios.
   - **Asignar letra** (en Windows): Acronis Backup & Recovery 10 asignará una letra que no esté en uso al volumen montado. Si fuera necesario, seleccione otra letra para asignar de la lista desplegable.
   - **Punto de montaje** (en Linux): especifique el directorio donde desea que se monte el volumen.
3. Si se seleccionan varios volúmenes para montar, haga clic en cada volumen para establecer sus parámetros de montaje, tal como se describió en el paso anterior.
4. Haga clic en **Aceptar**.

## 6.6 Gestión de imágenes montadas

Una vez que se haya montado un volumen, podrá examinar los archivos y carpetas incluidos en la copia de seguridad con un administrador de archivos, y copiar los archivos deseados en cualquier destino. Por lo tanto, si necesita sacar solo algunos archivos y carpetas de la copia de seguridad de un volumen, no es necesario que realice el procedimiento de recuperación.

#### Exploración de imágenes

La exploración de volúmenes montados le permite ver y modificar el contenido del volumen (si el montaje se realizó en el modo de lectura/grabación).

Para explorar un volumen montado, selecciónelo en la tabla y haga clic en **Explorar**. Se abrirá la ventana del administrador de archivos predeterminado, lo que permitirá al usuario examinar el contenido del volumen montado.

### Desmontaje de imágenes

Mantener los volúmenes montados ocupa una cantidad considerable de recursos del sistema. Se recomienda que desmonte los volúmenes una vez que se hayan completado las operaciones necesarias. Si no se desmonta manualmente, un volumen permanecerá montado hasta que se reinicie el sistema operativo.

Para desmontar una imagen, selecciónela en la tabla y haga clic en **Desmontar**.

Para desmontar todos los volúmenes montados, haga clic en **Desmontar todo**.

## 6.7 Exportación de archivos comprimidos y copias de seguridad

La operación de exportación crea una copia de un archivo comprimido o una copia parcial de un archivo comprimido en la ubicación especificada. El archivo comprimido original permanece intacto.

La operación de exportación puede aplicarse a:

- **un único archivo comprimido** - se creará una copia exacta del archivo comprimido
- **una única copia de seguridad** - se creará un archivo comprimido que contiene una única copia de seguridad completa. La exportación de una copia de seguridad incremental o diferencial se realiza utilizando la consolidación de las copias de seguridad anteriores hasta la última copia de seguridad completa
- **su selección de copias de seguridad** que pertenecen al mismo archivo comprimido, el archivo comprimido resultante contendrá sólo las copias de seguridad especificadas. La consolidación se realiza según sus necesidades, para que el archivo comprimido resultante pueda contener copias de seguridad completas, incrementales y diferenciales.
- **una bóveda completa** que puede exportarse utilizando la interfaz de línea de comandos. Para obtener más información, consulte la referencia de la línea de comandos de Acronis Backup & Recovery 10.

**Escenarios de usos:**

La exportación le permite separar una copia de seguridad específica de una cadena de copias de seguridad incrementales para una rápida recuperación, escribir sobre dispositivos extraíbles u otros propósitos.

**Ejemplo.** Al realizar una copia de seguridad de datos a una ubicación remota mediante una conexión de red inestable o con un bajo ancho de banda (como una copia de seguridad a través de WAN con acceso VPN), es posible que desee guardar la copia de seguridad completa inicial a un dispositivo extraíble. Después, enviar el dispositivo a la ubicación remota. Allí la copia de seguridad se exportará desde el dispositivo al almacenamiento de destino. Las copias de seguridad incrementales posteriores, que generalmente son mucho más pequeñas, se pueden transferir a través de la red.

Al exportar una bóveda gestionada a un dispositivo extraíble, obtiene una bóveda portátil sin gestionar que puede utilizarse en las siguientes situaciones:

- la conservación de una copia externa de su bóveda o de los archivos comprimidos más importantes

- el transporte físico de una bóveda a una sucursal distante
- la recuperación sin acceso al nodo de almacenamiento en el caso de problemas de red o fallos en el nodo de almacenamiento
- la recuperación del nodo de almacenamiento mismo.

La exportación desde una bóveda basada en HDD a un dispositivo de cinta puede considerarse como un simple ajuste de archivo bajo petición.

**El nombre del archivo comprimido resultante**

De manera predeterminada, el archivo comprimido exportado hereda el nombre del archivo original. Debido a que tener varios archivos con el mismo nombre en la misma ubicación no es conveniente, las siguientes acciones están desactivadas en el nombre de archivo comprimido predeterminado:

- exportación de parte de un archivo comprimido a la misma ubicación
- exportación de un archivo comprimido o parte de un archivo comprimido a una ubicación donde existe un archivo comprimido con el mismo nombre
- exportación de un archivo comprimido o parte de un archivo comprimido a la misma ubicación dos veces

En cualquiera de los casos anteriores, proporcione un nombre de archivo comprimido que sea único en la carpeta o bóveda de destino. Si debe rehacer la exportación utilizando el mismo nombre de archivo comprimido, elimine primero el archivo comprimido que resultó de la operación de exportación anterior.

**Las opciones del archivo comprimido resultante**

El archivo comprimido exportado hereda las opciones del archivo comprimido original, incluyendo el cifrado y la contraseña. Al exportar un archivo comprimido protegido con contraseña, se le pedirá que introduzca la contraseña. Si el archivo comprimido está cifrado, se utilizará la contraseña para cifrar el archivo comprimido resultante.

**Ubicación del origen y el destino**

Cuando la consola está conectada a un **equipo gestionado**, puede exportar un archivo comprimido o parte de un archivo hacia y desde cualquier ubicación accesible al agente que reside en el equipo. Estos incluyen bóvedas personales, dispositivos de cinta conectados localmente, medios extraíbles y, en las versiones avanzadas de los productos, bóvedas centralizadas gestionadas y sin gestionar.

Cuando la consola esté conectada al **management server**, están disponibles dos métodos de exportación:

- exportación desde una **bóveda centralizada**. El nodo de almacenamiento que gestiona la bóveda realiza la exportación. El destino puede ser una red compartida o una carpeta local del nodo de almacenamiento.
- exportación desde un **bóveda centralizada sin gestionar**. El agente instalado en el equipo gestionado que usted especifique realiza la exportación. El destino puede ser cualquier ubicación accesible al agente, incluyendo una bóveda gestionada.

***Consejo.*** *Cuando configure una exportación a una bóveda gestionada de deduplicación, seleccione un equipo donde esté instalado el complemento de deduplicación en el agente. De lo contrario la tarea de exportación fallará.*

**Operaciones con una tarea de exportación**

Una tarea de exportación comienza inmediatamente después de que complete su configuración. Una tarea de exportación puede detenerse o eliminarse de la misma manera que cualquier otra tarea.

Una vez que ha finalizado la tarea de exportación, puede ejecutarla nuevamente en cualquier momento. Antes de hacerlo, elimine el archivo comprimido que resultó de la ejecución de la tarea anterior si el archivo comprimido aún existe en la bóveda de destino. De lo contrario la tarea fallará. No puede editar una tarea de exportación para especificar otro nombre para el archivo comprimido de destino (esto es una limitación).

***Consejo.*** *Puede implementar el ajuste de la situación manualmente ejecutando regularmente la tarea de eliminación del archivo comprimido seguida de la tarea de exportación.*

**Maneras diferentes de crear una tarea de exportación**

La forma más general de crear una tarea de exportación consiste en usar la página **Exportación**. Aquí, puede exportar cualquier copia de seguridad o archivo comprimido al que tenga permiso para acceder.

Puede acceder a la página **Exportación** desde la vista **Bóvedas**. Haga clic en el objeto a exportar (archivos comprimidos o copias de seguridad) y seleccione **Exportar** desde el menú contextual. La página **Exportar** se abrirá con el objeto preseleccionado como origen. Todo lo que debe hacer es seleccionar el destino y (de manera opcional) proporcionar un nombre para la tarea.

***Para exportar un archivo comprimido o una copia de seguridad siga los siguientes pasos.***

## General

**Nombre de la tarea**

[Opcional] Introduzca un nombre único para la tarea. Un nombre pensado deliberadamente le permite identificar de manera rápida una tarea entre las demás.

**Credenciales de la tarea** (pág. 267)

[Opcional] La tarea de exportación se ejecutará en nombre del usuario que cree la tarea. De ser necesario, podrá cambiar las credenciales de la tarea. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

## Qué exportar

**Exportar**

Seleccione un objeto para exportar:

**Archivo comprimido** (pág. 237) - en ese caso, debe especificar solamente el archivo comprimido.

**Copias de seguridad** (pág. 268) - primero especifique el archivo comprimido y luego seleccione las copias de seguridad deseadas en este archivo comprimido

**Credenciales de acceso** (pág. 269)

[Opcional] Proporcione las credenciales para acceder al origen si la cuenta de la tarea no tiene suficientes privilegios para acceder a este. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

## Dónde exportar

**Archivo comprimido** (pág. 269)

Introduzca la ruta a la ubicación donde se creará el archivo comprimido nuevo.

Asegúrese de proporcionar un nombre distintivo e introduzca un comentario para el nuevo archivo comprimido.

**Credenciales de acceso** (pág. 271)

[Opcional] Proporcione las credenciales para el destino si las credenciales de la tarea no tienen suficientes privilegios para accederlas. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Después de realizar todos los pasos requeridos, haga clic en **Aceptar** para comenzar a exportar la tarea.

### 6.7.1 Credenciales de la tarea

Proporcione las credenciales para la cuenta con la que se ejecutará la tarea.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Ejecutar con el usuario actual**

     La tarea se ejecutará con las credenciales de la cuenta con la que el usuario que inicia las tareas haya iniciado la sesión. Si la tarea debe ejecutarse según la programación, se le solicitará la contraseña del usuario actual al finalizar la creación de la tarea.
   - **Utilizar las siguientes credenciales**

     La tarea se ejecutará siempre con las credenciales que especifique, ya sea que se inicie manualmente o según la programación.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

Para obtener más información sobre cómo utilizar las credenciales para Acronis Backup & Recovery 10, consulte la sección Propietarios y credenciales (pág. 33).

Para obtener más información sobre las operaciones disponibles según los privilegios del usuario, consulte la sección Privilegios de usuario en un equipo gestionado (pág. 33).

### 6.7.2 Selección de archivos comprimidos

***Para seleccionar un archivo comprimido***

1. Introduzca la ruta completa a la ubicación en el campo Ruta o seleccione la carpeta deseada en el árbol de carpetas.
   - Si el archivo comprimido se almacena en Acronis Online Backup Storage, haga clic en **Iniciar sesión** y especifique las credenciales de acceso al almacenamiento en línea. Después, expanda el grupo **Almacenamiento de copia de seguridad en línea** y seleccione la cuenta.

   *Las copias de seguridad almacenadas en Acronis Online Backup Storage no son aptas para la exportación ni el montaje.*
   - Si el archivo comprimido está almacenado en una bóveda centralizada, expanda el grupo **Centralizada** y haga clic en la bóveda.

- Si el archivo comprimido está almacenado en una bóveda personal, expanda el grupo **Personal** y haga clic en la bóveda.
- Si el archivo comprimido está almacenado en una carpeta local en el equipo, expanda en grupo **Carpetas locales** y haga clic en la carpeta correspondiente.

*Si el archivo comprimido se encuentra en un medio extraíble como, por ejemplo, un DVD, introduzca primero el último DVD y, a continuación, los discos en orden comenzando por el primero cuando el programa le pregunte.*

- Si el archivo comprimido se encuentra en una red compartida, expanda el grupo **Carpetas de red** y, a continuación, seleccione el equipo en red correspondiente y haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

***Nota para los usuario de Linux:*** *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como /mnt/share, seleccione este punto de montaje en lugar de la propia red compartida.*

- Si el archivo comprimido se encuentra en un servidor **FTP** o **SFTP**, escriba el nombre o la dirección del servidor en el campo **Ruta** tal y como se indica a continuación:

  **ftp://ftp_server:port _number o sftp://sftp_server:port number**

  Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

  Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

  Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

*Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

- Si el archivo comprimido se encuentra en un dispositivo de cinta conectado localmente, expanda el grupo **Dispositivos de cinta** y haga clic en el dispositivo correspondiente.

Para el management server: En el árbol de carpetas, seleccione la bóveda gestionada.

2. En la tabla ubicada a la derecha del árbol, seleccione el archivo comprimido. La tabla muestra los nombres de los archivos comprimidos contenidos en cada una de las bóvedas/carpetas que seleccione. Si el archivo comprimido está protegido con contraseña, proporcione la contraseña.

   Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.
3. Haga clic en **Aceptar**.

## 6.7.3 Selección de la copia de seguridad

***Para especificar una copia de seguridad a exportar***

1. En la parte superior de la ventana, seleccione la casilla de verificación correspondiente.

   Para asegurarse de que seleccionó la copia de seguridad correcta, haga clic en la copia de seguridad y observe la tabla de la parte inferior que muestra el volumen que contiene la copia de seguridad seleccionada.

   Para obtener información sobre un volumen, haga clic con el botón secundario sobre éste y después seleccione **Información**.

2. Haga clic en **Aceptar**.

### 6.7.4 Credenciales de acceso para el origen

Especifique las credenciales necesarias para acceder a la ubicación donde está almacenado el archivo comprimido (o la copia de seguridad) de origen.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Utilizar las credenciales de la tarea**

     El programa accederá a la ubicación utilizando las credenciales de la cuenta de la tarea especificada en la sección General.
   - **Utilizar las siguientes credenciales**

     El programa accederá a la ubicación utilizando las credenciales que especifique. Utilice esta opción si la cuenta de la tarea no dispone de permisos de acceso a la ubicación. Quizás necesite atribuir credenciales especiales para una red compartida o para una bóveda de nodo de almacenamiento.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

*Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

### 6.7.5 Selección de la ubicación

Especifique un destino donde se almacenará el objeto exportado. La exportación de copias de seguridad al mismo archivo comprimido no está permitida.

#### 1. Selección de destino de la exportación

Introduzca la ruta de destino completa en el campo **Ruta** o seleccione el destino deseado en el árbol de carpetas.

- Para exportar datos a una bóveda centralizada sin gestionar, expanda el grupo **Bóvedas centralizadas** y haga clic en la bóveda.
- Para exportar datos a una bóveda personal, expanda el grupo **Bóvedas personales** y haga clic en la bóveda.
- Para exportar datos a una carpeta local en el equipo, expanda el grupo **Carpetas locales** y haga clic en la carpeta requerida.
- Para exportar datos a una red compartida, expanda el grupo **Carpetas de red**, seleccione el equipo en red requerido y luego haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

  ***Nota para los usuario de Linux:*** *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como /mnt/share, seleccione este punto de montaje en lugar de la propia red compartida.*

- Para exportar datos a un servidor **FTP** o **SFTP**, escriba el nombre o la dirección del servidor en el campo **Ruta** de la siguiente manera:

  **ftp://ftp_server:port _number** o **sftp://sftp_server:port number**

  Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

  Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

  Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

  *De acuerdo con la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

- Para exportar datos a un dispositivo de cinta conectado a nivel local, amplíe el grupo **Unidades de cinta** y haga clic en el dispositivo correspondiente.

Para el management server el árbol de carpetas contiene:

- Un grupo de carpetas locales para exportar datos a los discos duros que son locales para el nodo de almacenamiento.
- Un grupo de carpetas en red para exportar datos a una red compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

  *Nota para los usuario de Linux: Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como /mnt/share, seleccione este punto de montaje en lugar de la propia red compartida.*

### 2. Uso de la tabla de archivos comprimidos

Para asistirle en la elección del destino correcto, la tabla a la derecha muestra los nombres de los archivos comprimidos contenidos en cada una de las ubicaciones que seleccione en el árbol.

Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.

### 3. Nombrar un archivo comprimido nuevo

De manera predeterminada, el archivo comprimido exportado hereda el nombre del archivo original. Debido a que tener varios archivos con el mismo nombre en la misma ubicación no es conveniente, las siguientes acciones están desactivadas en el nombre de archivo comprimido predeterminado:

- exportación de parte de un archivo comprimido a la misma ubicación
- exportación de un archivo comprimido o parte de un archivo comprimido a una ubicación donde existe un archivo comprimido con el mismo nombre
- exportación de un archivo comprimido o parte de un archivo comprimido a la misma ubicación dos veces

En cualquiera de los casos anteriores, proporcione un nombre de archivo comprimido que sea único en la carpeta o bóveda de destino. Si debe rehacer la exportación utilizando el mismo nombre de archivo comprimido, elimine primero el archivo comprimido que resultó de la operación de exportación anterior.

### 6.7.6 Credenciales de acceso para el destino

Especifique las credenciales necesarias para acceder a la ubicación donde se almacenará el archivo comprimido resultante. El usuario cuyo nombre se especifique se considerará el propietario del archivo comprimido.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Utilizar las credenciales de la tarea**

     El programa accederá a la ubicación utilizando las credenciales de la cuenta de la tarea especificada en la sección General.
   - **Utilizar las siguientes credenciales**

     El programa accederá a la ubicación utilizando las credenciales que especifique. Utilice esta opción si la cuenta de la tarea no dispone de permisos de acceso a la ubicación. Quizás necesite atribuir credenciales especiales para una red compartida o para una bóveda de nodo de almacenamiento.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

*Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

## 6.8 Acronis Secure Zone

Acronis Secure Zone es una partición segura que permite mantener archivos de copia de seguridad en el espacio de disco de un equipo gestionado y, por lo tanto, recuperar un disco del mismo disco donde reside la copia de seguridad.

Ciertas aplicaciones de Windows, como las herramientas de gestión de discos de Acronis pueden acceder a la zona.

Para obtener más información sobre las ventajas y limitaciones de Acronis Secure Zone, consulte el apartado Acronis Secure Zone (pág. 50) en la sección "Tecnologías patentadas de Acronis".

### 6.8.1 Creación de Acronis Secure Zone

Puede crear una Acronis Secure Zone cuando el sistema operativo se está ejecutando o cuando está utilizando un dispositivo de arranque.

***Para crear una Acronis Secure Zone, lleve a cabo los siguientes pasos.***

**Espacio**

Disco (pág. 272)

Escoja un disco duro (si hay más de uno) donde creará la zona. Acronis Secure Zone se crea utilizando un espacio no asignado, si hay espacio disponible, o a partir del espacio libre del volumen.

Tamaño (pág. 272)

Especifique el tamaño exacto de la zona. Mover o cambiar de tamaño de volúmenes bloqueados, tales como el volumen del actual sistema operativo activo, requiere reiniciar el sistema.

**Configuraciones**

Contraseña (pág. 273)

[Opcional] Proteja Acronis Secure Zone de accesos no autorizados mediante una contraseña. Se solicitará la contraseña para cualquier operación relacionada con la zona.

Después de configurar los ajustes requeridos, haga clic en Aceptar. En la ventana Confirmación de resultado (pág. 273), revise la distribución especificada y haga clic en Aceptar para comenzar a crear la zona.

## Disco de Acronis Secure Zone

Acronis Secure Zone puede ubicarse en cualquier disco duro fijo. Acronis Secure Zone siempre se crea al final del disco duro. Un equipo puede tener solo una Acronis Secure Zone. Acronis Secure Zone se crea utilizando un espacio no asignado, si hay espacio disponible, o a partir del espacio libre del volumen.

*Acronis Secure Zone no se puede organizar en un disco dinámico o disco que utiliza el estilo de partición GPT.*

***Para asignar espacio a Acronis Secure Zone***

1. Escoja un disco duro (si hay más de uno) donde creará la zona. El espacio no asignado se selecciona de manera predeterminada. El programa muestra la totalidad de espacio disponible para Acronis Secure Zone.
2. Si necesita asignar más espacio a la zona, puede seleccionar volúmenes desde donde se pueda obtener espacio libre. Nuevamente, el programa muestra la totalidad de espacio disponible para Acronis Secure Zone según su selección. Podrá configurar el tamaño exacto de la zona en la ventana **Tamaño de Acronis Secure Zone.** (pág. 272)
3. Haga clic en **Aceptar**.

## Tamaño de Acronis Secure Zone

Introduzca el tamaño de Acronis Secure Zone o arrastre el deslizador para seleccionar cualquier tamaño entre los mínimos y los máximos. El tamaño mínimo es aproximadamente de 50 MB, de acuerdo con la geometría del disco duro. El tamaño máximo es igual al espacio no asignado del disco más el espacio libre total de todos los volúmenes que haya seleccionado en el paso anterior.

Si tiene que sacar espacio del volumen de inicio o del sistema, tenga en cuenta lo siguiente:

- Para mover o cambiar el tamaño del volumen desde el cual se arranca actualmente el sistema, será necesario reiniciar.

- Sacar todo el espacio libre de un volumen del sistema puede hacer que el sistema operativo funcione de forma inestable e incluso que no pueda iniciarse. No configure el tamaño máximo de la zona si está seleccionado el volumen de inicio o del sistema.

## Contraseña para Acronis Secure Zone

Configurar una contraseña protege a Acronis Secure Zone contra accesos no autorizados. El programa solicitará la contraseña para cualquier operación relacionada con la zona y los archivos comprimidos que se encuentren en ella, como realización de copias de seguridad y recuperación de datos, validación de archivos comprimidos, modificación de tamaño y eliminación de la zona.

***Configurar una contraseña***

1. Seleccione **Utilizar contraseña**.
2. En el campo **Introducir contraseña**, escriba una nueva contraseña.
3. En el campo **Confirmar contraseña**, vuelva a escribir la contraseña.
4. Haga clic en **Aceptar**.

***Para deshabilitar la contraseña***

1. Seleccione **No utilizar**.
2. Haga clic en **Aceptar**.

## Confirmación del resultado

La ventana **Confirmación del resultado** muestra la distribución esperada de la partición de acuerdo con los ajustes que haya elegido. Haga clic en **Aceptar** si está de acuerdo con la distribución y se iniciará la creación de Acronis Secure Zone.

### Cómo se procesarán los ajustes que realiza

Esto le ayudará a comprender cómo la creación de Acronis Secure Zone transformará un disco que contenga varios volúmenes.

- Acronis Secure Zone siempre se crea al final del disco duro. Cuando calcule la distribución final de los volúmenes, el programa utilizará primero el espacio no asignado al final.
- Si no hay espacio o no suficiente espacio no asignado al final del disco, pero sí hay espacio no asignado entre volúmenes, los mismos se moverán para agregar más espacio no asignado al final.
- Cuando se recopile todo el espacio no asignado y el mismo siga siendo insuficiente, el programa sacará espacio libre de los volúmenes que seleccione, de forma proporcional, reduciendo el tamaño de los volúmenes. Para modificar el tamaño de los volúmenes bloqueados, es necesario reiniciar el sistema.
- Sin embargo, debería haber espacio libre en un volumen para que el sistema operativo y las aplicaciones puedan funcionar; por ejemplo, para crear archivos temporales. El programa no reducirá un volumen en el que el espacio libre ocupe o quede en un nivel inferior al 25% del tamaño total del mismo. El programa continuará reduciendo los volúmenes de forma proporcional, únicamente cuando todos los volúmenes del disco tengan el 25% o menos espacio libre.

Como se deduce de lo mencionado previamente, no es recomendable configurar el máximo posible para el tamaño de la zona. Acabará sin espacio libre en ningún volumen, lo que puede hacer que el sistema operativo o las aplicaciones funcionen de forma inestable e incluso que no puedan iniciarse.

## 6.8.2 Gestión de Acronis Secure Zone

Acronis Secure Zone se considera una bóveda (pág. 401) personal. Una vez que se crea en un equipo gestionado, la zona está presente siempre en la lista de **Bóvedas personales**. Los planes de copias de seguridad centralizados pueden utilizar Acronis Secure Zone al igual que los planes locales.

Si ha utilizado Acronis Secure Zone anteriormente, tenga en cuenta que se ha producido un cambio radical en su funcionamiento. La zona ya no realiza limpiezas automáticas, es decir, ya no elimina archivos comprimidos antiguos. Utilice esquemas de copia de seguridad con limpieza automática para realizar copias de seguridad en la zona o elimine manualmente archivos comprimidos desactualizados mediante la función de gestión de la bóveda.

Con el nuevo comportamiento de Acronis Secure Zone, puede conseguir:

- elaborar una lista de los archivos comprimidos ubicados en la zona y de las copias de seguridad en cada archivo comprimido
- examinar el contenido de una copia de seguridad,
- montar la copia de seguridad de un volumen para copiar archivos desde la copia de seguridad a un disco físico,
- eliminar de manera segura los archivos comprimidos y las copias de seguridad de los archivos comprimidos.

Para obtener más información acerca de las operaciones con bóvedas, consulte la sección Bóvedas (pág. 130).

### Aumento de Acronis Secure Zone

***Para aumentar Acronis Secure Zone***

1. En la página **Gestionar Acronis Secure Zone**, haga clic en **Aumentar**.
2. Seleccione los volúmenes que dispongan del espacio libre que se utilizará para aumentar Acronis Secure Zone.
3. Especifique el nuevo tamaño de la zona al:
   - arrastrar el deslizador y seleccionar cualquier tamaño entre los valores actuales y máximos. El máximo tamaño equivale al espacio no asignado del disco más el espacio libre total de las particiones seleccionadas;
   - escribir un valor exacto en el campo Tamaño de Acronis Secure Zone .

   Al aumentar el tamaño de la zona, el programa actuará de la siguiente manera:
   - en primer lugar, utilizará el espacio no asignado. De ser necesario, los volúmenes se moverán, pero no aumentarán su tamaño. Mover los volúmenes bloqueados requiere reiniciar el equipo.
   - Si no existe suficiente espacio no asignado, el programa obtendrá espacio libre de los volúmenes seleccionados, reduciendo proporcionalmente el tamaño de estos. Para modificar el tamaño de las particiones bloqueadas es necesario reiniciar el sistema.

   *Reducir el volumen del sistema al tamaño mínimo puede impedir el arranque del sistema operativo.*
4. Haga clic en **Aceptar**.

### Disminución de Acronis Secure Zone

***Para disminuir Acronis Secure Zone***

1. En la página **Gestión de Acronis Secure Zone**, haga clic en **Disminuir**.

2. Seleccione los volúmenes a los que se destinarán los espacios libres después de que se disminuya la zona.
3. Especifique el nuevo tamaño de la zona al:
   - arrastrar el deslizador y seleccionar cualquier tamaño entre los valores actuales y máximos. El tamaño mínimo es de aproximadamente 50 MB, de acuerdo con la geometría del disco duro;
   - escribir un valor exacto en el campo Tamaño de **Acronis Secure Zone.**
4. Haga clic en **Aceptar**.

### Eliminación de Acronis Secure Zone

***Para eliminar Acronis Secure Zone***

1. En la barra **Acciones de Acronis Secure Zone** (en el panel **Acciones y herramientas**), seleccione **Eliminar**.
2. En la ventana **Eliminar Acronis Secure Zone**, seleccione los volúmenes a los cuales quiere añadir el espacio liberado de la zona y haga clic en **Aceptar**.

   Si selecciona varios volúmenes, el espacio se distribuirá de manera proporcional para cada partición. Si no selecciona un volumen, el espacio liberado se convertirá en espacio no asignado.

Tras hacer clic en **Aceptar**, Acronis Backup & Recovery 10 comenzará a eliminar la zona.

## 6.9 Acronis Startup Recovery Manager

Acronis Startup Recovery Manager es una modificación del agente de arranque (pág. 401) que reside en el disco del sistema en Windows o en la partición /boot en Linux y está configurado para iniciarse en el tiempo de arranque al pulsar F11. Elimina la necesidad disponer de un dispositivo o conexión de red para ejecutar la utilidad de rescate de inicio.

#### Activar

Habilita el mensaje de tiempo de inicio "Pulse F11 para Acronis Startup Recovery Manager..." (si no tiene el cargador de inicio GRUB) o añade el elemento "Acronis Startup Recovery Manager" al menú de GRUB (si tiene GRUB). Si el sistema no arranca, podrá ejecutar la utilidad de rescate de inicio al pulsar F11 o al seleccionarlo en el menú, respectivamente.

*El disco del sistema (o la partición /boot en Linux) debe tener por lo menos 70 MB de espacio libre para activar Acronis Startup Recovery Manager.*

A menos que use el cargador de inicio GRUB y este esté instalado en el registro de inicio maestro (MBR), la activación de Acronis Startup Recovery Manager sobrescribirá el registro de inicio maestro con su propio código de inicio. Por lo tanto, necesitará activar nuevamente cargadores de inicio de terceros, si están instalados.

En Linux, cuando se utiliza un cargador de inicio que no sea GRUB (como LILO), considere instalarlo en un registro de inicio de partición de raíz (o inicio) de Linux en lugar de MBR antes de activar. De lo contrario, vuelva a configurar este cargador de inicio manualmente después de la activación.

### No activar

Deshabilita el mensaje de tiempo de inicio "Pulse F11 para Acronis Startup Recovery Manager..." (o el elemento del menú en GRUB). Si Acronis Startup Recovery Manager no está activado, necesitará realizar algunas de las siguientes acciones para recuperar el sistema cuando el arranque falle:

- arranque el equipo desde un dispositivo de rescate de arranque diferente
- realice el inicio de red desde Acronis PXE Server o Microsoft Remote Installation Services (RIS).

Consulte la sección Dispositivo de arranque (pág. 276) para obtener más información.

## 6.10 Dispositivo de arranque

### Dispositivo de arranque

Los dispositivos de arranque son un dispositivo físico (CD, DVD, unidad USB u otro dispositivo compatible con el BIOS de un equipo como dispositivo de arranque) que inicia en cualquier equipo compatible con PC y permite que ejecute el agente Acronis Backup & Recovery 10 tanto en un entorno basado en Linux como un entorno de preinstalación de Windows (WinPE), sin la ayuda de un sistema operativo. Los dispositivos de arranque se usan con frecuencia para:

- recuperar de un sistema operativo que no puede iniciar
- acceder a los datos que sobrevivieron en un sistema dañado y realizar copias de seguridad de éstos
- implementar un sistema operativo desde cero
- crear volúmenes básicos o dinámicos desde cero
- realizar copias de seguridad "sector por sector" de un disco con un sistema de archivos incompatible
- realizar copias de seguridad fuera de línea de cualquier dato que no se puede incluir en la copia de seguridad en línea por acceso restricto, con un bloqueo permanente por las aplicaciones en ejecución o por cualquier otra razón.

Se puede iniciar un equipo en los entornos anteriores, ya sea con los dispositivos físicos o desde la red con el servidor PXE de Acronis, Windows Deployment Services (WDS) o Servicios de Instalación Remota (RIS). Estos servidores con componentes de arranque cargados también puede considerarse un tipo de dispositivo de arranque. Puede crear dispositivos de arranque o configurar el servidor PXE o WDS/RIS con el mismo asistente.

### Dispositivo de arranque basado en Linux

Los dispositivos de arranque basados en Linux contienen el agente de arranque Acronis Backup & Recovery 10 basado en un núcleo Linux. El agente puede iniciar y realizar las operaciones en cualquier hardware compatible con PC, incluyendo desde cero y los equipo con sistemas de archivos corruptos o incompatibles. Se puede configurar y controlar las operaciones tanto a nivel local como remoto con la consola de administración.

### Dispositivo de arranque basado en PE

Los dispositivos de arranque basados en PE contienen un sistema Windows mínimo llamado Windows Preinstallation Environment (WinPE) y el complemento para WinPE de Acronis, es decir, una modificación del Agente de Acronis Backup & Recovery 10 que se puede ejecutar en el entorno de preinstalación.

Se comprobó que WinPE es la solución de arranque más conveniente en entornos grandes con hardware heterogéneo.

**Ventajas:**

- El uso de Acronis Backup & Recovery 10 con el entorno de preinstalación de Windows proporciona más funcionalidad que el uso de dispositivos de arranque basados en Linux. Como se inició un hardware compatible con PC en WinPE, no sólo puede utilizar el Agente de Acronis Backup & Recovery 10, sino también los comandos y secuencias de comando y otros complementos de PE que haya agregado.
- Los dispositivos de arranque basados en PE ayudan a superar los problemas de los dispositivos de arranque basados en Linux compatibles con ciertos controladores RAID de ciertos niveles de conjuntos de RAID solos. Los dispositivos basados en PE 2.x, es decir los núcleos de Windows Vista o Windows Server 2008, permiten la carga dinámica de controladores de dispositivos necesarios.

### 6.10.1 Cómo crear dispositivos de inicio

Para permitir la creación de los dispositivos físicos, el equipo debe tener una unidad grabadora de CD/DVD, o permitir que se conecte una unidad de memoria flash. Para habilitar la configuración de PXE o WDS/RIS, el equipo debe tener una conexión de red. El Generador de dispositivos de inicio también puede crear una imagen ISO de un disco de inicio para grabarla en un disco en blanco más tarde.

#### Dispositivos de inicio basados en Linux

Inicie el generador de dispositivos de inicio ya sea desde la consola de gestión seleccionando **Herramientas > Crear dispositivo de inicio** o como un componente separado.

Seleccione la manera en que los volúmenes y redes compartidas se manejarán (denominado estilo de los dispositivos).

- Un dispositivo con un manejo de volúmenes estilo Linux muestra los volúmenes como, por ejemplo, hda1 y sdb2. Intenta reconstruir los dispositivos MD y los volúmenes lógicos (LVM) antes de comenzar una recuperación.
- Un dispositivo con un manejo de volúmenes estilo Windows muestra los volúmenes como, por ejemplo, C: y D:. Proporciona acceso a los volúmenes dinámicos (LDM).

El asistente lo guiará a través de las operaciones. Para obtener más información, consulte Dispositivos de inicio basados en Linux (pág. 278).

#### Dispositivos de inicio basados en PE

Acronis Plug-in para WinPE puede añadirse a distribuciones de WinPE basadas en cualquiera de los siguientes kernel:

- Windows XP Professional con Service Pack 2 (PE 1.5)
- Windows Server 2003 con Service Pack 1 (PE 1.6)
- Windows Vista (PE 2.0)
- Windows Vista SP1 y Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0)

Si ya tiene dispositivos con la distribución PE1.x, extraiga el dispositivo ISO en una carpeta local e inicie el generador de dispositivos de inicio ya sea desde la consola de gestión seleccionando **Herramientas > Crear dispositivo de inicio** o como un componente separado. El asistente lo guiará a

través de las operaciones. Consulte Agregar el Acronis Plug-in a WinPE 1.x (pág. 283) para obtener más detalles.

Para poder crear o modificar las imágenes de PE 2.x o 3.0, instale el generador de dispositivos de inicio en un equipo en el que esté instalado el Windows Automated Installation Kit (AIK). Las demás operaciones se describen en la sección Agregar Acronis Plug-in para WinPE 2.x o 3.0 (pág. 283).

Si no tiene un equipo con WAIK, prepárelo de la siguiente manera:

1. Descargue e instale Windows Automated Installation Kit (WAIK).

   Automated Installation Kit (AIK) para Windows Vista (PE 2.0):

   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=es

   Automated Installation Kit (AIK) para Windows Vista SP1 y Windows Server 2008 (PE 2.1):

   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=es

   Automated Installation Kit (AIK) para Windows 7 (PE 3.0):

   http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=es

   Puede encontrar los requisitos del sistema para la instalación en los siguientes enlaces.
2. [opcional] Grabe el WAIK en un DVD o cópielo en una unidad de memoria flash.
3. Instale Microsoft .NET Framework v.2.0 desde este kit (NETFXx86 o NETFXx64, según su hardware)
4. Instale Microsoft Core XML (MSXML) 5.0 o 6.0 Parser de este kit.
5. Instale Windows AIK de este kit.
6. Instale el generador de dispositivos de inicio en el mismo equipo.

Se recomienda que se familiarice con la documentación de ayuda suministrada con Windows AIK. Para acceder a la documentación, seleccione del menú de inicio **Microsoft Windows AIK -> Documentación**.

### Uso de Bart PE

Puede crear una imagen Bart PE con Acronis Plug-in usando el builder de Bart PE. Consulte Creación de Bart PE con el componente Acronis de distribución de Windows (pág. 284)para obtener más detalles.

## Medios de inicio basados en Linux

***Cuando use el generador de dispositivos, debe especificar:***

1. [opcional] Los parámetros del kernel de Linux. Separe los diferentes parámetros con espacios.

   Por ejemplo, para poder seleccionar un modo de visualización para el agente de inicio cada vez que se inicia el dispositivo, escriba: **vga=ask**

   Para obtener una lista de parámetros, consulte Parámetros del kernel (pág. 279).
2. Los componentes de arranque de Acronis se ubicarán en el dispositivo.
   - Se puede habilitar Universal Restore de Acronis Backup & Recovery 10 si se instaló Universal Restore en el equipo donde se creó el dispositivo.
3. [opcional] El intervalo de tiempo de espera para el menú de inicio además del componente que se iniciará automáticamente en el tiempo de espera.
   - Si no se configura, el cargador de Acronis espera que alguien seleccione si iniciar desde el sistema operativo (de estar presente) o desde el componente de Acronis.

- Si configura, por ejemplo, **10 seg** para el agente de inicio, el agente se iniciará 10 segundos después de que se muestre el menú. Esto permite la operación desatendida del sitio cuando inicie desde un servidor PXE o WDS/RIS.

4. [opcional] Configuraciones de inicio de sesión remota:
   - el nombre de usuario y contraseña que se ingresarán del lado de la consola cuando se conecte con el agente. Si deja estos campos en blanco, se habilitará la conexión para ingresar cualquier símbolo en la ventana de línea de comandos.
5. [opcional] Configuración de red (pág. 281):
   - La configuración TCP/IP que será asignada a los adaptadores de red del equipo.
6. [opcional] Puerto del red (pág. 282):
   - el puerto TCP que el agente de inicio escucha para las conexiones entrantes.
7. El tipo de dispositivo que desea crear. Puede:
   - crear CD, DVD u otros dispositivos de arranque como una unidad de memoria flash USB si la BIOS del hardware permite el inicio desde tal dispositivo
   - crear una imagen ISO de un disco de arranque para grabar más tarde en un disco en blanco
   - cargar los componentes seleccionados en el servidor PXE de Acronis
   - cargar los componentes seleccionados A WDS/RIS.
8. [opcional] los controladores del sistema Windows que usará Universal Restore de Acronis (pág. 282). La ventana aparece sólo si está instalado el complemento para Universal Restore de Acronis y si selecciona otro dispositivo que no sea PXE o WDS/RIS.
9. La ruta del archivo ISO o el nombre o dirección IP y las credenciales para PXE o WDS/RIS.

## Parámetros de kernel

Esta ventana le permite especificar uno o más parámetros del kernel de Linux. Se aplicarán automáticamente cuando se ejecute el dispositivo de arranque.

Estos parámetros se utilizan comúnmente cuando hay problemas mientras se trabaja con el dispositivo de arranque. Normalmente, puede dejar este campo vacío.

También puede especificar cualquiera de estos parámetros pulsando F11 mientras está en el menú de inicio.

### Parámetros

Cuando especifique varios parámetros, sepárelos con espacios.

**acpi=desactivada**

Desactiva la interfaz de alimentación de configuración avanzada (ACPI). Puede utilizar este parámetro cuando experimente problemas con la configuración de un hardware en particular.

**noapic**

Desactiva el Controlador de interrupciones programable avanzado (APIC). Puede utilizar este parámetro cuando experimente problemas con la configuración de un hardware en particular.

**vga=ask**

Solicita que seleccione el modo de video que utilizará la interfaz gráfica de usuario del dispositivo de arranque. Sin el parámetro **vga**, el modo vídeo se detecta automáticamente.

**vga=***mode_number*

Especifica el modo de video que utilizará la interfaz gráfica de usuario del dispositivo de arranque. El número de modo aparece en *mode_number* en formato hexadecimal, por ejemplo: **vga=0x318**

La resolución de la pantalla y el número de colores correspondiente a un número de modo puede ser diferente en equipos diferentes. Recomendamos utilizar primero el parámetro **vga=ask** para seleccionar un valor para *mode_number*.

**silencio**

Desactiva la muestra de mensajes de inicio cuando el kernel de Linux se está cargando y ejecuta la consola de gestión una vez que el kernel está cargado.

Este parámetro está especificado implícitamente cuando crea el dispositivo de arranque, pero puede borrar este parámetro mientras esté en el menú de inicio.

Sin este parámetro, se mostrarán todos los mensajes de inicio, seguidos de una entrada de comandos. Para iniciar la consola de gestión desde la entrada de comandos, ejecute el comando: **/bin/product**

**nousb**

Desactiva la carga del subsistema del USB (bus universal en serie).

**nousb2**

Desactiva la compatibilidad con USB 2.0. No obstante, los dispositivos USB 1.1 trabajan con este parámetro. Este parámetro le permite utilizar algunas unidades USB en el modo USB 1.1 si no funcionan en el modo USB 2.0.

**nodma**

Desactiva el acceso directo a memoria (DMA) para todas las unidades del disco duro IDE. Evita que el kernel se congele en algún hardware.

**nofw**

Desactiva la compatibilidad con la interfaz de FireWire (IEEE1394).

**nopcmcia**

Desactiva la detección del hardware PCMCIA.

**nomouse**

Desactiva la compatibilidad con el ratón.

*module_name*=**desactivado**

Desactiva el módulo cuyo nombre aparece en *module_name*. Por ejemplo, para desactivar el uso del módulo SATA, especifique: **sata_sis=desactivado**

**pci=bios**

Obliga al uso de PCI BIOS en vez de acceder directamente al dispositivo del hardware. Es conveniente que utilice este parámetro si el equipo tiene un puente PCI no estándar de host.

**pci=nobios**

Desactiva el uso de PCI BIOS; solo se pueden utilizar métodos de acceso directo al hardware. Es conveniente que utilice este parámetro cuando el dispositivo de arranque no puede iniciarse, lo que puede deberse a la BIOS.

**pci=biosirq**

Utiliza las alertas PCI BIOS para obtener la tabla de rutas de interrupción. Es conveniente que utilice este parámetro si el kernel no puede asignar solicitudes de interrupción (IRQ) o descubrir enlaces secundarios de PCI en la placa madre.

Estas llamadas pueden no funcionar correctamente en algunos equipos. Pero puede ser la única manera de obtener la tabla de rutas de interrupción.

## Configuraciones de red

Mientras crea el dispositivo de arranque Acronis, usted tiene la opción de preconfigurar las conexiones de red que serán usadas por el agente de inicio. Se pueden preconfigurar los siguientes parámetros:

- Dirección IP
- Máscara de subred
- Puertas de enlace
- Servidor DNS
- Servidor WINS.

Una vez que se inicia el agente de arranque en un equipo, se aplica la configuración en la tarjeta de interfaz de red (NIC) del equipo. Si no se preconfiguran las configuraciones, el agente usa la configuración automática del servidor DHCP. También tienen la capacidad de establecer manualmente la configuración de red cuando se ejecuta el agente de inicio en el equipo.

### Preconfiguración de múltiples conexiones de red

Puede preestablecer la configuración TCP/IP de hasta 10 tarjetas de interfaz de red. Para asegurar que cada NIC tendrá asignada la configuración adecuada, cree el dispositivo en el servidor en donde se personalizan los dispositivos. Cuando seleccione la NIC existente en al agente de Windows, se selecciona su configuración para guardarlos en el dispositivo. También se guarda la dirección MAC de cada NIC en los dispositivos.

Puede cambiar la configuración, excepto por la dirección MAC, o establecer la configuración para una NIC no existente, de ser necesario.

Una vez que el dispositivo de inicio se ejecute en el servidor, recupera la lista de NIC disponibles. Esta lista está ordenada por las ranuras que ocupan las NIC, las más cercanas al procesador están en la parte superior.

El agente de inicio asigna la configuración apropiada a cada NIC conocida y las identifica por sus direcciones MAC. Después de que se configuran las NIC con direcciones MAC conocidas, se asigna la configuración que realizó para NIC no existentes a las NIC restantes, comenzando por la NIC no asignada superior.

Puede personalizar los dispositivos de arranque para cualquier equipo, y no sólo para el equipo en donde se crea el dispositivo. Para hacerlo, configure las NIC de acuerdo con el orden de ranuras del equipo. Nic1 ocupa la ranura más cercana al procesador, NIC2 es la siguiente ranura. Cuando el agente de inicio se ejecuta en el equipo, no encontrará NIC con direcciones MAC conocidas y configurará las NIC en el mismo orden que usted.

**Ejemplo**

El agente de arranque podría usar uno de los adaptadores de red para la comunicación con la consola de administración por medio de la red de producción. Se podría establecer la configuración

automática para esta conexión. Se pueden transferir los datos que se pueden dividir para su recuperación por la segunda NIC, incluida en la red de copia de seguridad por medio de la configuración TCP/IP.

## Puerto de red

Cuando cree dispositivos de arranque, tiene la opción de preconfigurar el puerto de red que el agente de inicio escuchará para la conexión entrante. La opción disponible entre:

- el puerto predeterminado
- el puerto usado actualmente
- el puerto nuevo (ingrese el número de puerto)

Si no se preconfiguró el puerto, el agente usa el número de puerto predeterminado (9876.) Este puerto que se usa predeterminado por la consola de administración de Acronis Backup & Recovery 10. La configuración temporal del puerto está disponible. Mientras se conecta la consola al agente, especifique el puerto para dicha sesión en la dirección URL <Agent-IP>:<port>.

## Controladores para Universal Restore

Cuando crea dispositivos de arranque, tiene la opción de agregar controladores para Windows al dispositivo. Se usarán los controladores para Universal Restore cuando se recupera Windows en un equipo con un procesador diferente, placa madre diferente o dispositivo de almacenamiento masivo diferente de los que se utilizan en el sistema del que se realizó la copia de seguridad.

Entonces podrá configurar Universal Restore:

- para buscar los controladores en los dispositivos que mejor se ajustan con el hardware de destino.
- para obtener los controladores de almacenamiento masivo que especifica desde el dispositivo. Esto debe hacerse cuando el hardware de destino tiene el controlador para almacenamiento masivo (como adaptador SCSI, RAID, o Fiber Channel) para el disco duro.

Para obtener más información, consulte Universal Restore (pág. 248).

Los controladores serán ubicados en la carpeta de controladores visibles en el dispositivo de arranque. No se cargan los controladores en la memoria RAM del equipo de destino, el dispositivo debe estar insertado o conectado por medio de la operación de Universal Restore.

Puede agregar controladores a un dispositivo de arranque, siempre que:

1. El complemento para Universal Restore de Acronis Backup & Recovery 10 esté instalado en el equipo en donde se crea el dispositivo de arranque
2. Cree un dispositivo extraíble o su ISO o medio extraíble, como una unidad de memoria flash. Los controladores se pueden cargar en el servidor PXE o WDS/RIS.

Se pueden agregar los controladores a la lista sólo en grupos, al agregar los archivos INF o carpetas que contienen dichos archivos. La selección de controladores individuales desde los archivos INF no es posible, pero el generador de dispositivos muestra el contenido del archivo para su información.

***Para agregar unidades:***

1. Haga clic en **Agregar** y navegue hasta el archivo INF o la carpeta que contiene los archivos INF.
2. Seleccione el archivo INF o la carpeta.
3. Haga clic en **Aceptar**.

Se pueden eliminar los controladores de la lista sólo en grupos, al eliminar los archivos INF.

***Para eliminar los controladores:***

1. Seleccione el archivo INF.
2. Haga clic en **Remover**.

## Adición del complemento de Acronis a WinPE 1.x

Se puede agregar el complemento de Acronis para WinPE a:

- Windows PE 2004 (1.5) (Windows XP Professional con Service Pack 2)
- Windows PE 2005 (1.6) (Windows XP Professional con Service Pack 1)

***Para agregar el complemento de Acronis a WinPE 1.x:***

1. Extraiga todos los archivos de su WinPE 1.x ISO para separar la carpeta en el disco duro.
2. Inicie el generador de dispositivos de inicio ya sea desde la consola de gestión seleccionando **Herramientas > Crear dispositivo de inicio** o como un componente separado.
3. Seleccione **Tipo de dispositivo de inicio**: **Windows PE**:
   - Seleccione **Utilizar los archivos WinPE ubicados en la carpeta que especifique**.
4. Especifique la ruta a la carpeta donde están ubicados los archivos de WinPE.
5. Especifique las configuraciones de red (pág. 281) de los adaptadores de red del equipo o elija la configuración automática DHCP.
6. Especifique la ruta completa al archivo ISO resultante incluyendo el nombre de archivo.
7. Compruebe su configuración en la pantalla de resumen y haga clic en **Continuar**.
8. Grabe el .ISO en un CD o DVD con una herramienta de otra empresa o cópielo en una unidad de memoria flash.

Una vez que el equipo se inicia en WinPE, Acronis Backup & Recovery 10 inicia automáticamente.

## Adición del complemento de Acronis a WinPE 2.x o 3.0

El generador de dispositivo de inicio proporciona tres métodos para integrar Acronis Backup & Recovery 10 con WinPE 2.x o 3.0:

- Adición del complemento de Acronis al PE ISO existente. Esto es útil cuando tiene que añadir el complemento al PE ISO previamente configurado que ya está en uso.
- Creación del PE ISO con el complemento desde cero.
- Adición del complemento de Acronis a un archivo WIM para cualquier propósito (creación manual de imagen ISO, adición de otras herramientas a la imagen y demás).

Para poder realizar cualquiera de las operaciones anteriores, instale el generador de dispositivos de inicio en un equipo donde se haya instalado Windows Automated Installation Kit (WAIK). Si no tiene dicho equipo, prepare tal como se describe en Cómo crear dispositivos de inicio (pág. 277).

---

*El generador de dispositivos de inicio solo es compatible con x86 WinPE 2.x o 3.0. Estas distribuciones de WnPE también pueden funcionar con hardware x64.*

*Una imagen PE basada en Win PE 2.0 necesita al menos 256 MB de RAM para funcionar. El tamaño de memoria recomendado para PE 2.0 es 512 MB. Una imagen PE basada en Win PE 3.0 necesita al menos 512 MB de RAM para funcionar.*

---

### Adición del complemento de Acronis a WinPE 2.x o 3.0 ISO

***Para agregar el complemento de Acronis a WinPE 2.x o 3.0 ISO:***

1. Cuando añada el complemento al Win PE ISO existente, extraiga todos los archivos de su Win ISO en una carpeta separada de su disco duro.
2. Inicie el generador de dispositivos de inicio ya sea desde la consola de gestión seleccionando **Herramientas > Crear dispositivo de inicio** o como un componente separado.
3. Seleccione **Tipo de dispositivo de inicio**: **Windows PE**:

   Cuando cree un nuevo PE ISO:

   - Seleccione **Crear Windows PE 2.x o 3.0 automáticamente**
   - El software ejecuta la secuencia de comandos apropiada y continúa a la siguiente ventana.

   Cuando añada el complemento al PE ISO existente:

   - Seleccione **Utilizar los archivos WinPE ubicados en la carpeta que especifique**.
   - Especifique la ruta a la carpeta donde están ubicados los archivos de WinPE.
4. Especifique las configuraciones de red (pág. 281) de los adaptadores de red del equipo o elija la configuración automática DHCP.
5. [opcional] Especifique los controladores de Windows que se deben añadir a Windows PE. Cuando haya iniciado su equipo en Windows PE, los controladores le ayudarán a acceder al dispositivo donde está ubicado el archivo de copia de seguridad. Haga clic en **Añadir** y especifique la ruta al archivo *.inf necesario para el correspondiente controlador SCSI, RAID o SATA, adaptador de red, unidad de cinta u otro dispositivo. Tendrá que repetir este procedimiento para cada controlador que desee incluir en el dispositivo de inicio WinPE resultante.
6. Elija si desea crear una imagen ISO o WIM o cargar el dispositivo a Acronis PXE Server.
7. Especifique la ruta completa al archivo de imagen que se obtendrá incluyendo el nombre del archivo o especifique el servidor PXE y proporcione el nombre de usuario y la contraseña para acceder a él.
8. Compruebe su configuración en la pantalla de resumen y haga clic en **Continuar**.
9. Grabe el .ISO en un CD o DVD con una herramienta de otra empresa o cópielo en una unidad de memoria flash.

Una vez que el equipo se inicia en WinPE, Acronis Backup & Recovery 10 lo hace automáticamente.

***Para crear una imagen PE (archivo ISO) del archivo WIM resultante:***

- Reemplace el archivo boot.wim predeterminado en su carpeta de Windows PE junto al archivo WIM creado recientemente. Para el ejemplo anterior, escriba:

  ```
  copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
  ```

- Use la herramienta **Oscdimg**. Para el ejemplo anterior, escriba:

  ```
  oscdimg -n –bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO
  c:\winpe_x86\winpe_x86.iso
  ```

Para obtener más información sobre como personalizar Windows PE, consulte la guía del usuario de entorno de preinstalación de Windows (Winpe.chm).

## Creación de Bart PE con el complemento de Acronis desde la distribución de Windows

1. Obtenga Bart PE builder.
2. Instale el generador de dispositivo de inicio desde el archivo de instalación de Acronis Backup & Recovery 10.

3. Cambie la carpeta actual a la carpeta donde está instalado el complemento de Acronis para WinPE de manera predeterminada: C:\Archivos de programa\Acronis\Bootable Components\WinPE.

   Si el complemento está instalado en una carpeta que no es la predeterminada, cambie la ruta según corresponda (compruebe la clave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Bootable Components\Settings\WinPE para conocer la ubicación del complemento).
4. Extraiga el archivo WinPE.zip en la carpeta actual.
5. Ejecute el siguiente comando:

   ```
   export_license.bat
   ```
6. Copie el contenido de la carpeta actual, de manera predeterminada: C:\Archivos de programa\Acronis\Bootable Components\WinPE—a %BartPE folder%\plugins\Acronis.
7. Inserte el CD de la distribución de Windows si no tiene una copia de los archivos de instalación de Windows en el HDD.
8. Inicie Bart PE builder.
9. Especifique la ruta de la instalación de Windows o el CD con la distribución de Windows.
10. Haga clic en **Complementos** y compruebe si el complemento de Acronis Backup & Recovery 10 está habilitado. Habilítelos sin están deshabilitados.
11. Especifique la carpeta de salida y la ruta completa del archivo ISO resultante, incluidos el nombre de archivo o el dispositivo que desea crear.
12. Cree Bart PE.
13. Grabe la imagen ISO a un CD o DVD (si no se ha hecho ya) o copie el archivo a la unidad flash.

Una vez que el equipo inicia en Bart PE y usted configura la conexión de red, seleccione **Ir a -> Sistema -> Almacenamiento -> Acronis Backup & Recovery 10** para iniciar.

### 6.10.2 Conexión a un equipo que se inició desde un dispositivo

Una vez que un equipo inicia desde un dispositivo de inicio, la terminal del equipo muestra una ventana de inicio con la dirección IP que el servidor DHCP proporcionó o la establecida de acuerdo a los valores preconfigurados.

**Conexión remota**

Para conectar el equipo remotamente, seleccione **Conectar -> Administración de un equipo remoto** en la consola de menú y especifique una de las direcciones IP del equipo. Proporcione el nombre de usuario y contraseña si se establecieron cuando se creó el dispositivo de arranque.

**Conexión Local**

La consola de administración Acronis Backup & Recovery 10 está siempre presente en el dispositivo de arranque. Cualquiera que tenga acceso físico a la terminal del equipo puede ejecutar la consola y conectarse. Sólo haga clic en **Ejecutar la Consola de administración** en la ventana de inicio del agente de arranque.

### 6.10.3 Trabajo desde dispositivo de arranque

Las operaciones que se realizan en equipos que iniciaron desde dispositivo de arranque son muy parecidas a las copias de seguridad y la recuperación en el sistema operativo. La diferencia es la siguiente:

1. Las letras de los discos que se ven en los dispositivos de inicio de estilo Windows pueden diferir de la manera en que Windows identifica las unidades. Por ejemplo, la unidad D: en la utilidad de rescate puede corresponder a la unidad E: de Windows.

   *¡Tenga cuidado! Para estar seguro, se aconseja asignar nombres únicos a los volúmenes.*

2. Los dispositivos de inicio de estilo Linux muestran los discos y volúmenes locales como desmontados (sda1, sda2...).
3. El dispositivo de arranque de estilo Linux no puede realizar copias de seguridad en un volumen formateado con NTFS. Si es necesario, cambie al estilo de Windows.
4. Puede cambiar el dispositivo de arranque entre el estilo de Windows y el de Linux al seleccionar **Herramientas** > **Cambiar la representación del volumen**.
5. Los medios de GUI no tienen un árbol de **Navegación**. Use el menú de **Navegación** para navegar entre las vistas.
6. No se pueden programar las tareas; de hecho, tampoco se pueden crear las tareas. Si necesita repetir la operación, configúrela desde cero.
7. La vida útil del registro se limita a la sesión actual. Puede guardar todo el registro o las entradas del registro filtradas a en un archivo.
8. Las bóvedas centralizadas no se muestran en el árbol de carpetas de la ventana de **Archivos**.

   Para acceder a una bóveda gestionada, escriba la siguiente cadena en el campo de **Ruta**:

   **bsp://dirección_nodo/nombre_bóveda/**

   Para acceder a una bóveda centralizada sin gestionar, escriba la ruta completa de la carpeta de la bóveda.

   Después de introducir las credenciales de acceso, verá una lista de los archivos comprimidos que se encuentran en la bóveda.

## Configuración del modo de visualización

Para un equipo que se inicia desde un dispositivo, se detecta automáticamente un modo de vídeo de visualización basado en la configuración del hardware (especificaciones de la tarjeta del monitor y de los gráficos). Si, por alguna razón, el modo vídeo se detecta de manera incorrecta, realice lo siguiente:

1. Pulse F11 en el menú de inicio.
2. Añada el siguiente comando en la entrada de comandos: **vga=ask** y prosiga con el arranque.
3. En la lista de modos de vídeo compatibles, escoja el correcto al escribir su número (por ejemplo, **318**) y pulse INTRO.

Si no desea seguir este procedimiento cada vez que inicie desde un dispositivo en una configuración de hardware en concreto, cree de nuevo el dispositivo de arranque con el número de modo apropiado (en nuestro ejemplo, **vga=0x318**) escrito en la ventana **Parámetros del kernel** (consulte la sección Generador de dispositivos de arranque (pág. 278) para obtener más detalles).

## Configuración de los dispositivos iSCSI y NDAS

Esta sección describe cómo configurar los dispositivos de la Internet Small Computer System Interface (iSCSI) y los de Network Direct Attached Storage (NDAS) mientras trabaja desde un dispositivo de arranque.

Estos dispositivos están conectados al equipo a través de una interfaz de red y aparecen como si fueran dispositivos asociados localmente. En la red, un dispositivo iSCSI se identifica mediante su dirección IP y un dispositivo NDAS mediante el ID del dispositivo.

Un dispositivo iSCSI a veces se denomina un objetivo iSCSI. Un componente hardware o software que proporciona interacción entre el equipo y el objetivo iSCSI se denomina un iniciador iSCSI. El nombre del iniciador iSCSI generalmente está definido por un administrador del servidor que aloja el dispositivo.

***Para añadir un dispositivo iSCSI***

1. En un dispositivo de arranque (basado en Linux o basado en PE), ejecute la consola de gestión.
2. Haga clic en **Configurar dispositivos iSCSI/NDAS** (en un medio basado en Linux) o **Ejecutar la configuración iSCSI** (en un medio basado en PE).
3. Especifique la dirección de IP y el puerto del servidor del dispositivo iSCSI y el nombre del iniciador iSCSI.
4. Si el servidor requiere autenticación, especifique el nombre de usuario y contraseña para el mismo.
5. Haga clic en **Aceptar**.
6. Seleccione el dispositivo iSCSI de la lista y después haga clic en **Conectar**.
7. Si se le solicita, especifique el nombre de usuario y la contraseña para acceder al dispositivo iSCSI.

***Para añadir un dispositivo NDAS***

1. En un dispositivo de arranque basado en Linux, ejecute la consola de gestión.
2. Haga clic en **Configurar dispositivos iSCSI/NDAS**.
3. En **Dispositivos NDAS**, haga clic en **Añadir dispositivo**.
4. Especifique el ID de 20 caracteres del dispositivo.
5. Para desea permitir datos de escritura en el dispositivo, especifique la clave de escritura de cinco caracteres. Sin esta clave, el dispositivo solo estará disponible en el modo de solo lectura.
6. Haga clic en **Aceptar**.

### 6.10.4 Lista de comandos y utilidades disponibles en los dispositivos de inicio basados en Linux

Los dispositivos de inicio basados en Linux contienen los siguientes comandos y utilidades de línea de comandos, que puede usar cuando se ejecuta un shell de comando. Para comenzar el shell de comandos, pulse CTRL+ALT+F2 mientras esté en la consola de gestión del dispositivo de inicio.

**Utilidades de línea de comandos Acronis**

- `acronis`
- `asamba`
- `lash`
- `restoreraids`
- `trueimagecmd`
- `trueimagemnt`

**Comandos y utilidades de Linux**

| | | |
|---|---|---|
| `busybox` | `ifconfig` | `rm` |
| `cat` | `init` | `rmmod` |
| `cdrecord` | `insmod` | `route` |

```
chmod      iscsiadm    scp
chown      kill        scsi_id
chroot     kpartx      sed
cp         ln          sg_map26
dd         ls          sh
df         lspci       apagar
dmesg      lvm         ssh
dmraid     mdadm       sshd
e2fsck     mkdir       strace
e2label    mke2fs      swapoff
echo       mknod       swapon
egrep      mkswap      sysinfo
fdisk      more        tar
fsck       montar      tune2fs
fxload     mtx         udev
gawk       mv          udevinfo
gpm        pccardctl   udevstart
grep       ping        umount
growisofs  pktsetup    uuidgen
grub       poweroff    vconfig
gunzip     ps          vi
halt       raidautorun zcat
hexdump    readcd
hotplug    reiniciar
```

### 6.10.5 Recuperación de los dispositivos MD y los volúmenes lógicos

Para recuperar los dispositivos MD, conocidos como Linux Software RAID, y/o dispositivos creados por el Administrador de volúmenes lógicos (LVM), conocidos como volúmenes lógicos, necesita crear la estructura del volumen correspondiente antes de comenzar la recuperación.

Puede crear la estructura del volumen de una de las siguientes maneras:

- Automáticamente, en dispositivos de arranque basados en Linux, utilizando la consola de gestión o una secuencia de comandos; consulte Creación de la estructura del volumen automáticamente (pág. 289).

- Manualmente utilizando las utilidades **mdadm** y **lvm** . Vea Creación de la estructura de volumen de forma manual (pág. 289).

## Creación de la estructura del volumen automáticamente

Asumamos que usted ha guardado la estructura de volumen en el directorio /etc/Acronis y que el volumen para este directorio está incluido en el archivo comprimido.

Para recrear la estructura del volumen en el dispositivo de arranque basado en Linux, utilice cualquiera de los métodos que se describen abajo.

***Precaución:*** *Como resultado de los siguientes procedimientos, la estructura actual del volumen en el equipo se cambiará por una almacenada en el archivo comprimido. Esto destruirá los datos que se encuentran almacenados actualmente en alguno o todos los discos duros del equipo.*

**Si ha cambiado la configuración del disco.** Un dispositivo MD o volumen lógico reside en uno o más discos, cada uno con un tamaño propio. Si entre la realización de la copia de seguridad y la recuperación cambió cualquiera de estos discos o si está recuperando los volúmenes en equipos diferentes, asegúrese de que la configuración del disco nuevo incluye por lo menos una cantidad de discos de tamaños iguales a los de los originales.

### *Para crear la estructura del volumen utilizando la consola de gestión*

1. Inicie el equipo desde una dispositivo de arranque basado en Linux.
2. Haga clic en **Acronis Bootable Agent**. Luego, haga clic en **Ejecutar la consola de administración**.
3. En la consola de gestión, haga clic en **Recuperar**.

   Bajo los contenidos del archivo comprimido, Acronis Backup & Recovery 10 mostrará un mensaje indicando que ha detectado información sobre la estructura del volumen.
4. Haga clic en **Detalles** en el área en la que se encuentra ese mensaje.
5. Revise la estructura del volumen y luego haga clic en **Aplicar RAID/LVM** para crearla.

### *Creación de la estructura del volumen con una secuencia de comandos*

1. Inicie el equipo desde una dispositivo de arranque basado en Linux.
2. Haga clic en **Acronis Bootable Agent**. Luego, haga clic en **Ejecutar la consola de administración**.
3. En la barra de herramientas, haga clic en **Acciones** y luego haga clic en **Ejecutar shell**. O bien, puede pulsar CTRL+ALT+F2.
4. Ejecute la secuencia de comandos **restoreraids.sh**, especificando el nombre completo del archivo, por ejemplo:

   ```
   /bin/restoreraids.sh
   smb://server/backups/linux_machine_2010_01_02_12_00_00_123D.tib
   ```
5. Vuelva a la consola de administración presionando CTRL+ALT+F1, o ejecutando el comando: **/bin/product**
6. Haga clic en **Recuperar**, luego especifique la ruta al archivo comprimido y otros parámetros necesarios, y luego haga clic en **Aceptar.**

Si Acronis Backup & Recovery 10 no crease la estructura del volumen (o si no está presente en el archivo comprimido), cree la estructura de forma manual.

## Creación de la estructura del volumen manualmente

A continuación se brinda un procedimiento general para la recuperación de dispositivos MD y volúmenes lógicos utilizando los dispositivos de arranque basados en Linux y un ejemplo de dicha recuperación. Puede utilizar un procedimiento parecido en Linux.

***Para recuperar dispositivos MD y volúmenes lógicos.***

1. Inicie el equipo desde una dispositivo de arranque basado en Linux.
2. Haga clic en **Acronis Bootable Agent**. Luego, haga clic en **Ejecutar la consola de administración**.
3. En la barra de herramientas, haga clic en **Acciones** y luego haga clic en **Ejecutar shell**. O bien, puede pulsar CTRL+ALT+F2.
4. De ser necesario, examine la estructura de volúmenes almacenados en el archivo comprimido, mediante la utilidad **trueimagecmd**. Además, puede usar la utilidad **trueimagemnt** para montar uno o más de estos volúmenes como si fueran volúmenes comunes (consulte "Montaje de volúmenes de copia de seguridad" que se desarrolla a continuación dentro de este tema).
5. Cree la estructura del volumen de acuerdo con el archivo comprimido, mediante la utilidad **mdadm** (para los dispositivos MD), la utilidad **lvm** (para volúmenes lógicos) o ambas.

   ***Nota:*** *Las utilidades frl Administrador de volúmenes lógico como* ***pvcreate*** *y* ***vgcreate****, que suelen estar disponibles en Linux, no están incluidas en el entorno de los dispositivos de inicio, por lo que necesita usar la utilidad* ***lvm*** *con un comando correspondiente:* ***lvm pvcreate****,* ***lvm vgcreate****, etc.*

6. Si montó previamente la copia de seguridad con la utilidad **trueimagemnt**, use esta utilidad de nuevo para desmontar la copia de seguridad (consulte "Montaje de volúmenes de copias de seguridad", más adelante).
7. Vuelva a la consola de administración presionando CTRL+ALT+F1, o ejecutando el comando: **/bin/product**

   (No reinicie el equipo en este momento. De otro modo, tendrá que crear la estructura del volumen de nuevo).
8. Haga clic en **Recuperar**, luego especifique la ruta al archivo comprimido y otros parámetros necesarios, y luego haga clic en **Aceptar.**

***Nota:*** *Este procedimiento no funciona cuando se conecta remotamente a Acronis Backup & Recovery 10 Bootable Agent porque el shell del comando no está disponible en este caso.*

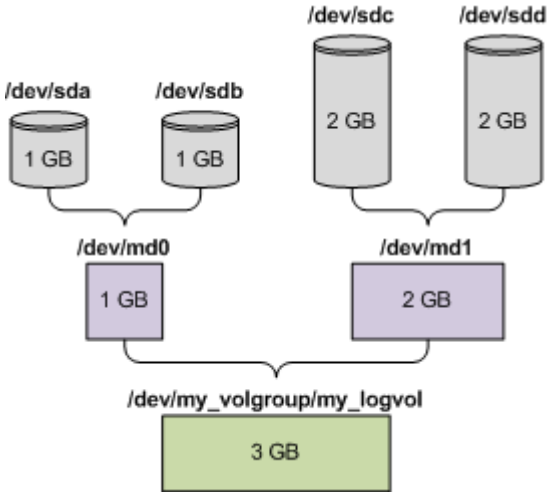
## Ejemplo

Suponga que se realiza previamente una copia de seguridad del disco de un equipo con la siguiente configuración de disco:

- El equipo tiene dos discos duros SCSI: uno de 1 gigabyte y otro de 2 gigabytes, montados en **/dev/sda**, **/dev/sdb**, **/dev/sdc**, y **/dev/sdd,** respectivamente.
- El primer y el segundo par de discos duros están configurados como dos dispositivos MD, ambos en la configuración RAID-1, y están montados en **/dev/md0** y **/dev/md1**, respectivamente.
- Un volumen lógico está basado en dos dispositivos MD y está montado en **/dev/my_volgroup/my_logvol**.

La siguiente imagen ilustra esta configuración.




Haga lo siguiente para recuperar datos del archivo comprimido.

**Paso 1: Creación de la estructura del volumen**

1. Inicie el equipo desde una dispositivo de arranque basado en Linux.
2. En la consola de administración, presione CTRL+ALT+F2.
3. Ejecute los siguientes comandos para crear los dispositivos MD:

   ```
   mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sd[ab]
   mdadm --create /dev/md1 --level=1 --raid-devices=2 /dev/sd[cd]
   ```

4. Ejecute los siguientes comandos para crear el volumen lógico del grupo:

   ***Precaución:*** *El comando* ***pvcreate*** *destruye todos los datos en los dispositivos* ***/dev/md0*** *y* ***/dev/md1****.*

   ```
   lvm pvcreate /dev/md0 /dev/md1
   lvm vgcreate my_volgroup /dev/md0 /dev/md1
   lvm vgdisplay
   ```

   La salida del comando **lvm vgdisplay** será similar a:

   ```
   --- Volume group ---
   VG Name     my_volgroup
   ...
   VG Access   read/write
   VG Status   resizable
   ...
   VG Size     1.99 GB
   ...
   VG UUID     0qoQ4l-Vk7W-yDG3-uF1l-Q2AL-C0z0-vMeACu
   ```

5. Ejecute el siguiente comando para crear el volumen lógico, en el parámetro**-L**, y especifique el tamaño dado por **VG Size**:

   ```
   lvm lvcreate -L1.99G --name my_logvol my_volgroup
   ```

6. Active el volumen del grupo al ejecutar el siguiente comando:

   ```
   lvm vgchange -a y my_volgroup
   ```

7. Presione CTRL+ALT+F1 para volver a la consola de administración.

**Paso 2: Comienzo de la recuperación**

1. En la consola de gestión, haga clic en **Recuperar**.

2. En **Archivo comprimido**, haga clic en **Cambio** y luego especifique el nombre del archivo comprimido.
3. En **Copia de Seguridad**, haga clic en **Cambio** y luego selecciones la copia de seguridad de la que quiere recuperar datos.
4. En los **tipos de datos**, seleccione **Volúmene**s.
5. En **Elementos a recuperar**, seleccione la casilla de verificación que se encuentra junto a **my_volgroup-my_logvol**.
6. En **Dónde recuperar,** haga clic en **Cambio** y luego seleccione el volumen lógico que creó en el Paso 1. Haga clic en los botones para expandir la lista de discos.
7. Haga clic en **Aceptar** para comenzar la recuperación.

Para obtener una lista completa de comandos y utilidades que puede usar en el entorno de los dispositivos de arranque, consulte Lista de comandos y utilidades disponibles en dispositivos de arranque basados en Linux (pág. 287). Para obtener una descripción detallada de las utilidades **trueimagecmd** y **trueimagemnt**, consulte la referencia de línea de comandos Acronis Backup & Recovery 10.

## Montaje de los volúmenes de copia de seguridad

Se recomienda a montar un volumen almacenado en una copia de seguridad del disco, por ejemplo, para ver algunos archivos antes de comenzar la recuperación.

### *Para montar un volumen de copia de seguridad*

1. Use la lista de comandos **--list** para enumerar los volúmenes que están almacenados en la copia de seguridad. Por ejemplo:

   ```
   trueimagecmd --list --filename:smb://server/backups/linux_machine.tib
   ```

   La salida contendrá líneas similares a las siguientes:

   ```
   Num  Idx Partition Flags Start Size      Type
   ---- --- --------- ----- ----- --------- ------
   Disk 1:
            Table           0               Table
   Disk 2:
            Table           0               Table
   ...
   Dynamic & GPT Volumes:
   DYN1 4   my_volgroup-my_logvol 12533760  Ext2
   ```

   En el próximo paso, necesitará el índice del volumen, el cual se proporciona en la columna **idx**.
2. Use el comando **--mount** y especifique el índice del volumen en el parámetro **-i** Por ejemplo:

   ```
   trueimagemnt --mount /mnt --filename smb://server/backups/linux_machine.tib -i
   4
   ```

   Este comando monta un volumen lógico DYN1 cuyo índice en la copia de seguridad es 4, en el punto de montaje /mnt.

### *Para montar un volumen de copia de seguridad*

- Use el comando **--unmount** y especifique el punto de montaje del volumen como parámetro. Por ejemplo:

  ```
  trueimagemnt --unmount /mnt
  ```

## 6.10.6 Acronis PXE Server

El servido PXE de Acronis permite el inicio del equipo de los componentes de arranque de Acronis a través de la red.

Inicio en red:

- Elimina la necesidad de contar con un técnico en el lugar para instalar el dispositivo de arranque en el sistema que debe iniciarse.
- Durante las operaciones de los grupos, reduce el tiempo requerido para el inicio de múltiples equipos en comparación al uso de dispositivos de arranque.

Los componentes se cargan al Servidor Acronis PXE utilizando el Constructor de Medios Reiniciables Acronis. Para subir los componentes reiniciables, inicie el Constructor de Medios Reiniciables (desde la consola de administración, seleccionando **Herramientas > Crear medio reiniciables** o como un componente por separado) y siga las instrucciones paso-a-paso descriptas en la sección "Constructor de Medios Reiniciables (pág. 278)".

El inicio de varios equipos desde el Servidor PXE de Acronis tiene sentido si hay un servidor de Protocolo de configuración dinámica de servidores (DHCP) en su red. Entonces, las interfaces de red de los equipos iniciados obtendrán sus direcciones IP automáticamente.

### Instalación del servidor PXE de Acronis

***Para instalar el servidor PXE de Acronis:***

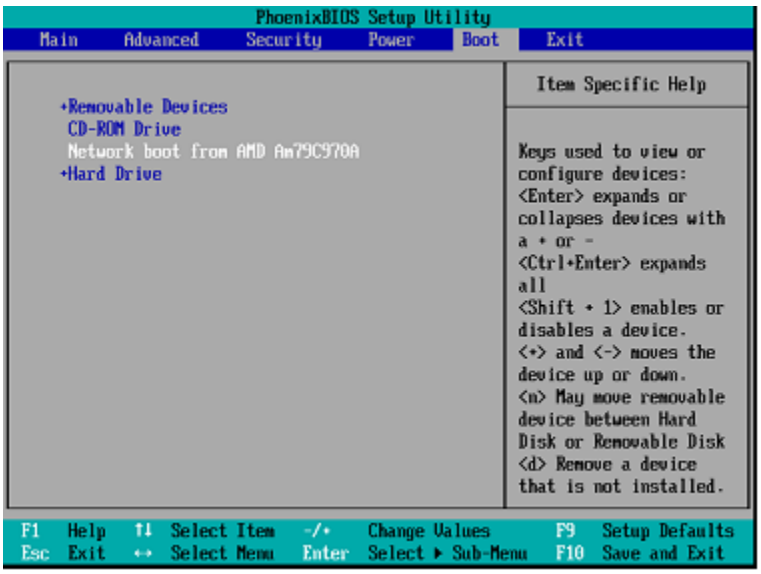
1. Ejecute el archivo de configuración de Acronis Backup & Recovery 10.
2. Seleccione el servidor PXE de Acronis de una lista de la **administración centralizada de los componentes**.
3. Siga las instrucciones en pantalla.

El servidor PXE de Acronis se ejecuta como servicio inmediatamente después de la instalación. Más adelante, se iniciará automáticamente en cada reinicio del sistema. Puede detener e iniciar el servidor PXE de Acronis del mismo modo que otros servicios de Windows.

### Configuración de un equipo para que inicie desde PXE.

Para que sea completa, es suficiente que el BIOS del equipo admita el inicio en red.

En un equipo que tiene un sistema operativo en el disco duro, se debe configurar el BIOS para que la interfaz de red sea el primer dispositivo de arranque o, al menos, tenga prioridad ante la unidad de disco duro. El ejemplo que se muestra a continuación indica una de las configuraciones de BIOS razonables. Si no inserta el dispositivo de arranque, el equipo iniciará desde la red.




En algunas versiones de BIOS, debe guardar los cambios de la BIOS después de activar la tarjeta de interfaz de red para que ésta aparezca en la lista de dispositivos de arranque.

Si el hardware cuenta con múltiples tarjetas de interfaz de red, asegúrese de que la tarjeta compatible con la BIOS tenga el cable de red conectado.

### PXE y DHCP en el mismo servidor

Si el servidor PXE de Acronis y el servidor DHCP están en el mismo equipo, agregue la opción 60 al servidor DHCP: “Client Identifier” con valor de cadena “PXE Client”. Esto se puede realizar de la siguiente manera:

```
C:\WINDOWS\system32>netsh
netsh>dhcp
netsh>dhcp>server \\<server_machine_name>  <Idirección IP>
netsh dhcp>add optiondef 60 PXEClient STRING 0 comment=”Option added for PXE support”
netsh dhcp>set optionvalue 60 STRING PXEClient
```

### Trabajo en todas las subredes

Para permitir que el servidor PXE de Acronis trabaje en otra subred (mediante el conmutador), configure el conmutador para que retransmita el tráfico de PXE. Las direcciones IP del servidor PXE se configuran por interfaz mediante la función auxiliar IP, de la misma manera que las direcciones del servidor DHCP. Para obtener más información, consulte: http://support.microsoft.com/kb/257579/es.

## 6.11 Gestión del disco

Acronis Disk Director Lite es una herramienta para preparar la configuración del disco/volumen de un equipo para recuperar las imágenes del volumen guardadas por el software de Acronis Backup & Recovery 10.

A veces, después de realizar la copia de seguridad de un volumen y guardar la imagen en un lugar seguro, puede cambiar la configuración del disco del equipo a causa de unl reemplazo de un HDD o pérdida de hardware. En dicho caso, con la ayuda de Acronis Disk Director Lite, el usuario tiene la posibilidad de recrear la configuración necesaria de disco para que se pueda recuperar con exactitud la imagen del disco "como estaba" o con cualquier alteración del disco o estructura del disco que el usuario pueda considerar necesario.

*Todas las operaciones con discos y volúmenes involucran cierto riesgo de daños de los datos. Las operaciones en el sistema, los volúmenes de arranque o datos, deben realizarse con mucho cuidado para evitar cualquier problema potencial con el proceso de arranque o el almacenamiento de los datos en el disco duro.*

*Las operaciones con disco duros y volúmenes llevan cierto tiempo, y cualquier pérdida de potencia, apagado involuntario del equipo o pulsación accidental del botón Reiniciar durante el proceso podría causar daños y pérdida de datos.*

*Todas las operaciones sobre volúmenes de discos dinámicos en Windows XP y Windows 2000 requieren del la ejecución del Servicio de Máquinas Gestionadas de Acronis bajo una cuenta con derechos administrativos.*

Tome todas las precauciones (pág. 295) necesarias para evitar cualquier posible pérdida de datos.

### 6.11.1 Precauciones posibles

Para evitar cualquier daño posible al disco y a la estructura del volumen o pérdida de datos, tome todas las precauciones necesarias y siga las siguientes reglas simples:

1. Crear la copia de seguridad del disco en los que se crearán o gestionarán los volúmenes Teniendo la copia de seguridad de sus datos más importantes en otro disco duro, red compartida o dispositivo extraíble le permitirá trabajar en los volúmenes de discos sabiendo que sus datos están seguros.
2. Pruebe su disco para asegurarse de que es completamente funcional y no contiene sectores defectuosos o errores del sistema de archivos.
3. No realice ninguna operación de disco/volumen mientras ejecuta otro software que tenga acceso bajo a nivel de disco. Cierre estos programas antes de ejecutar Acronis Disk Director Lite.

Con estas precauciones simples podrá protegerse contra pérdida de datos accidentales.

### 6.11.2 Ejecución de Acronis Disk Director Lite

Puede ejecutar Acronis Disk Director Lite bajo Windows o iniciarlo desde un dispositivo de arranque.

#### Ejecución de Acronis Disk Director Lite en Windows

Si ejecuta la consola de administración Acronis Backup & Recovery 10 y la conecta con el equipo administrado la vista de **Administración del disco** estará disponible en el árbol de **Navegación** de la consola, con el que se puede iniciar Acronis Disk Director Lite.

#### Ejecución de Acronis Disk Director Lite desde un dispositivo de arranque

Puede ejecutar Acronis Disk Director Lite en una restauración completa, en un equipo que no se pueda iniciar o en uno que no tenga Windows. Para hacerlo, inicie el equipo desde un dispositivo de arranque (pág. 410) creado con un generador Acronis de dispositivos de arranque; ejecute la consola de administración y después haga clic en **Administración del disco**.

### 6.11.3 Elección del sistema operativo para la gestión de discos

En un equipo con dos o más sistemas operativos, la representación de los discos y volúmenes depende de qué sistema operativo esté ejecutándose actualmente.

Un volumen puede tener una letra diferente en diferentes sistemas operativos de Windows. Por ejemplo, el volumen E: puede aparecer como D: o L: cuando inicia otro sistema operativo de Windows instalado en el mismo equipo. (También es posible que este volumen tenga la misma letra E: en cualquier sistema operativo de Windows instalado en el equipo.)

Un disco dinámico credo en un sistema operativo de Windows se considera un **Disco externo** en otro sistema operativo de Windows o puede no ser compatible con este sistema operativo.

Cuando debe realizar una operación de gestión de discos en dicho equipo, es necesario especificar para qué sistema operativo se mostrará la distribución del disco y la operación de gestión de discos se realizará.

El nombre del sistema operativo seleccionado actualmente se muestra en la barra de herramientas de la consola después de "**La distribución del disco actual es para:**". Haga clic en el nombre del sistema operativo para seleccionar otro sistema operativo en la ventana **Selección del sistema operativo**. En el dispositivo de inicio, esta ventana aparece después de hacer clic en **Gestión del disco**. La distribución del disco se mostrará según el sistema operativo que seleccione.

### 6.11.4 Vista "Administración del disco"

Acronis Disk Director Lite se controla mediante la vista **Administración del disco** de la consola.

La parte superior de la vista contiene una tabla de discos y volúmenes que permite la clasificación de datos y la personalización de columnas y barra de herramientas. La tabla presenta los números de los discos, la letra asignada, la etiqueta, el tipo, la capacidad, el espacio libre del disco, el espacio utilizado, el sistema de archivos y el estado para cada volumen. La barra de herramientas incluye los iconos que iniciarán las acciones de **Deshacer**, **Rehacer y Ejecutar** para operaciones pendientes (pág. 311).

El panel gráfico al pie de la vista también representa gráficamente todos los discos y sus volúmenes como rectángulos con datos básicos (etiqueta, letra, tamaño, estado, tipo y sistema de archivos).

Ambas partes de la vista representan todo el espacio de disco no asignado que se puede utilizar en la creación de volúmenes.

#### Comienzo de las operaciones

Se puede iniciar cualquier operación:

- Desde el menú contextual del volumen o disco (tanto en la tabla como en el panel gráfico)
- Desde el menú de **Administración del disco** de la consola
- Desde la barra de **Operaciones** en el panel de **Acciones y herramientas**

*Tenga en cuenta que la lista de operaciones disponibles en el menú contextual, el menú de **Administración del disco** y la barra de **Operaciones** dependen del volumen seleccionado o del tipo de disco. Lo mismo sucede con el espacio no asignado.*

### Visualización de resultados de las operaciones

Los resultados de cualquier operación de disco o volumen que acaba de planear se visualizan de inmediato en la vista **Administración del disco** de la consola. Por ejemplo, si crea un volumen, se muestra de inmediato en la tabla y en forma gráfica al pie de la vista. Cualquier cambio en el volumen, incluso el cambio de la letra o la etiqueta de éste, se visualiza de inmediato en la vista.

## 6.11.5 Operaciones del disco

Acronis Disk Director Lite incluye las siguientes operaciones que se pueden realizar en los discos:

- Inicio del disco (pág. 297) : inicia el nuevo hardware agregado al sistema
- Clonación básica del disco (pág. 298) : transfiere datos completos desde el disco básico MBR de origen al disco de destino
- Conversión del disco: de MBR a GUID (GPT) (pág. 300) : convierte una tabla de partición MBR en GUID (GPT)
- Conversión del disco: de GUID (GPT) a MBR (pág. 301) : convierte una tabla de partición GUID (GPT) en MBR
- Conversión del disco: de básico a dinámico (pág. 301) : convierte un disco básico en dinámico
- Conversión del disco: de dinámico a básico (pág. 302) : convierte un disco dinámico en básico

La versión completa del Acronis Disk Director brindará más herramientas y utilidades para trabajar con discos.

*Acronis Disk Director Lite debe obtener acceso exclusivo al disco de destino. Esto significa que ninguna otra utilidad de Administración del disco (como utilidad de Administración del disco de Windows) puede acceder en ese momento. Si recibe un mensaje que indica que no se puede bloquear el disco, cierre las aplicaciones de Administración del disco que están utilizando ese disco y comience de nuevo. Si no puede determinar qué aplicaciones utilizan el disco, cierre todas las aplicaciones.*

### Inicio del disco

Si agregó un disco nuevo a su equipo, Acronis Disk Director Lite notará el cambio de configuración y explorará el disco agregado, para incluirlo en la lista de discos y volúmenes. Si aún no se ha iniciado el disco o si quizá tiene una estructura desconocida para el sistema del equipo, esto significa que no se pueden instalar programas en el sistema y que no podrá restaurar ninguno de los archivos allí.

Acronis Disk Director Lite detectará que el disco no puede ser utilizado por el sistema y requiere de inicialización. La vista **Administración de disco** mostrará el hardware nuevo detectado como un bloque gris con un icono deshabilitado para su selección, que indica que el sistema no puede utilizar el disco.

***Si necesita inicializar el disco:***

1. Seleccione un disco para inicializar.
2. Haga clic con el botón secundario sobre el volumen seleccionado y después en **Inicializar** en el menú contextual. Pasará a la ventana **Inicialización de disco,** que ofrece los detalles de hardware básicos, como el número, capacidad y estado del disco, para ayudarle a escoger su posible acción.
3. En la ventana, podrá configurar el esquema de partición de disco (MBR o GPT) y el tipo de disco (básico o dinámico). El nuevo estado del disco se representará gráficamente de inmediato en la vista **Gestión del disco** de la consola.
4. Al hacer clic en **Aceptar**, añadirá una operación pendiente de la inicialización del disco.

(Para finalizar la operación agregada, deberá ejecutarla (pág. 311). La salida del programa sin la ejecución de las operaciones pendientes las cancelará de manera efectiva).

Después de la inicialización, todo el espacio de disco permanece no asignado, por lo cual es imposible usarlo para la instalación de programas o el almacenamiento de archivos. Para poder usarlo, proceda con normalidad a la operación de **Crear volumen**.

*Si decide cambiar las configuraciones del disco, puede hacerlo más adelante con las herramientas estándar de disco de Acronis Disk Director Lite*

## Clonación de disco básico

A veces es necesario transferir todos los datos del disco a un disco nuevo. Puede ser un caso de expansión del volumen del sistema, el comienzo de un nuevo diseño del sistema o la evacuación del disco, debido a una falla del hardware. En cualquier caso, la razón para la operación de **Clonar disco básico** se puede resumir como la necesidad de transferir todos los datos del disco origen a un disco de destino, tal como están.

Acronis Disk Director Lite permite la operación sólo entre discos básicos MBR.

Para planear la operación de **Clonar disco básico**:

1. Seleccione un disco que desee clonar.
2. Seleccione un disco como destino para la operación de clonación.
3. Seleccione un método de clonación y opciones avanzadas específicas.

La nueva estructura de volumen se representará gráficamente en la vista **Administración del disco** de inmediato.

*Se recomienda que desactive Acronis Startup Recovery Manager (pág. 400) (ASRM) si está activado antes de clonar un disco de sistema. De lo contrario, el sistema operativo clonado es posible que no inicie. Puede activar ASRM nuevamente cuando haya finalizado la clonación. Si no se puede desactivar, escoja el método **Tal como está** para clonar el disco.*

### Selección de los discos de origen y de destino

El programa muestra una lista de discos particionados y le pide al usuario que seleccione el disco de origen, desde el cual se transferirán los datos a otro disco.

El próximo paso es la selección de un disco como destino para la operación de clonación. El programa le permite al usuario seleccionar un disco, si su tamaño será suficiente para recibir todos los datos del disco de origen, sin ninguna pérdida.

Si hay algunos datos en el disco que se eligió como destino, el usuario recibirá la advertencia siguiente: "**El disco de destino seleccionado no está vacío. Se sobrescribirán los datos de sus volúmenes.**", esto significa que todos los datos actualmente ubicados en el disco de destino elegido se perderán irrevocablemente.

### Método de clonación y opciones avanzadas

La operación de **Clonar disco básico** por lo general significa que la información del disco de origen se transfiere al disco de destino "**tal como está**". Por lo tanto, si el disco de destino es del mismo tamaño, e incluso si es más grande, es posible transferir toda la información exactamente como está almacenada en el disco de origen.

Pero, con el amplio rango de hardware disponible, es normal que el disco de destino difiera en tamaño con respecto al de origen. Si el disco de destino es más grande, es recomendable redimensionar los volúmenes del disco de origen, para evitar dejar espacio no asignado en el disco de destino, con la selección de la opción **Redimensionar volúmenes proporcionalmente**. La opción para **Clonar disco básico** "tal como está" permanece, pero el método de clonación por defecto se llevará a cabo con el aumento proporcional de todos los volúmenes del disco de **origen** para que no quede espacio no asignado en el disco de **destino**.

Si el disco de destino es más pequeño, la opción de clonación **tal como está** no estará disponible y será obligatorio redimensionar proporcionalmente los volúmenes del disco de **origen**. El programa analiza el disco de **destino** para establecer si su tamaño será suficiente para guardar todos los datos del disco de **origen** sin ninguna pérdida. Si es posible tal transferencia con el redimensionamiento proporcional de los volúmenes del disco de **origen**, pero sin ninguna pérdida de datos, el usuario podrá continuar. Si, debido a las limitaciones de tamaño, es imposible la transferencia de todos los datos del disco de **origen** al disco de **destino**, incluso con el redimensionamiento proporcional de los volúmenes, entonces la operación de **Clonar disco básico** será imposible y el usuario no podrá continuar.

Si está por clonar un disco que incluye un **volumen del sistema**, preste atención a las **Opciones avanzadas**.

Al hacer clic en **Finalizar**, agregará la operación pendiente de la clonación de disco.

(Para finalizar la operación agregada, deberá ejecutarla (pág. 311). La salida del programa sin la ejecución de las operaciones pendientes las cancelará de manera efectiva).

### Uso de opciones avanzadas

Al clonar un disco que incluye un **volumen del sistema**, necesita retener la capacidad de inicio del sistema operativo en el volumen del disco de destino. Esto significa que el sistema operativo debe tener la misma información de volumen del sistema (por ejemplo, la letra del volumen) coincidente con la firma NT del disco que se mantiene en el registro de MBR del disco. Pero dos discos con la misma firma NT no pueden funcionar de manera correcta en un sistema operativo.

*Si hay dos discos que tienen la misma firma NT e incluyen un volumen del sistema en un equipo, al inicio el sistema operativo se ejecuta desde el primer disco, descubre la misma firma en el segundo, genera de manera automática una nueva firma NT única y se la asigna al segundo disco. Como resultado, todos los volúmenes del segundo disco perderán sus letras, todas las rutas serán inválidas en el disco y los programas no encontrarán sus archivos. El sistema operativo de ese disco no se iniciará.*

Tiene las dos alternativas siguientes para retener la capacidad de inicio del sistema en el volumen del disco de destino:

1. Copiar firma NT: para darle al disco de destino la firma NT del disco de origen coincidente con las claves de registro también copiadas en el disco de destino.
2. Dejar la firma NT: para mantener la antigua firma del disco de destino y actualizar el sistema operativo de acuerdo con esa firma.

***Si necesita copiar la firma NT:***

1. Seleccione la casilla de verificación **Copiar firma NT**. Recibirá la siguiente advertencia: "Si hay un sistema operativo en el disco duro, desinstale la unidad de disco duro de origen o de destino de su equipo antes de reiniciarlo. De otro modo, el SO se iniciará desde el primero de los dos discos y el SO en el segundo no se podrá iniciar." Se selecciona y deshabilita automáticamente la casilla de verificación **Apagar el equipo después de la operación de clonación**.
2. Haga clic en **Finalizar** para agregar la operación pendiente.

3. Haga clic en **Ejecutar** en la barra de herramientas y después en **Continuar** en la ventana de **Operaciones pendientes**.
4. Espere hasta que haya finalizado la operación.
5. Espere hasta que el equipo esté apagado.
6. Desconecte del equipo la unidad de disco duro de origen o de destino.
7. Inicie el equipo.

***Si necesita dejar la firma NT:***

1. Haga clic para borrar la casilla de verificación **Copiar firma NT**, si es necesario.
2. Haga clic para borrar la casilla de verificación **Apagar el equipo después de la operación de clonación**, si es necesario.
3. Haga clic en **Finalizar** para agregar la operación pendiente.
4. Haga clic en **Ejecutar** en la barra de herramientas y después en **Continuar** en la ventana de **Operaciones pendientes**.
5. Espere hasta que haya finalizado la operación.

## Conversión del disco: de MBR a GPT

Podría elegir convertir un disco básico MBR a uno básico GPT en los casos siguientes:

- Si necesita más de 4 volúmenes primarios en un disco.
- Si necesita confiabilidad adicional de un disco, ante cualquier posibilidad de daño de los datos.

***Si necesita convertir un disco básico MBR a uno básico GPT:***

1. Seleccione un disco básico MBR para convertirlo a GPT.
2. Haga clic con el botón secundario sobre el volumen seleccionado y después en **Convertir a GPT** en el menú contextual.

   Recibirá una ventana de advertencia que indica que está por convertir un disco MBR a GPT.
3. Al hacer clic en **Aceptar**, agregará una operación pendiente de conversión de disco MBR a GPT.

(Para finalizar la operación agregada, deberá ejecutarla (pág. 311). La salida del programa sin la ejecución de las operaciones pendientes las cancelará de manera efectiva).

---

*Tenga en cuenta que un disco particionado con GPT reserva el espacio necesario para el área de copia de seguridad al final del área particionada, la cual almacena copias del encabezado GPT y la tabla de partición. Si el disco está lleno y el tamaño de volumen no se puede reducir automáticamente, la operación de conversión del disco MBR a GPT fallará.*

*La operación es irreversible. Si tiene un volumen primario, que pertenece a un disco MBR, y convierte el disco primero a GPT y después de regreso a MBR, el volumen será lógico y no se podrá utilizar como volumen del sistema.*

---

Si planea instalar un SO que no admite discos GPT, también es posible la conversión inversa del disco a MBR, a través de los mismos elementos del menú. El nombre de la operación se enumerará como **Convertir a MBR**.

### Conversión de disco dinámico: de MBR a GPT

Acronis Disk Director Lite no admite la conversión directa de MBR a GPT para discos dinámicos. Sin embargo, puede efectuar las siguientes conversiones para lograr el objetivo mediante el uso del programa:

1. Conversión de disco MBR: de dinámico a básico (pág. 302) mediante el uso de la operación **Convertir a básico**.

2. Conversión de disco básico: de MBR a GPT mediante el uso de la operación **Convertir a GPT**.
3. Conversión de disco GPT: de básico a dinámico (pág. 301) mediante el uso de la operación **Convertir a dinámico**.

## Conversión del disco: de GPT a MBR

Si planea instalar un SO que no admite discos GPT, la conversión del disco GPT a MBR es posible y el nombre de la operación se enumerará como **Convertir a MBR**.

**Si necesita convertir un disco GPT a MBR:**

1. Seleccione un disco GPT para convertirlo a MBR.
2. Haga clic con el botón secundario sobre el volumen seleccionado y después en **Convertir a MBR** en el menú contextual.

   Recibirá una ventana de advertencia que indica que está por convertir un disco GPT a MBR.

   Se le explicarán los cambios que se producirán en el sistema después que se haya convertido el disco elegido de GPT a MBR. Es decir, si tal conversión evitará que el sistema acceda a un disco, si el sistema operativo dejará de cargar después de tal conversión o si algunos de los volúmenes del disco GPT seleccionado no serán accesibles con MBR (por ejemplo, los volúmenes ubicados a más de 2 TB del comienzo del disco), y se le advertirá aquí acerca de este daño.

   *Tenga en cuenta que un volumen que pertenece a un disco GPT a convertir será un volumen lógico después de que se haya completado la operación, y es irreversible.*
3. Al hacer clic en **Aceptar**, agregará una operación pendiente de conversión de disco GPT a MBR.

(Para finalizar la operación agregada, deberá ejecutarla (pág. 311). La salida del programa sin la ejecución de las operaciones pendientes las cancelará de manera efectiva).

## Conversión del disco: de básico a dinámico

Podría elegir convertir un disco básico a uno dinámico en los casos siguientes:

- Si planea usar el disco como parte de un grupo de discos dinámicos.
- Si desea lograr confiabilidad adicional del disco para el almacenamiento de datos.

***Si necesita convertir un disco básico a dinámico:***

1. Seleccione el disco básico para convertirlo a dinámico.
2. Haga clic con el botón secundario sobre el volumen seleccionado y después en **Convertir a dinámico** en el menú contextual. Recibirá una advertencia final acerca de la conversión del disco básico a dinámico.
3. Si hace clic en **Aceptar** en esta ventana de advertencia, la conversión se efectuará de inmediato y, si es necesario, su equipo se reiniciará.

   *Tenga en cuenta que un disco dinámico ocupa el último megabyte del disco físico para almacenar la base de datos, incluso la descripción de cuatro niveles (volumen, componente, partición, disco) para cada volumen dinámico. Si durante la conversión a dinámico, resulta que el primer disco básico está lleno y que el tamaño de sus volúmenes no se puede reducir automáticamente, fallará la operación de conversión del disco básico a dinámico.*

Si decide revertir la conversión de sus discos dinámicos a básicos, por ejemplo, si desea comenzar a usar un SO en su equipo que no admite discos dinámicos, puede convertir sus discos con los mismos elementos del menú, mediante la operación que ahora se denominará **Convertir a básico**.

### Conversión del disco de sistema

Acronis Disk Director Lite no requiere el reinicio del sistema operativo después de la conversión del disco de básico a dinámico, si:

1. Hay un único sistema operativo Windows 2008/Vista instalado en el disco.
2. El equipo ejecuta este sistema operativo.

*La conversión del disco de básico a dinámico, que incluye volúmenes de sistema, lleva cierto tiempo y cualquier pérdida de energía, apagado involuntario del equipo o presión accidental del botón de Restablecimiento durante el procedimiento podrían generar una pérdida en la capacidad de inicio .*

En contraste con el Administrador de discos de Windows, el programa asegura la capacidad de inicio de un **sistema operativo fuera de línea** en el disco, después de la operación.

## Conversión del disco: de dinámico a básico

Podría elegir convertir discos dinámicos de nuevo a básicos, por ejemplo, si desea comenzar a usar un SO en su equipo que no admita discos dinámicos.

***Si necesita convertir un disco dinámico a básico:***

1. Seleccione el disco dinámico para convertirlo a básico.
2. Haga clic con el botón secundario sobre el volumen seleccionado y después en **Convertir a básico** en el menú contextual. Recibirá una advertencia final acerca de la conversión del disco dinámico a básico.

   Se le explicarán los cambios que se producirán en el sistema, si el disco elegido se convierte de dinámico a básico. Es decir, si tal conversión evitará que el sistema acceda a un disco, si el sistema operativo dejará de cargar después de tal conversión o si el disco que desea convertir a básico contiene algún volumen del tipo no admitido por los discos dinámicos (todos los tipos de volúmenes excepto los Simples), después se le advertirán los daños posibles de los datos involucrados en la conversión.

   *Tenga en cuenta que la operación no está disponible para un disco dinámico que contenga volúmenes extendidos, segmentados o RAID-5.*

3. Si hace clic en **Aceptar** en esta ventana de advertencia, la conversión se efectuará de inmediato.

Después de la conversión, los últimos 8Mb de espacio de disco se reservan para la conversión futura del disco de básico a dinámico.

En algunos casos, es posible que difieran el espacio no asignado posible y el tamaño máximo de volumen propuesto (por ejemplo, cuando el tamaño de un espejo establece el del otro o cuando los últimos 8Mb de espacio de disco están reservados para la conversión futura del disco de básico a dinámico).

### Conversión del disco de sistema

Acronis Disk Director Lite no requiere el reinicio del sistema operativo después de la conversión del disco de dinámico a básico, si:

1. Hay un único sistema operativo Windows 2008/Vista instalado en el disco.
2. El equipo ejecuta este sistema operativo.

*La conversión del disco de dinámico a básico, que incluye volúmenes del sistema, lleva cierto tiempo y cualquier pérdida de energía, apagado involuntario del equipo o presión accidental del botón de Restablecimiento durante el procedimiento podrían generar una pérdida en la capacidad de inicio.*

En contraste con el Administrador de discos de Windows, el programa asegura:

- una segura conversión de un disco dinámico de modo básico cuando contiene volúmenes **con datos** para volúmenes simples y duplicados
- en los sistemas de inicio múltiples, la capacidad de iniciación del sistema que estuvo **fuera de línea** durante la operación.

## Cambio del estado del disco

El cambio del estado del disco es eficaz para los sistemas operativos Windows Vista SP1, Windows Server 2008, Windows 7 y se aplica a la actual distribución del disco (pág. 296).

Uno de los siguientes estados de disco siempre aparece en la vista gráfica del disco al lado del nombre del disco:

- **En línea**

  El estado en línea significa que el disco es accesible en el modo lectura-escritura. Este es el estado normal del disco. Si necesita un disco que sea accesible en el modo lectura-escritura, seleccione el disco y luego cambie su estado a fuera de línea seleccionando **Cambiar el estado del disco a fuera de línea** desde el menú **Operaciones**.
- **Fuera de Línea**

  El estado fuera de línea significa que se puede acceder al disco en el modo sólo lectura. Para que el disco seleccionado vuelva a estar en línea, seleccione **Cambiar estado del disco a en línea** desde el menú **Operaciones**.
  Si el disco tiene el estado fuera de línea y el nombre del disco es **Ausente**, esto significa que el sistema operativo no puede ubicar o identificar el disco. Puede estar dañado, desconectado o apagado. Para más información sobre cómo hacer que un disco que está fuera de línea y ausente vuelva a estar en línea, consulte el siguiente artículo de la Base de Conocimiento de Microsoft: http://technet.microsoft.com/es-es/library/cc732026.aspx.

## Importación de discos externos

En un equipo con dos o más sistemas operativos, la representación de los discos y volúmenes depende de qué sistema operativo esté ejecutándose actualmente.

Por lo general, todos los discos dinámicos creados dentro del mismo equipo y sistema operativo son miembros del mismo grupo de discos. Al moverse a otro equipo o añadirse a otro sistema operativo en el mismo equipo, el grupo de discos se considera **externo.** Los discos del grupo externo no se pueden utilizar hasta que se hayan importado al grupo de discos existente. Un grupo externo se importa tal como está (tendrá el nombre original) si no existe el grupo de discos en el equipo.

Para acceder a los datos en los discos externos, tendrá que añadir estos discos a la configuración del sistema de su equipo con la operación **Importar discos externos** .

---

*Todos los discos dinámicos del grupo de discos externos si importan al mismo tiempo, no puede importar solo un disco dinámico.*

---

### *Para importar discos externos*

1. Haga clic con el botón derecho en uno de los discos externos y después haga clic en **Importar discos externos**.

   La ventana que aparece enumera todos los discos dinámicos externos que se añadieron al equipo y muestra la información sobre los volúmenes que se importarán. Los estatus de los volúmenes le permiten detectar si está importando todos los discos necesarios de un grupo de discos. Al

importar todos los discos necesarios, todos los volúmenes tendrán el estatus **En buen estado**. Los estatus que sean diferentes a **En buen estado** indican que no todos los discos se importarán.

Para obtener más información sobre los estatus de los volúmenes, consulte el siguiente artículo de Microsoft: http://technet.microsoft.com/es-es/library/cc771775.aspx.

2. Haga clic en **Aceptar** para añadir la operación de importación de discos externos pendiente.

Los resultados de la operación pendiente se visualizan inmediatamente como si la operación se hubiese realizado.

Para realizar la operación pendiente tendrá que ejecutarla. Si abandona el programa sin ejecutar las operaciones pendientes se cancelarán.

## 6.11.6 Operaciones del volumen

Acronis Disk Director Lite incluye las siguientes operaciones que se pueden realizar en los volúmenes:

- Crear volumen (pág. 304) : crea un volumen nuevo con la ayuda del Asistente para crear volumen.
- Eliminar volumen (pág. 308) : elimina el volumen seleccionado.
- Configurar activo (pág. 309) : configura el volumen Activo seleccionado para que el equipo pueda iniciarse con el SO instalado allí.
- Cambiar letra (pág. 309) : cambia la letra del volumen seleccionada.
- Cambias etiqueta (pág. 310) : cambia la etiqueta de volumen seleccionada.
- Formatear volumen (pág. 310) : formatea un volumen y le otorga el sistema de archivos necesario.

La versión completa del Acronis Disk Director brindará más herramientas y utilidades para trabajar con volúmenes.

*Acronis Disk Director Lite debe obtener acceso exclusivo al volumen de destino. Esto significa que ninguna otra utilidad de administración del disco (como utilidad de Administración del disco de Windows) puede acceder en ese momento. Si recibe un mensaje que indica que no se puede bloquear el volumen, cierre las aplicaciones de administración del disco que están utilizando ese volumen y comience de nuevo. Si no puede determinar qué aplicaciones utilizan el volumen, cierre todas las aplicaciones.*

### Creación de un volumen

Es posible que necesite un volumen nuevo para:

- recuperar una copia de seguridad guardada previamente en la configuración “tal como estaba”;
- almacenar colecciones de archivos similares por separado, por ejemplo, una colección de archivos MP3 o de video en un volumen separado;
- almacenar copias de seguridad (imágenes) de otros volúmenes/discos en un volumen especial;
- instalar un sistema operativo nuevo (o archivo de intercambio) en un volumen nuevo;
- agregar hardware nuevo a un equipo.

En Acronis Disk Director Lite la herramienta para crear volúmenes es el **Asistente para crear volumen**.

## Tipos de volúmenes dinámicos

**Volumen simple**

Un volumen creado desde espacio libre de un único disco físico. Puede constar de una o varias regiones en el disco, unidas virtualmente por el Administrador de discos lógicos (LDM). No brinda confiabilidad adicional, ni mejora de velocidad, ni tamaño extra.

**Volumen extendido**

Un volumen creado desde espacio de disco libre unido virtualmente por el LDM, a partir de varios discos físicos. Se pueden incluir hasta 32 discos en un solo volumen, de manera tal que se superan las limitaciones de tamaño del hardware, pero si al menos un disco falla, se perderán todos los discos y no se podrá eliminar ninguna parte del volumen extendido, sin destruirlo en su totalidad. Por lo tanto, un volumen extendido no brinda confiabilidad adicional ni una mejor tasa de E/S.

**Volumen segmentado**

Un volumen, también denominado RAID 0, que consta de segmentos de datos de igual tamaño, escritos a través de cada disco en el volumen; esto significa que para crear un volumen segmentado, el usuario necesitará dos o más discos dinámicos. No es necesario que los discos de un volumen segmentado sean idénticos, pero debe haber espacio no utilizado disponible en cada disco que desee incluir en el volumen y el tamaño del volumen dependerá del tamaño del espacio más pequeño. El acceso a los datos de un volumen segmentado por lo general es más rápido que el acceso a los mismos datos en un disco físico único, porque la E/S está distribuida entre más de un disco.

Los volúmenes segmentados se crean para mejorar el rendimiento, no por su confiabilidad superior, ya que no contienen información redundante.

**Volumen espejado**

Un volumen tolerante a las fallas, también denominado RAID 1, cuyos datos se duplican en dos discos físicos idénticos. Todos los datos de un disco se copian a otro, para brindar redundancia de datos. Casi todos los volúmenes se pueden espejar, incluso los de sistema e inicio, si uno de los discos falla, es posible acceder a los datos desde los discos restantes. Desafortunadamente, las limitaciones del hardware en cuanto a tamaño y rendimiento son aún más graves con el uso de volúmenes espejados.

**Volumen espejado-segmentado**

Un volumen tolerante a las fallas, también denominado RAID 1+0, que combina la ventaja de la alta velocidad de E/S del diseño segmentado y la redundancia del tipo espejado. La desventaja evidente sigue siendo inherente a a arquitectura de espejo: una baja proporción de tamaño de disco a volumen.

**RAID-5**

Un volumen tolerante a las fallas cuyos datos se segmentan a través de un conjunto de tres o más discos. No es necesario que los discos sean idénticos, pero debe haber bloques de igual tamaño de espacio no asignado disponible en cada disco del volumen. La paridad (un valor calculado que se puede utilizar para recuperar datos después de un fallo) también se segmenta en el conjunto de discos y iempre se almacena en un disco diferente al que contiene los datos. Si un disco físico falla, la porción del volumen RAID-5 que estaba en el disco donde se produjo el fallo se puede volver a crear a partir de los datos y la paridad restantes. Un volumen RAID-5 brinda confiabilidad y puede superar las limitaciones físicas del tamaño de discos con una proporción superior de tamaño disco a volumen, comparada con la del tipo espejado.

## Asistente para crear volumen

El asistente para **Crear volumen** le permite crear cualquier tipo de volumen (incluso de sistema y activo), seleccionar un sistema de archivos, etiquetas, asignar una letra. Además, le brinda otras funciones de Administración del disco.

Sus páginas le permitirán ingresar parámetros de operaciones, continuar paso a paso y regresar a cualquier paso anterior, si es necesario, para cambiar cualquiera de las opciones seleccionadas previamente. Para ayudarlo con sus opciones, cada parámetro está complementado con instrucciones detalladas.

**Si desea crear un volumen**:

Ejecute el asistente para **Crear volumen** al seleccionar **Crear volumen** en la barra de **Asistentes,** o haga clic en el botón secundario sobre cualquier espacio no asignado y seleccione **Crear volumen** en el menú contextual que aparece.

## Seleccionar el tipo de volumen que creará

En el primer paso, debe especificar el tipo de volumen que desea crear. Se encuentran disponibles los siguientes tipos de volumen:

- Básico
- Simple/Extendido
- Segmentado
- Replicado
- RAID-5

Obtendrá una descripción breve de cada tipo de volumen para una mejor comprensión de las ventajas y limitaciones de cada arquitectura de volumen posible.

*Si el sistema operativo actual instalado en ese equipo no admite el tipo de volumen seleccionado, recibirá la advertencia adecuada. En este caso, se deshabilitará el botón **Siguiente** y deberá seleccionar otro tipo de volumen para continuar con la creación de volúmenes.*

Después de hacer clic en el botón **Siguiente** , continuará a la página siguiente: Seleccionar discos de destino (pág. 306).

## Seleccionar discos de destino

La página siguiente le solicita que elija los discos, cuy espacio se utilizará para la creación de volúmenes.

**Para crear un volumen básico:**

- Seleccione un disco de destino y especifique el espacio no asignado donde creará el volumen básico.

**Para crear un volumen simple/extendido:**

- Seleccione uno o más discos de destino donde creará el volumen.

**Para crear un volumen espejado:**

- Seleccione dos discos de destino donde creará el volumen.

**Para crear un volumen segmentado:**

- Seleccione dos o más discos de destino donde creará el volumen.

**Para crear un volumen RAID-5:**

- Seleccione tres discos de destino donde creará el volumen.

Después de elegir los discos, el asistente calculará el tamaño máximo del volumen resultante, según el tamaño del espacio no asignado en los discos que eligió y los requisitos del tipo de volumen por el cual se decidió previamente.

Si está creando un volumen **dinámico** y selecciona uno o varios discos **básicos**, como destino, recibirá una advertencia que indica que el disco seleccionado se convertirá a dinámico automáticamente.

Si es preciso, se le solicitará que agregue el número necesario de discos a su selección, según el tipo de volumen futuro elegido.

Si hace clic en el botón **Atrás** , regresará a la página anterior: Seleccionar el tipo de volumen que creará. (pág. 306)

Si hace clic en el botón **Siguiente** , continuará a la página siguiente: Configurar el tamaño del volumen (pág. 307).

## Configurar el tamaño del volumen

En la tercera página del asistente podrá definir el tamaño del volumen futuro, de acuerdo con las selecciones previas. Para elegir el tamaño necesario entre los valores mínimos y máximos, utilice el deslizador o ingrese los valores necesarios en las ventanas especiales entre los mínimos y máximos, o bien haga clic en el controlador especial y mantenga y arrastre los bordes de la imagen del disco con el cursor.

Por lo general, el valor máximo incluye el mayor espacio no asignado posible. Pero en algunos casos, es posible que difieran el espacio no asignado posible y el tamaño máximo de volumen propuesto (p. e., cuando el tamaño de un espejo establece el del otro o cuando los últimos 8Mb de espacio de disco están reservados para la conversión futura del disco de básico a dinámico).

Para volúmenes básicos, si queda espacio no asignado en el disco, también podrá elegir la posición del volumen nuevo en el disco.

Si hace clic en el botón **Atrás** , regresará a la página anterior: Seleccionar discos de destino (pág. 306).

Si hace clic en el botón **Siguiente** , continuará a la página siguiente: Configurar las opciones de volumen (pág. 307).

## Configurar las opciones de volumen

En la página siguiente del asistente, puede asignar la **Letra** de volumen (por defecto, la primera letra del abecedario) y, como opción, una **Etiqueta** (por defecto, ninguna). Aquí también puede especificar el **Sistema de archivos** y el **Tamaño del clúster**.

El asistente le solicitará que elija uno de los sistemas de archivos de Windows: FAT16 (deshabilitado, si el tamaño del volumen se configuró en más de 2 GB), FAT32 (deshabilitado, si el tamaño de volumen se configuró en más 2 TB), NTFS, o bien que deje el volumen en **Sin formatear**.

Al configurar el tamaño del clúster, puede elegir entre cualquier número en la cantidad preconfigurada, para cada sistema de archivos. Tenga en cuenta que el programa sugiere el mejor tamaño del clúster para el volumen, con el sistema de archivos elegido.

Si está creando un volumen básico, el cual se puede convertir en un volumen del sistema, esta página será diferente y le brindará la oportunidad de seleccione el **Tipo** de volumen: **primario** (**activo primario**) o **lógico**.

Por lo general, se selecciona **Primario** para instalar un sistema operativo en un volumen. Seleccione el valor **Activo** (por defecto) si desea instalar un sistema operativo en este volumen, para que se inicie al arrancar el equipo. Si el botón **Primario** no está seleccionado, la opción **Activo** estará inactiva. Si utilizará el volumen para almacenamiento de datos, seleccione **Lógico**.

*Un disco básico puede contener hasta cuatro volúmenes primarios. Si ya existen, se deberá convertir el disco a dinámico, de otro modo las opciones **Activo** y **Primario** se deshabilitarán y sólo podrá seleccionar el tipo de volumen **Lógico** . El mensaje de advertencia le indicará que uno de los SO instalados en este volumen no tendrá capacidad de inicio.*

*Si utiliza caracteres, al configurar una nueva etiqueta de volumen, no admitidos por el sistema operativo instalado en la actualidad, recibirá la advertencia adecuada y se deshabilitará el botón **Siguiente**. Deberá cambiar la etiqueta para continuar con la creación del volumen nuevo.*

Si hace clic en el botón **Atrás**, regresará a la página anterior: Configurar el tamaño del volumen (pág. 307).

Si hace clic en el botón **Finalizar**, completará la planificación de la operación.

Para realizar la operación planeada, haga clic en **Ejecutar** en la barra de herramientas y después en **Continuar** en la ventana de **Operaciones pendientes .**

*Si configura un tamaño del clúster de 64K para FAT16/FAT32, o bien un tamaño del clúster de 8KB-64KB para NTFS, Windows puede montar el volumen, pero algunos programas (p.e., los programas de Configuración) podrían calcular su espacio de disco de manera incorrecta.*

## Eliminar volumen

*Esta versión de Acronis Disk Director Lite tiene funcionalidad reducida, porque es principalmente una herramienta para preparar sistemas completos para recuperar imágenes de volúmenes guardadas con anterioridad. Las funciones de redimensionar los volúmenes existentes y crear nuevos, utilizando espacio libre de los ya existentes, existen* en la versión completa de software*, de modo que con esta versión, eliminar un volumen existente puede ser, en ocasiones, la única manera de liberar el espacio de disco necesario sin cambiar su configuración existente.*

Después de eliminar un volumen, se agrega su espacio al espacio de disco no asignado. Se puede utilizar para la creación de un volumen nuevo o para cambiar el tipo de otro volumen.

***Si necesita eliminar un volumen:***

1. Seleccione un disco duro y un volumen para eliminar.
2. Seleccione **Eliminar volumen** o un elemento similar en la lista de la barra lateral de **Operaciones** o haga clic en el icono de **Eliminar el volumen seleccionado** en la barra de herramientas.

   *Si el volumen contiene algún dato, recibirá la advertencia de que toda la información de ese volumen se perderá irrevocablemente.*
3. Al hacer clic en **Aceptar** en la ventana **Eliminar volumen**, agregará la operación pendiente de eliminación de volumen.

(Para finalizar la operación agregada, deberá ejecutarla (pág. 311). La salida del programa sin la ejecución de las operaciones pendientes las cancelará de manera efectiva).

## Configurar volumen activo

Si tiene varios volúmenes primarios, debe especificar uno para que sea el volumen de inicio. Para esto, puede configurar un volumen para que sea el activo. Un disco sólo puede tener un volumen activo, de manera que si configura un volumen como activo, el volumen que estaba activo antes, se desconfigurará de manera automática.

***Si necesita configurar un volumen activo:***

1. Seleccione un volumen primario como activo, en un disco MBR básico.
2. Haga clic con el botón secundario sobre el volumen seleccionado y después en **Marcar como activo** en el menú contextual.

   Si no hay otro volumen activo en el sistema, se agregará la operación pendiente de configuración de volumen activo.

   *Tenga en cuenta que, debido a la configuración del volumen activo nuevo, la letra del anterior se podría cambiar y algunos de los programas instalados podrían dejar de ejecutarse.*
3. Si hay otro volumen activo presente en el sistema, recibirá la advertencia de que el volumen activo anterior se deberá configurar como pasivo en primer lugar. Al hacer clic en **Aceptar** en la ventana **Advertencia**, agregará la operación pendiente de configuración de volumen activo.

   *Tenga en cuenta que, incluso si tiene el sistema operativo en el nuevo volumen activo, en algunos casos, el equipo no podrá iniciarse desde allí. Deberá confirmar su decisión para configurar el volumen nuevo como activo.*

(Para finalizar la operación agregada, deberá ejecutarla (pág. 311). La salida del programa sin la ejecución de las operaciones pendientes las cancelará de manera efectiva).

La nueva estructura de volumen se representará gráficamente en la vista **Administración del disco** de inmediato.

## Cambiar la letra del volumen

Los sistemas operativos Windows les asignan letras (C:, D:, etc.) a los volúmenes de los discos duros en el inicio. Las aplicaciones y los sistemas operativos usan estas letras para ubicar archivos y carpetas en los volúmenes.

Al conectar un disco adicional y al crear o eliminar un volumen en los discos existentes, se podría cambiar la configuración del sistema. Como resultado, algunas aplicaciones dejan de funcionar correctamente o es posible que no se puedan encontrar ni abrir de manera automática los archivos del usuario. Para evitar esto, puede cambiar manualmente las letras que el sistema operativo asigna de manera automática a los volúmenes.

***Si necesita cambiar una letra que asignó el sistema operativo a un volumen:***

1. Seleccione un volumen para cambiar la letra.
2. Haga clic con el botón secundario sobre el volumen seleccionado y después en **Cambiar letra** en el menú contextual.
3. Seleccione una letra nueva en la ventana **Cambiar letra**.
4. Al hacer clic **Aceptar** en la ventana **Cambiar letra**, agregará una operación pendiente a la asignación de letra del volumen.

   (Para finalizar la operación agregada, deberá ejecutarla (pág. 311). La salida del programa sin la ejecución de las operaciones pendientes las cancelará de manera efectiva).

La nueva estructura de volumen se representará gráficamente en la vista **Administración del disco** de inmediato.

## Cambiar la etiqueta de volumen

La etiqueta de volumen es un atributo opcional. Es un nombre asignado a un volumen para reconocerlo con mayor facilidad. Por ejemplo, un volumen podría llamarse SISTEMA (un volumen con un sistema operativo) o PROGRAMA (un volumen con aplicaciones), DATOS (un volumen con datos, etc.) pero no implica que solamente el tipo de datos indicado en la etiqueta podría almacenarse en tal volumen.

En Windows, las etiquetas de volumen se muestran en el Explorador y en el árbol de carpetas: ETIQUETA1(C:), ETIQUETA2(D:), ETIQUETA3(E:), etc. ETIQUETA1, ETIQUETA2 y ETIQUETA3 son etiquetas de volumen. Se muestra una etiqueta de volumen en todas los cuadros de diálogo de las aplicaciones, para abrir y guardar archivos.

***Si necesita cambiar una etiqueta de volumen:***

1. Haga clic en el botón secundario sobre el volumen seleccionado y después en **Cambiar etiqueta**.
2. Ingrese una etiqueta nueva en el campo de texto de la ventana **Cambiar etiqueta** .
3. Al hacer clic en **Aceptar** en la ventana **Cambiar etiqueta**, agregará la operación pendiente de cambiar la etiqueta de volumen.

   *Si al configurar una nueva etiqueta de volumen utiliza caracteres no admitidos por el sistema operativo instalado en la actualidad, recibirá la advertencia adecuada y se deshabilitará el botón **Aceptar**. Deberá usar únicamente caracteres admitidos para continuar con el cambio de la etiqueta de volumen.*

   (Para finalizar la operación agregada, deberá ejecutarla (pág. 311). La salida del programa sin la ejecución de las operaciones pendientes las cancelará de manera efectiva).

La nueva etiqueta de volumen se representará gráficamente de inmediato en la vista **Administración del disco** de la consola.

## Formatear volumen

Se recomienda formatear un volumen si quiere cambiar su sistema de archivos:

- para guardar espacio adicional que se está perdiendo debido al tamaño del clúster en los sistemas de archivos FAT16 o FAT32
- como una manera más rápida y más o menos confiable de destruir datos que se encuentran en este volumen

***Si desea formatear un volumen:***

1. Seleccione un volumen para formatear.
2. Haga clic con el botón secundario sobre el volumen seleccionado y después en **Formatear** en el menú contextual.

   Llegará a la ventana **Formatear Volumen**, donde podrá configurar las nuevas opciones para el sistema de archivos. Puede elegir uno de los sistemas de archivos de Windows: FAT16 (deshabilitado, si el tamaño del volumen es más de 2 GB), FAT32 (deshabilitado, si el tamaño del volumen es más de 2 TB) o NTFS.

   En la ventana de texto podrá ingresar la etiqueta de volumen, si es necesario (por defecto, la ventana está vacía).

   Al configurar el tamaño del clúster, puede elegir entre cualquier número en la cantidad preconfigurada, para cada sistema de archivos. Tenga en cuenta que el programa sugiere el mejor tamaño del clúster para el volumen, con el sistema de archivos elegido.
3. Si hace clic en **Aceptar** para continuar con la operación de **Formatear Volumen**, agregará una operación pendiente de formateo de volumen.

(Para finalizar la operación agregada, deberá ejecutarla (pág. 311). La salida del programa sin la ejecución de las operaciones pendientes las cancelará de manera efectiva).

La nueva estructura de volumen se representará gráficamente en la vista **Administración del disco**.

*Si configura un tamaño del clúster de 64K para FAT16/FAT32, o bien un tamaño del clúster de 8KB-64KB para NTFS, Windows puede montar el volumen, pero algunos programas (por ejemplo, los programas de Configuración) podrían calcular su espacio de disco de manera incorrecta.*

### 6.11.7 Operaciones pendientes

Todas las operaciones, las que preparó el usuario en modo manual o con la ayuda de un asistente, se consideran pendientes hasta que el usuario emite el comando específico para que los cambios sean permanentes. Hasta entonces, Acronis Disk Director Lite sólo demostrará la nueva estructura de volumen que resultará de las operaciones planeadas, para su ejecución en los discos y volúmenes. Este enfoque le permite controlar todas las operaciones planeadas, verificar dos veces los cambios pensados y, si es necesario, cancelar operaciones antes de que se ejecuten.

Para evitar que introduzca cambios involuntarios en su disco, el programa le mostrará en primer lugar la lista de todas las operaciones pendientes.

La vista **Administración del disco** contiene la barra de herramientas con iconos para iniciar las acciones de **Deshacer**, **Rehacer** y **Ejecutar** para las operaciones pendientes. Estas acciones también se podrían iniciar desde el menú **Administración del disco** de la consola.

Todas las operaciones planeadas se agregan a la lista de operaciones pendientes.

La acción **Deshacer** le permite deshacer la última operación de la lista. En tanto que la lista no esté vacía, esta acción está disponible.

La acción **Rehacer** le permite rehacer la última operación pendiente que se deshizo.

La acción **Ejecutar** lo envía a la ventana de **Operaciones pendientes**, donde podrá visualizar la lista de operaciones pendientes. Al hacer clic en **Continuar** se iniciará su ejecución. No podrá deshacer ninguna acción ni operación después de elegir la operación **Continuar**. También puede cancelar la ejecución al hacer clic en **Cancelar**. De este modo no se introducirán cambios en la lista de operaciones pendientes.

Si sale del Acronis Disk Director Lite sin ejecutar las operaciones pendientes, éstas se cancelarán, de modo que si intenta salir de **Administración del disco** sin ejecutar las operaciones pendientes, recibirá la advertencia adecuada.

## 6.12 Recolección de información del sistema

La herramienta de recolección de información del sistema recopila información acerca del equipo al cual está conectada la consola de gestión y la guarda en un archivo. Es conveniente que proporcione este archivo cuando se ponga en contacto con la asistencia técnica de Acronis.

Esta opción está disponible en los dispositivos de inicios y para equipos donde Agente para Windows, Agente para Linux o Acronis Backup & Recovery 10 Management Server esté instalado.

***Para recolectar la información del sistema***

1. Seleccione **Ayuda** > **Recopilar información del sistema desde** 'nombre del equipo' en el menú superior de la consola de gestión.

2. Especifique dónde guardar al archivo con la información de sistema.

# 7 Gestión centralizada

Esta sección cubre las operaciones que pueden realizarse centralmente al utilizar los componentes para la gestión centralizada. El contenido de esta sección solo es aplicable a las ediciones avanzadas de Acronis Backup & Recovery 10.

## 7.1 Administración de Acronis Backup & Recovery 10 Management Server

Esta sección describe las vistas que están disponibles a través del árbol de navegación de la consola conectada a un servidor de gestión y explica cómo trabajar en cada vista.

### 7.1.1 Tablero

Utilice el Tablero para calcular rápidamente el estado de la protección de los datos en los equipos registrados. El Tablero muestra la actividad de los agentes de Acronis Backup & Recovery 10, le permite comprobar si existe espacio libre disponible en las bóvedas gestionadas e identifica y resuelve rápidamente cualquier problema.

#### Alertas

La sección Alertas llama su atención sobre los problemas que han ocurrido en el servidor de gestión, en los equipos registrados y en las bóvedas centralizadas, a la vez que le ofrece métodos para resolverlos o examinarlos. Los problemas más críticos se muestran en la parte superior. Si no hay alertas o advertencias en ese momento, el sistema muestra "No hay alertas ni advertencias".

#### Tipos de alertas

La siguiente tabla muestra los tipos de mensajes que podría observar.

| | Descripción | Solución | Comentario |
|---|---|---|---|
| | Tareas fallidas: *X* | Ver las tareas | **Ver las tareas** abrirá la vista **Planes y tareas de copia de seguridad** con las tareas fallidas, donde se puede averiguar la razón del fallo.. |
| | Tareas que necesitan interacción: *X* | Resolver | Cuando existe al menos una tarea en la base de datos del servidor de gestión que necesita la interacción del usuario, el Tablero muestra una alerta. Haga clic en **Resolver...** para abrir la ventana **Tareas que necesitan interacción** donde se puede valorar cada caso y tomar una decisión. |
| | No se pudieron comprobar las licencias en *X* equipo(s) | Ver registro | Acronis Backup & Recovery 10 Agent se conecta a Acronis License Server en el inicio y después de 1 a 5 días, según se encuentre especificado en los parámetros de configuración del agente. Si la comprobación de una licencia no se ha completado correctamente al menos en un agente, se muestra una alerta. Esto podría suceder si el servidor de licencias no estuviera disponible o si los datos de la clave de licencia estuvieran dañados. Haga clic en **Ver registro** para descubrir la causa de una comprobación |

| | | | |
|---|---|---|---|
| | | | incorrecta.<br><br>Si la comprobación de la licencia no se realiza correctamente antes de 1 a 60 días (según se encuentre especificado en los parámetros de configuración del agente), el agente dejará de funcionar hasta que una comprobación de licencia resulte correcta. |
|  | Bóvedas con poco espacio libre: *X* | Ver bóvedas | Se muestra una alerta si al menos una de las bóvedas centralizadas posee menos del 10% del espacio libre. **Ver bóvedas** le llevará a la vista **Bóvedas centralizadas (pág. 132)** , donde se puede examinar el tamaño de la bóveda, el espacio libre y el contenido y realizar los pasos que sean necesarios para aumentar el espacio libre. |
|  | El dispositivo de inicio no se creó | Crear ahora | Para poder recuperar un sistema operativo cuando un equipo no se puede iniciar, debe:<br><br>1. Realizar una copia de seguridad del volumen del sistema (y del volumen de inicio, si es diferente).<br><br>2. Crear al menos un dispositivo de inicio (pág. 410).<br><br>**Crear ahora** ejecutará el Generador de dispositivos de inicio (pág. 406). |
|  | No se han creado copias de seguridad en los últimos *X* días(s) en *Y* equipo(s) | Mostrar lista | El Tablero lo alerta de que no se ha realizado ninguna copia de seguridad de los datos en los equipos registrados en un periodo de tiempo.<br><br>Para configurar el periodo de tiempo que considere adecuado, seleccione **Opciones> Opciones de la consola > Alertas según el momento**. |
|  | No se han conectado al servidor de gestión en los últimos *X* día(s): *Y* equipo(s) | Ver los equipos | El Tablero le avisa de que no se ha establecido ninguna conexión entre algunas de los equipos registrados y el servidor de gestión durante un periodo de tiempo, indicando por lo tanto que los equipos podrían no estar gestionados de manera centralizada.<br><br>Haga clic en **Ver los equipos** para abrir la vista **Equipos** con la lista de los equipos filtrada por el campo "Ultima conexión".<br><br>Para configurar el periodo de tiempo que considere adecuado, seleccione **Opciones> Opciones de la consola > Alertas según el momento**. |
|  | Se recomienda realizar un copia de seguridad del servidor de gestión para proteger su configuración. Instalar el agente en la máquina del servidor de gestión y agregue la máquina al AMS. | Instale los componentes de Acronis | Instale Acronis Backup & Recovery 10 Agent de Windows para realizar copias de seguridad del equipo donde está instalado Acronis Backup & Recovery 10 Management Server.<br><br>Haga clic en **Instalar ahora** para ejecutar el asistente de instalación. |
|  | No se ha creado una copia de seguridad de Acronis Backup & Recovery 10 Management Server desde hace *X* día(s) | Crear copia de seguridad ahora | Solamente se muestra una alerta si Acronis Backup & Recovery 10 Agent de Windows se encuentra instalado en el servidor de gestión. La alerta lo advierte de que no se realizaron copias de seguridad |

| | | | |
|---|---|---|---|
| | | | en el servidor de gestión durante un periodo de tiempo.<br><br>**Crear copia de seguridad ahora** le llevará a la página **Crear plan de copia de seguridad**, donde puedes configurar y ejecutar el plan de copia de seguridad al instante.<br><br>Para configurar el periodo de tiempo que considere adecuado, seleccione **Opciones> Opciones de la consola > Alertas según el momento**. |

### Actividades

El gráfico de barras apiladas le permite examinar el historial diario de las actividades de los agentes de Acronis Backup & Recovery 10. El historial se basa en las entradas del registro, recopiladas a partir de los equipos registrados y del servidor de gestión. El gráfico muestra el número de entradas del registro de cada tipo (error, advertencia, información) para un día en particular.

Las estadísticas para la fecha seleccionada se muestran en la parte derecha del gráfico. Todos los campos de las estadísticas son interactivos, es decir, si hacemos clic en uno de los campos, se abrirá la vista **Registro** con las entradas del registro prefiltradas por este campo.

En la parte superior de la gráfica, puede seleccionar las actividades que se muestran, dependiendo de la presencia y de la gravedad de los errores.

El enlace **Seleccionar fecha actual** aplica la fecha actual a la selección.

### Vista Sistema

La sección **Vista Sistema** muestra las estadísticas de los equipos registrados, las tareas, las políticas de copia de seguridad y los planes de copias de seguridad centralizados. Haga clic en cada uno de los elementos de estas secciones (excepto para planes de copias de seguridad centralizados) para obtener la información correspondiente. Esto lo llevará a la vista oportuna con, respectivamente, equipos, tareas o políticas de copia de seguridad prefiltrados. Por ejemplo, si hace clic en **Inactivo** en **Tareas**, se abrirá la vista **Tareas** con las tareas prefiltradas por el estado **Inactivo**.

La información presentada en la sección **Vista Sistema** se actualiza cada vez que el servidor de gestión se sincroniza con los equipos. La información del resto de las secciones se actualiza cada 10 minutos y siempre que accede al Tablero.

### Bóvedas

La sección **Bóvedas** muestra información sobre las bóvedas gestionadas centralizadas. Puede ordenar las bóvedas por nombre o por espacio utilizado. En algunas ocasiones, la información acerca del espacio libre en una bóveda podría no estar disponible, por ejemplo, si la bóveda se encuentra ubicada en una biblioteca de cintas. Si la propia bóveda no estuviera disponible (desconectada), aparecerá el mensaje "La bóveda no se encuentra disponible".

## 7.1.2 Políticas de copia de seguridad

Para poder gestionar y proteger varios equipos como un conjunto, puede crear una plantilla de plan de copias de seguridad llamada "política de copias de seguridad". Al aplicar esta plantilla a un grupo de equipos, se implementarán varios planes de copias de seguridad con una sola acción. Las políticas de copias de seguridad solo existen en Acronis Backup & Recovery 10 Management Server.

No hace falta que se conecte a cada equipo por separado para comprobar si los datos se encuentran protegidos correctamente. En su lugar, compruebe el estado acumulativo de la política (pág. 316) en todos los equipos en los que se aplica dicha política.

Para comprobar en cualquier momento si una política se está implementando, recovando o actualizando, compruebe el estado de implementación (pág. 316) de la política.

### Modo de trabajo con la vista Políticas de copia de seguridad

- Utilice los botones de la **barra de herramientas** para crear nuevas políticas, aplicar las ya existentes o realizar otras operaciones con políticas de copia de seguridad (pág. 318).
- Utilice las pestañas del panel **Información** para ver información detallada sobre la política seleccionada y realizar operaciones adicionales como, por ejemplo, revocar la política, ver los detalles del equipo (grupo) en los que se aplica la política, etc. De manera predeterminada, el panel se encuentra minimizado. Para expandir el panel, haga clic en la flecha tipo  . El contenido del panel también se encuentra en la ventana Detalles de la política (pág. 320).
- Utilice las funciones de filtrado y clasificación (pág. 319) de la tabla de políticas para encontrarlas y examinarlas con facilidad.

## Estados de implementación de la política de copias de seguridad.

Un estado de implementación de una política de copias de seguridad es una combinación de los estados de implementación de la política en cada uno de los equipos en los que se aplica esa política. Por ejemplo, si una política se aplica en tres equipos y el 1.º equipo se encuentra en el estado "Implementación", el 2.º en el estado "Actualizando" y el 3.º en "Implementada", el estado de esa política será "Implementando, Actualizando, Implementado".

Un estado de una política de copias de seguridad en un grupo de equipos es una combinación de los estados de implementación de la política de los equipos incluidos en el grupo.

Para obtener una información más completa acerca de los estados de implementación de las políticas de copias de seguridad, consulte la sección Estado y estatus de las políticas de copias de seguridad (pág. 65).

## Estatus de la política de copias de seguridad

Un estado de una política de copias de seguridad es una combinación de los estatus de los equipos en los que se aplica dicha política. Por ejemplo, si una política se aplica en tres equipos y el estado del 1.º equipo es "OK", el del 2.º "Advertencia" y el del 3.º "Error", el estado de esa política será "Error".

El estado de la política de copias de seguridad en un grupo de equipos es el estado acumulado de cada uno de los estatus de los equipos del grupo.

La siguiente tabla muestra un resumen de los posibles estatus de las políticas de copias de seguridad.

| | Estado | Cómo se determina | Cómo manejarlo |
|---|---|---|---|
| 1 | **Error** | El estado de la política en alguno de los equipos es "Error".<br><br>En caso contrario, consulte el punto 2. | Vea el registro o identifique las tareas que han fallado para averiguar la causa y a continuación, realice al menos una de estas cosas:<br>▪ Elimine la causa del fallo -> [opcionalmente] Inicie la tarea fallida manualmente<br>▪ Edite la política de copias de seguridad para evitar el mismo fallo en el futuro |

| | | | |
|---|---|---|---|
| 2 | **Advertencia** | El estado de la política en alguno de los equipos es "Advertencia".<br>En caso contrario, vea el punto 3. | Vea el registro para leer las advertencias- [opcionalmente] realice las acciones para evitar las mismas advertencias o fallos en el futuro. |
| 3 | **OK** | El estado de la política en todos los equipos es "OK". | No se necesita tomar ninguna medida. Tenga en cuenta que si una política de copias de seguridad no se aplica en ningún equipo, su estado también es "OK". |

### Qué hacer si una política se encuentra en el estado Error

1. Para averiguar la causa del fallo, realice al menos una de las siguientes cosas:
   - Haga clic en el hipervínculo **Error** para ver la entrada del registro del último error ocurrido.
   - Seleccione la política y haga clic en **Ver tareas**. Compruebe las tareas cuyo último resultado ha sido **Fallida**: seleccione una tarea y haga clic en **Ver registro**. Seleccione una entrada del registro y haga clic en **Ver detalles**. Este enfoque resulta muy útil si el estado de la política es Implementado, es decir, si las tareas de la política ya existen en los equipos gestionados.
   - Seleccione la política y haga clic en **Ver registro**. Compruebe las entradas de "error" del registro para determinar la causa del fallo: seleccione una entrada del registro y haga clic en **Ver detalles**. Este enfoque resulta muy útil si se han detectado errores en la política mientras esta se ha implementado, revocado o actualizado.

   *En la vista **Tareas**, utilice el filtro **Último resultado- Fallido** si se muestran demasiadas tareas. También puede ordenar las tareas fallidas por planes de copias de seguridad o por equipos.*

   *En la vista **Registro**, utilice el filtro Error si se muestran demasiadas entradas del registro. También puede ordenar las entradas de "error" por planes de copia de seguridad, entidades gestionadas o equipos.*
2. Una vez que la causa del fallo está clara, realice al menos una de las siguientes cosas:
   - Elimine la causa del fallo. Después de esto, puede que desee ejecutar la tarea fallida manualmente para conservar la consistencia del esquema de copia de seguridad, por ejemplo, si la política utiliza los esquemas GFS o Torres de Hanói.
   - Edite la política de copias de seguridad para evitar el mismo fallo en el futuro.

*Utilice la sección **Actividades** del Tablero para acceder rápidamente a las entradas de "error" del registro.*

### Qué hacer si una política se encuentra en el estado Advertencia

1. Para averiguar la causa de la advertencia, realice al menos una de las siguientes cosas:
   - Haga clic en el hipervínculo **Advertencia** para ver la entrada del registro de la última advertencia.
   - Seleccione la política y haga clic en **Ver tareas**. Compruebe las tareas cuyo último resultado ha sido **Completada correctamente con advertencias**: seleccione una tarea y haga clic en **Ver registro**. Este enfoque resulta muy útil si el estado de la política es Implementado, es decir, si las tareas de la política ya existen en los equipos gestionados.
   - Seleccione la política y haga clic en **Ver registro**. Compruebe las entradas de "advertencia" del registro para determinar la causa de las advertencias: seleccione una entrada del registro y haga clic en **Ver detalles**. Este enfoque resulta muy útil si se han detectado advertencias en la política mientras esta se ha implementado, revocado o actualizado.

   *En la vista **Tareas**, utilice el filtro **Último resultado- Completada correctamente con advertencias** si se muestran demasiadas tareas. También puede ordenar las tareas completadas correctamente con advertencias por planes de copias de seguridad o por equipos.*

*En la vista **Registro**, utilice el filtro Advertencia ⚠ si se muestran demasiadas entradas del registro. También puede ordenar las entradas de "advertencia" por planes de copia de seguridad, entidades gestionadas o equipos.*

2. Una vez que la causa de la advertencia está clara, puede que desee realizar acciones para evitar las mismas advertencias o fallos en el futuro.

*Utilice la sección **Actividades** del Tablero para acceder rápidamente a las entradas de "advertencia" del registro.*

### Qué hacer si una política se encuentra en el estado OK

No se necesita tomar ninguna medida.

## Acciones en políticas de copia de seguridad

Todas las operaciones descritas a continuación se llevan a cabo al hacer clic en los elementos correspondientes en la **barra de herramientas** de tareas. Las operaciones pueden llevarse a cabo también utilizando el menú contextual (haciendo clic con el botón derecho en la política de copias de seguridad seleccionada) o utilizando la barra **Acciones de "nombre de política de copias de seguridad"** o el panel **Acciones y herramientas**.

A continuación, se muestra una guía para llevar a cabo operaciones con las políticas de copias de seguridad.

| Operación | Procedimiento |
|---|---|
| Crear una política de copias de seguridad. | Haga clic en **Crear política de copias de seguridad**.<br>El procedimiento de creación de una política de copias de seguridad se describe en profundidad en la sección Crear política de copias de seguridad (pág. 377). |
| Aplicar la política a equipos o grupos | Haga clic en **Aplicar a**.<br>En la ventana Selección de equipos (pág. 319), especifique los equipos (grupos) en los que se aplicará la política de copias de seguridad seleccionada. Si el equipo se encuentra actualmente desconectado, la política se implementará en cuanto el equipo vuelva a conectarse. |
| Editar una política | Haga clic en **Editar**.<br>La edición de las políticas se lleva a cabo de la misma manera que la creación (pág. 377). Una vez que la política se ha editado, el servidor de gestión actualizará la política en todos los equipos en los que se había implementado esa política. |
| Eliminar una política | Haga clic en **Eliminar**.<br>De esta manera, se revoca la política de los equipos en los que se había implementado y se elimina del servidor de gestión. Si el equipo se encuentra actualmente desconectado, la política se revocará en cuanto el equipo vuelva a conectarse. |
| Ver información detallada sobre una política o revocar una política | Haga clic en **Ver detalles**.<br>En la ventana Detalles de la política (pág. 320), examine la información de la política seleccionada. Desde ahí, también es posible revocar la política de los equipos o grupos en los que se aplica. |
| Ver las tareas de una política | Haga clic en **Ver tareas**.<br>La vista Tareas (pág. 347) mostrará una lista de las entradas del registro relacionadas con la política seleccionada. |

| | |
|---|---|
| Ver el registro de una política | Haga clic en **Ver registro**.<br>La vista Registro (pág. 349) mostrará una lista de las entradas del registro relacionadas con la política seleccionada. |
| Actualizar una lista de políticas | Haga clic en **Actualizar**.<br>La consola de gestión actualizará la lista de políticas de copias de seguridad del servidor de gestión con la información más reciente. Aunque la lista de políticas se actualiza automáticamente en función de los eventos, es posible que los datos no se puedan recuperar inmediatamente del servidor de gestión debido a un tiempo de latencia. La actualización manual garantiza la visualización de los datos más recientes. |

## Selección de equipos

***Para aplicar la política de copias de seguridad a equipos o grupos de equipos***

1. Elija en qué equipos aplicar la política de copias de seguridad seleccionada
   - **Grupos**

     En el árbol de grupos, seleccione el equipo o los equipos en los que se aplicará la política. La lista de los equipos del grupo seleccionado se muestra en la parte derecha de la ventana.
   - **Equipos individuales**

     En el árbol de grupos, seleccione el grupo que desee. Después, en la parte derecha de la ventana, seleccione los equipos en los que desea aplicar la política de copias de seguridad.
2. Haga clic en **Aceptar**.

Acronis Backup & Recovery 10 Management Server implementará la política en los equipos seleccionados y en los equipos pertenecientes a los grupos seleccionados.

## Filtrado y clasificación de las políticas de copia de seguridad

A continuación, se muestra una guía para filtrar y ordenar las políticas de copias de seguridad.

| Para | Realizar |
|---|---|
| Ordenar las políticas de copia de seguridad por alguna de las columnas | Haga clic en el encabezado de la columna para ordenar las políticas de copia de seguridad por orden ascendente.<br>Haga clic de nuevo para ordenar las políticas de copia de seguridad por orden descendente. |
| Filtrar las políticas de copia de seguridad por nombre/propietario | Escriba un nombre de la política o del propietario en los campos debajo de los encabezados de las columnas correspondientes.<br>De esta manera, verá la lista de las políticas de copias de seguridad cuyos nombres (o nombres de sus propietario) coinciden total o parcialmente con el valor introducido. |
| Filtrar las políticas de copia de seguridad por estado de implementación, estado, tipo de origen, último resultado o programación | En el campo situado debajo del encabezado correspondiente, seleccione el valor que desee de la lista. |

### Configuración de la tabla de políticas de copia de seguridad

De manera predeterminada, la tabla que se muestra se compone de siete columnas, las demás se encuentran ocultas. Puede adecuar la presentación de las columnas según sus necesidades o preferencias.

***Mostrar u ocultar columnas***

1. Haga clic con el botón derecho en el encabezado de cualquier columna para abrir el menú contextual. Los elementos del menú que no estén seleccionados corresponden a los encabezados de las columnas presentadas en la tabla.
2. Haga clic sobre los elementos que quiera mostrar/ocultar.

## Detalles de la política

La ventana **Detalles de la política** acumula en cinco pestañas toda la información de la política de copias de seguridad seleccionada y le permite realizar operaciones con los equipos y los grupos de equipos en los que se aplica dicha política.

Esta información se encuentra también en el panel **Información**.

### Política de copias de seguridad

Esta pestaña muestra información sobre la política seleccionada.

### Origen

Esta pestaña muestra información sobre el tipo de origen sobre el que se realizará la copia de seguridad y las reglas de selección de origen.

### Destino

Esta pestaña muestra información sobre el destino de la copia de seguridad.

### Configuraciones

Esta pestaña muestra información sobre el esquema de copias de seguridad que usa la política y las opciones de copia de seguridad que se modificaron a partir de las configuraciones predeterminadas.

### Aplicado a

Esta pestaña muestra la lista de los equipos o grupos en los que se aplica la política.

**Acciones**

| Para | Realizar |
|---|---|
| Ver información detallada del equipo o grupo. | Haga clic en **Ver detalles**.<br>En la ventana Detalles del equipo (pág. 328)/Detalles del grupo (pág. 337), examine toda la información relacionada con el equipo o grupo seleccionado. |
| Ver información detallada de las tareas. | Haga clic en **Ver tareas**.<br>La vista Tareas (pág. 347) mostrará una lista de las tareas prefiltradas por el equipo o grupo de equipos seleccionado. |
| Ver registro del equipo o grupo. | Haga clic en **Ver registro**.<br>La vista Registro (pág. 349) mostrará una lista de las entradas del registro prefiltradas por el equipo o grupo de equipos seleccionado. |
| Revocar la política de un equipo o grupo. | Haga clic en **Revocar**.<br>El servidor de gestión revocará la política del equipo o grupo de equipos seleccionado. Sin embargo, la política misma permanece en el servidor de gestión. |

### 7.1.3 Equipos físicos

Acronis Backup & Recovery 10 le permite al administrador proteger datos y realizar operaciones de gestión en diferentes equipos. El administrador agrega un equipo a un servidor de gestión usando el nombre del equipo o la dirección IP, importa los equipos de Active Directory o de archivos de texto. Una vez que un equipo está registrado (pág. 412) en el servidor de gestión, pasa a estar disponible para agrupar, aplicar políticas de copia de seguridad y verificar actividades relacionadas con la protección de datos.

Para estimar si los datos se protegieron correctamente en un equipo gestionado, el administrador del servidor de gestión comprueba su estado. El estado de un equipo se define como el estado de mayor gravedad de todos los planes de copias de seguridad (pág. 193) (tanto locales como centralizados) que existen en el equipo y todas las políticas de copia de seguridad (pág. 316) aplicadas a ella. Puede ser "Correcto", "Advertencias" o "Errores".

#### Grupos

El administrador del servidor de gestión posee la capacidad de agrupar los equipos. Cada equipo puede ser miembro de más de un grupo. Dentro de los grupos creados por el administrador se pueden crear uno o más grupos anidados.

La creación de grupos ayuda a organizar la protección de datos por parte de los departamentos de la empresa, los dominios de Active Directory y las unidades organizativas.

El objetivo principal de la creación de grupos es la protección de varios equipos con una sola política. Una vez que un equipo aparece en un grupo, la política aplicada al grupo se aplica también al equipo y esta política crea las nuevas tareas en dicho equipo. Al eliminar un equipo de un grupo, la política aplicada al grupo se revoca y las tareas creadas por dicha política quedan sin efecto.

**Grupo integrado**: grupo siempre presente en un servidor de gestión. El grupo no se puede eliminar ni se puede modificar su nombre. Los grupos integrados no pueden incluir grupos anidados. Se puede aplicar una política de copia de seguridad en un grupo integrado. Un ejemplo de un grupo integrado es el grupo **Todos los equipos físicos**, el cual incluye a todas los equipos registrados en el servidor de gestión.

**Grupos personalizados**: grupos creados manualmente por el administrador del servidor de gestión.

- *Grupos estáticos*

  Los grupos estáticos incluyen equipos añadidos manualmente por el administrador. Cada miembro estático permanece en el grupo hasta que el administrador extrae al miembro del grupo o elimina el equipo gestionado correspondiente del servidor de gestión.

- *Grupos dinámicos*

  Los grupos dinámicos contienen equipos añadidos automáticamente de acuerdo con los criterios especificados por el administrador. Una vez que se han especificado los criterios, el servidor de gestión comienza a analizar las propiedades de los equipos existentes y analiza cada nuevo equipo que se registra. El equipo que cumpla con un determinado criterio dinámico aparecerá en todos los grupos que utilicen dicho criterio.

Para obtener más información sobre la agrupación de equipos, consulte la sección Agrupación de los equipos registrados (pág. 60).

Para obtener más información sobre la aplicación de las políticas a los equipos y a los grupos, consulte la sección de Políticas de equipos y grupos (pág. 61).

### Modo de trabajo con equipos

- Primero, añada los equipos al servidor de gestión Para acceder a las acciones de adición, seleccione la vista **Equipos físicos** o el grupo **Todos los equipos físicos** en el árbol de **navegación**.
- Seleccione el grupo en el que se encuentra el equipo, después seleccione el equipo.
- Utilice los botones de la **barra de herramientas** para llevar a cabo acciones en el equipo (pág. 324).
- Utilice las pestañas del panel **Información** para ver información detallada sobre el equipo seleccionado y realizar operaciones adicionales como, por ejemplo, tareas de inicio/detención, revocar la política, explorar la herencia de las políticas, etc. De manera predeterminada, el panel se encuentra minimizado. Para expandir el panel, haga clic en la flecha tipo . El contenido del panel también se puede encontrar en la ventana **Detalles del equipo** (pág. 328).
- Utilice las funciones de filtrado y clasificación (pág. 333) para encontrar y examinar con facilidad los equipos en cuestión.

### Modo de trabajo con grupos

- En la vista **Equipo físico**, seleccione el grupo.
- Utilice los botones de la barra de herramientas para realizar acciones en el grupo seleccionado (pág. 333).
- Utilice las pestañas del panel **Información** para ver información detallada sobre el grupo seleccionado y realizar operaciones adicionales como, por ejemplo, revocar políticas o explorar la herencia de las políticas. De manera predeterminada, el panel se encuentra minimizado. Para expandir el panel, haga clic en la flecha tipo . El contenido del panel también se puede encontrar en la ventana **Detalles del grupo** (pág. 337).

## Acciones sobre equipos

### Cómo registrar equipos en el servidor de gestión

Una vez que el equipo se agrega o importa al grupo **Todos los equipos físicos**, queda registrado en el servidor de gestión. Los equipos registrados se encuentran disponibles para la implementación de políticas de copia de seguridad y para la realización de otras operaciones de gestión centralizadas. El registro ofrece una relación confiable entre el agente, que reside en el equipo, y el servidor de gestión.

Para acceder a las acciones de adición e importación, seleccione la vista **Equipos físicos** o el grupo **Todos los equipos físicos** en el árbol de navegación.

| Operación | Procedimiento |
|---|---|
| Agregar un nuevo equipo al servidor de gestión | Haga clic en **Agregar un equipo al servidor de gestión de Acronis**.<br>En la ventana **Agregar equipo** (pág. 324), seleccione el equipo que debe agregarse al servidor de gestión. |
| Importar equipos desde Active Directory | Haga clic en **Importar equipos desde Active Directory**.<br>En la ventana **Importar equipos desde Active Directory** (pág. 325), especifique los equipos o las unidades organizativas cuyos equipos debe importar al servidor de gestión. |
| Importar equipos desde | Haga clic en **Importar equipos desde archivo**. |

| | |
|---|---|
| un archivo de texto | En la ventana **Importar equipos desde archivo** (pág. 327), busque un archivo .txt o .csv que contenga los nombres (o las direcciones IP) de los equipos que se deben importar al servidor de gestión. |

La consola de gestión se dirige al agente e inicia el procedimiento de registro. Debido a que el registro exige la participación del agente, no puede llevarse a cabo cuando el equipo está fuera de línea.

Un agente adicional instalado en un equipo registrado se registra automáticamente en el mismo servidor de gestión. Varios agentes se registran y se eliminan del registro de forma conjunta.

### Aplicación de las políticas

| Operación | Procedimiento |
|---|---|
| Aplicar una política de copia de seguridad a un equipo | Haga clic en **Aplicar política de copia de seguridad**.<br>En la ventana **Selección de política**, especifique la política de copia de seguridad que debe aplicar al equipo seleccionado. |

### Acciones de agrupación

| Operación | Procedimiento |
|---|---|
| Crear un grupo estático o dinámico personalizado | Haga clic en **Crear grupo**.<br>En la ventana **Crear grupo** (pág. 334), especifique los parámetros necesarios del grupo. Se creará un nuevo grupo en el grupo del cual el equipo seleccionado forma parte (excepto para el grupo integrado **Todos los equipos físicos**). |
| Agregar un equipo a otro grupo estático | Haga clic en **Agregar a otro grupo**.<br>En la ventana **Agregar al grupo** (pág. 327), especifique el grupo en el cual desea copiar el equipo seleccionado. En el equipo se implementarán las políticas de copia de seguridad aplicadas a los grupos de los cuales el equipo es miembro. |
| **Para los equipos de grupos personalizados** | |
| Agregar equipos a un grupo estático | Haga clic en **Agregar equipos al grupo**.<br>En la ventana **Agregar equipos al grupo** (pág. 328), seleccione los equipos que debe agregar. |
| Mover un equipo a otro grupo estático | Haga clic en **Mover a otro grupo**.<br>En la ventana **Mover al grupo** (pág. 327), seleccione el grupo al cual desea mover el equipo.<br>Todas las políticas de copia de seguridad aplicadas al grupo en el que se encontraba el equipo se revocarán. En el equipo se implementarán las políticas de copia de seguridad aplicadas al grupo del cual ahora forma parte el equipo. |
| Quitar un equipo del grupo estático actual | Haga clic en **Quitar del grupo**.<br>Las políticas de copia de seguridad aplicadas al grupo se revocarán automáticamente del equipo. |

### Eliminación del equipo seleccionado del servidor de gestión

| Operación | Procedimiento |
|---|---|
| Eliminar un equipo del | Haga clic en **Eliminar equipo del servidor de gestión de Acronis**. |

| | |
|---|---|
| servidor de gestión | Como resultado, las políticas de copia de seguridad se revocarán y los accesos directos a las bóvedas centralizadas se eliminarán del equipo. Si el equipo no se encuentra disponible en ese momento, estas acciones se llevarán a cabo tan pronto como el equipo esté disponible para el servidor de gestión. |

### Otras acciones

| **Operaciones de gestión directa** | |
|---|---|
| Crear un plan de copias de seguridad en un equipo | Haga clic en **Copia de seguridad**.<br>Esta operación se describe en detalle en la sección Creación de un plan de copias de seguridad (pág. 207). |
| Recuperar datos | Haga clic en **Recuperar**.<br>Esta operación se describe en detalle en la sección Recuperación de datos. |
| Establecer una conexión directa con un equipo | Haga clic en **Conectar directamente.**<br>Se establece una conexión directa con el equipo gestionado. Permite administrar un equipo gestionado y llevar a cabo todas las operaciones de gestión directa. |
| **Otras operaciones** | |
| Ver información detallada sobre un equipo | Haga clic en **Ver detalles**.<br>En la ventana **Detalles del equipo** (pág. 328), examine la información sobre el equipo. |
| Ver las tareas existentes en un equipo | Haga clic en **Ver tareas**.<br>La vista **Tareas** (pág. 347) mostrará una lista de las tareas existentes en el equipo. |
| Ver las entradas del registro de un equipo | Haga clic en **Ver registro**.<br>La vista **Registro** (pág. 349) mostrará una lista de las entradas de registro del equipo. |
| Actualice toda la información relacionada con el equipo | Haga clic en **Sincronizar**.<br>El management server consultará al equipo y actualizará la base de datos con la información más reciente. Junto con la sincronización se realizará la operación de actualización automáticamente para restaurar la lista de equipos. |
| Actualizar una lista de equipos | Haga clic en **Actualizar**.<br>La consola de gestión actualizará la lista de los equipos desde el servidor de gestión con la información más reciente. Aunque la lista de equipos se actualiza automáticamente en función de los eventos, es posible que los datos no se puedan recuperar inmediatamente del servidor de gestión debido a un tiempo de latencia. La actualización manual garantiza la visualización de los datos más recientes. |

## Incorporación de un equipo en el servidor de gestión

Para poder implementar políticas de copia de seguridad desde Acronis Backup & Recovery 10 Management Server a un equipo gestionado y llevar a cabo otras operaciones de gestión centralizada, debe registrar el equipo en el servidor de gestión.

***Para añadir un equipo***

1. En el árbol de **Navegación**, seleccione **Equipos físicos**.
2. Haga clic en **Añadir equipo a AMS** en la barra de herramientas.

3. En el campo **IP/Nombre**, ingrese el nombre del equipo o la dirección IP, o haga clic en **Examinar...** y busque la red del equipo.

   ***Nota para los usuarios de Virtual Edition:*** *Al añadir un servidor VMware ESX/ESXi, introduzca la dirección IP de la aplicación virtual que está ejecutando el agente de Acronis Backup & Recovery 10 para ESX/ESXi.*

4. Especifique el nombre de usuario y contraseña de un usuario que sea miembro del grupo de **Administradores** del equipo.

   ***Nota para los usuarios de Virtual Edition:*** *Al añadir un servidor VMware ESX/ESXi, especifique el nombre de usuario y contraseña de su servidor vCenter o ESX/ESXi.*

   Haga clic en **Opciones>>** y especifique:

   - **Nombre de usuario**. Cuando ingrese el nombre de la cuenta de un usuario de Active Directory, asegúrese de especificar el nombre de dominio (DOMINIO\Nombreusuario).
   - **Contraseña**. La contraseña de la cuenta.

   Seleccione la casilla de verificación **Guardar contraseña** para almacenar la contraseña para futuras conexiones.

5. Haga clic en **Aceptar**.

### Iniciación del registro en el lado del equipo

El procedimiento de registro puede iniciarse en el equipo.

1. Conecte la consola al equipo en el que está instalado el agente de Acronis Backup & Recovery 10. Si se le solicitan credenciales, especifique las credenciales de un miembro del grupo de **Administradores** del equipo.
2. Seleccione del menú **Opciones** > **Opciones del equipo** > **Gestión del equipo**.
3. Seleccione **Gestión centralizada** y especifique el servidor de gestión donde se registrará el equipo. Consulte "Gestión del equipo (pág. 91)" para más detalles.

## Importación de equipos desde Active Directory

***Para importar equipos desde Active Directory***

1. En el árbol de **Navegación**, seleccione **Equipos físicos** o **Todos los equipos físicos**.
2. Haga clic en **Importar equipos desde Active Directory** en la barra de herramientas.
3. En el campo **Buscar**, ingrese el nombre del equipo (o de la unidad organizativa) y después haga clic en **Buscar**. Puede utilizar el asterisco (*) como sustituto del cero o más caracteres en un nombre de un equipo (u otra unidad organizacional).

   La parte izquierda de la ventana muestra el equipo (o unidad organizacional) que coinciden completa o parcialmente con el valor ingresado. Haga clic en el elemento que desea agregar para importar y después haga clic en **Agregar>>.** El elemento se moverá a la parte derecha de la ventana. Para agregar todos los elementos encontrados, haga clic en **Agregar todo>>**.

   *Si se encuentran más de 1000 coincidencias, solo se mostrarán los primeros 1000 elementos. En este caso, se recomienda que refine su búsqueda y lo intente nuevamente.*

   La parte derecha de la ventana muestra los elementos que seleccionó para importar. Si fuera necesario, elimine los elementos seleccionados de forma errónea al utilizar los correspondientes botones **Eliminar** y **Eliminar todo**.

4. Haga clic en **Aceptar** para iniciar la importación.

## Sincronización de equipos con un archivo de texto

Durante la sincronización, el servidor de gestión ajusta el grupo **Todos los equipos físicos** de acuerdo con la lista de equipos proporcionada en un archivo .txt o .csv. El servidor de gestión:

- Añade equipos que están presentes en la lista pero que no están registrados
- Elimina los equipos registrados que no están presentes en la lista
- Elimina y luego intenta añadir equipos registrados que están presentes en la lista nuevamente, pero su disponibilidad (pág. 328) actual es **Retirado**.

Como resultado, solo esos equipos físicos que están en la lista en el archivo estarán presentes en el grupo **Todos los equipos físicos**.

### Requisitos del archivo de texto

El archivo debe contener los nombres o las direcciones IP de los equipos, un equipo por línea.

Ejemplo:

```
Nombre_equipo_1
Nombre_equipo_2
192.168.1.14
192.168.1.15
```

La especificación de un archivo vacío provoca la eliminación de todos los equipos físicos del servidor de gestión.

*Un equipo registrado debe especificarse por su dirección de registro, es decir, debe proporcionar exactamente el mismo nombre de servidor, el nombre de dominio completamente cualificado (FQDN) o la dirección IP que se especificó cuando el equipo se añadió originalmente al servidor de gestión. De lo contrario, el equipo se eliminará y se añadirá nuevamente como si fuera otro equipo. Esto significa que todas las políticas, tanto heredadas como aplicadas directamente, se revocarán del equipo y su membresía de grupo estático se perderá.*

La dirección de registro de cada equipo puede encontrarse en la columna **Dirección de registro** en cualquier vista del servidor de gestión que contenga el equipo (la columna está oculta de manera predeterminada).

Para evitar una discrepancia, puede importar inicialmente los equipos desde un archivo de texto. Modifique este archivo más adelante según sea necesario al añadir o quitar equipos, pero no cambie los nombres/direcciones de los equipos que tienen que permanecer registrados.

#### *Para sincronizar los equipos con un archivo de texto*

1. En el árbol de **Navegación**, seleccione **Equipos físicos** o **Todos los equipos físicos**.
2. Haga clic en **Sincronizar los equipos con un archivo de texto** en la barra de herramientas.
3. En el campo **Ruta**, introduzca la ruta al archivo .txt o .csv que contiene la lista de equipos o haga clic en **Examinar** y seleccione el archivo en la ventana **Examinar**.
4. En **Configuración de inicio de sesión**, especifique el nombre y contraseña del usuario que es miembro del grupo de Administradores en todos los equipos de la lista del archivo.
5. Haga clic en **Aceptar** para comenzar a sincronizar los equipos.

### Herramienta de línea de comandos de sincronización

Acronis Backup & Recovery 10 Management Server cuenta con una herramienta de línea de comandos que le permite crear un archivo por lotes y programar la tarea de sincronización con el programador de Windows.

***Para sincronizar los equipos con un archivo de texto a través de la línea de comandos***

1. Inicie la sesión como miembro del grupo de seguridad de **Acronis Centralized Admins**.
2. En la entrada de comandos, cambie el directorio a la carpeta en la que se ha instalado Acronis Backup & Recovery 10 Management Server de manera predeterminada: **C:\Archivos de programa\Acronis\AMS**.
3. Ejecute el siguiente comando:

   ```
   syncmachines [ruta_al_archivo] {nombre de usuario contraseña}
   ```

   donde:

   - [ruta_al_archivo] es la ruta de un archivo .txt o .csv que contiene la lista de equipos. La herramienta no acepta espacios en el nombre de la ruta.
   - {nombre de usuario contraseña} pertenece a un usuario que es miembro del grupo de Administradores en todos los equipos enumerados en el archivo. Si no se especifica, se utiliza el mecanismo de inicio de sesión único para operar en todos los equipos.

## Importar equipos desde un archivo de texto

***Para importar equipos desde un archivo de texto***

1. En el árbol de **Navegación**, seleccione **Equipos físicos** o **Todos los equipos físicos**.
2. Haga clic en **Importar equipos desde archivo** en la barra de herramientas.
3. En el campo **Ruta**, introduzca una ruta al archivo .txt o .csv o haga clic en **Examinar** y seleccione el archivo en la ventana **Examinar**.

   El archivo .txt o .csv debe contener los nombres de los equipos o sus direcciones IP a partir de una línea nueva para cada equipo.

   Ejemplo:

   ```
   Nombre_equipo_1
   Nombre_equipo_2
   192.168.1.14
   192.168.1.15
   ```
4. En **Configuraciones de inicio de sesión**, especifique el nombre de y contraseña del usuario que es miembro del grupo de Administradores en todos los equipos que aparecen en la lista del archivo.
5. Haga clic en **Aceptar** para iniciar la importación.

## Incorporación de un equipo en otro grupo

***Para agregar el equipo seleccionado a otro grupo***

1. Seleccione el grupo al cual se agregará el equipo.
2. Haga clic en **Aceptar**.

El equipo que se está agregando será miembro de más de un grupo. Como resultado, las políticas de copia de seguridad aplicadas al primer grupo permanecerán en el equipo y las políticas de copia de seguridad aplicadas al grupo segundo, tercero, etc. se implementarán en el equipo.

## Mover un equipo a otro grupo

***Para mover el equipo seleccionado a otro grupo***

1. En el árbol de grupos, seleccione el grupo al que se moverá el equipo.
2. Haga clic en **Aceptar**.

El equipo que se está moviendo deja un grupo para ser miembro de otro grupo. Como resultado, las políticas de copia de seguridad aplicadas al primer grupo se revocarán del equipo y las políticas de copia de seguridad aplicadas al segundo grupo se implementarán en el equipo.

## Incorporación de equipos en un grupo

***Para agregar equipos al grupo seleccionado***

1. En el árbol de grupos, seleccione los grupos cuyos equipos debe agregar.
2. En la la parte derecha de la ventana, seleccione los equipos.
3. Para agregar más equipos desde otros grupos, repita los pasos 1 y 2 para cada grupo.
4. Haga clic en **Aceptar** para agregar los equipos.

Una vez que los equipos aparecen en el grupo, la política que se aplicó al grupo (si hubiera) se implementa en los equipos. Si alguno de los equipos seleccionados no está disponible o no se puede acceder a él en ese momento, la acción se mantendrá pendiente en el servidor de gestión y se llevará a cabo tan pronto como el equipo esté disponible en el servidor.

## Detalles del equipo

Recoge en cuatro pestañas toda la información sobre el equipo seleccionado. Deje que el administrador del servidor de gestión realice todas las operaciones con los planes y tareas de copia de seguridad que existen en el equipo, y las políticas aplicadas al equipo.

Esta información se encuentra también en el panel **Información**.

### Equipo

La pestaña muestra la siguiente información sobre el equipo registrado:

- **Nombre**: nombre del equipo seleccionado (tomado del **Nombre del equipo** en Windows).
- **Dirección IP**: dirección IP del equipo seleccionado.
- **Estatus**: el estatus del equipo. Se determina en función del estatus (pág. 194) de mayor gravedad de todos los planes de copias de seguridad (tanto locales como centralizados) que existen en el equipo y las políticas de copia de seguridad (pág. 316) aplicadas a ella.
- **Última conexión**: tiempo transcurrido desde la última conexión del servidor de gestión al equipo.
- **Última copia de seguridad correcta**: tiempo transcurrido desde la última copia de seguridad realizada correctamente.
- **Disponibilidad:**
  - **En línea**: el equipo se encuentra disponible para el servidor de gestión. Esto significa que la última conexión del servidor de gestión al equipo se realizó correctamente. La conexión se establece cada 2 minutos.
  - **Fuera de línea**: el equipo no se encuentra disponible para el servidor de gestión: está apagada o el cable de red está desconectado.
  - **Desconocido**: este estatus se muestra hasta que se establece la primera conexión entre el servidor de gestión y el equipo, después de agregar el equipo o de iniciar el servicio del servidor de gestión.
  - **Retirado**: el equipo se registró en otro servidor de gestión o se seleccionó el parámetro **Gestión autónoma** en **Opciones > Opciones del equipo > Gestión del equipo** (pág. 91). Como resultado, no es posible controlar el equipo desde el servidor de gestión actual. Sin embargo, puede recuperar el control del equipo si especifica la dirección del servidor de gestión en la configuración de **Gestión del equipo**.

- **Caducado**: la versión de prueba del agente del equipo ha caducado. Para especificar una clave de licencia completa, utilice la función **Cambiar licencia** o ejecute el programa de instalación y siga las instrucciones.

- **Agentes instalados**: nombre completo de los agentes de Acronis instalados en el equipo.
- **Sistema operativo**: el sistema operativo que ejecuta el agente del equipo.
- **Procesador**: el tipo de CPU utilizado en el equipo gestionado
- **Reloj del CPU**: frecuencia del reloj de la CPU
- **RAM**: tamaño de la memoria
- **Comentarios**: descripción del equipo (tomada de **Descripción del equipo** en Windows)

### Políticas de copia de seguridad

Muestra una lista de las políticas de copia de seguridad aplicadas al equipo seleccionado y permite que el administrador del servidor de gestión realice las siguientes operaciones:

| Para | Procedimiento |
|---|---|
| Ver los detalles de una política | Haga clic en **Ver detalles**.<br>En la ventana **Detalles de la política** (pág. 320), examine toda la información relacionada con la política seleccionada de copia de seguridad. |
| Ver las tareas de una política | Haga clic en **Ver tareas**.<br>La vista **Tareas** (pág. 347) mostrará una lista de las tareas relacionadas con la política seleccionada de copias de seguridad. |
| Ver registro de una política | Haga clic en **Ver registro**.<br>La vista **Registro** (pág. 349) mostrará una lista de las entradas del registro relacionadas con la política de copias de seguridad seleccionada. |
| Revocar una política desde el equipo. | Haga clic en **Revocar**.<br>El servidor de gestión revocará la política desde el equipo. La política permanecerá en el servidor de gestión.<br>Si el equipo es miembro de un grupo y la política se aplica a dicho grupo, no podrá revocar la política de un solo equipo sin antes quitar el equipo del grupo. |
| Determinar el origen de la política aplicada | Haga clic en **Explorar herencia**.<br>La ventana de **Orden de herencia** (pág. 333) mostrará el orden de herencia de la política aplicada al equipo. |

#### Filtrado y clasificación

El filtrado y la clasificación de las políticas de copia de seguridad se realiza de la misma manera que en la vista **Políticas de copia de seguridad**. Consulte la sección Filtrado y clasificación de políticas de copia de seguridad (pág. 319) para obtener más información.

### Planes y tareas

Muestra una lista de los planes (tanto locales como centralizados) y de las tareas existentes en el equipo seleccionado.

#### Operaciones

A continuación se ofrece una guía para la realización de operaciones con planes y tareas de copia de seguridad.

| Operación | Procedimiento |
|---|---|
| Ver los detalles de un plan o una tarea | **Plan de copia de seguridad**<br><br>Haga clic en **Ver detalles**.<br>En la ventana de **Detalles del plan** (pág. 203), revise los detalles del plan.<br><br>**Tarea**<br><br>Haga clic en **Ver detalles**.<br>En la ventana de **Detalles de la tarea** (pág. 201), revise los detalles de la tarea. |
| Ver el registro del plan o de la tarea | **Plan de copia de seguridad**<br><br>Haga clic en **Ver registro**.<br><br>Accederá a la sección de **Registro** (pág. 204), la cual incluye la lista de las entradas de registro relacionadas con el plan.<br><br>**Tarea**<br><br>Haga clic en **Ver registro**.<br><br>Accederá a la sección de **Registro** (pág. 204), la cual incluye la lista de las entradas de registro relacionadas con la tarea. |
| Ejecutar un plan o una tarea | **Plan de copia de seguridad**<br><br>Haga clic en **Ejecutar**.<br><br>En la ventana **Ejecutar plan de copias de seguridad** (pág. 201), seleccione la tarea que debe ejecutar.<br><br>La ejecución del plan de copia de seguridad inicia inmediatamente la tarea seleccionada de dicho plan, independientemente de la programación y de las condiciones.<br><br>**Tarea**<br><br>Haga clic en **Ejecutar**.<br><br>La tarea se ejecutará inmediatamente, independientemente de la programación y de las condiciones. |
| Detener un plan o una tarea | **Plan de copia de seguridad**<br><br>Haga clic en **Detener**.<br><br>Al detener el plan de copia de seguridad en ejecución se detendrán todas las tareas. Por lo tanto, se cancelarán todas las operaciones de tareas.<br><br>**Tarea**<br><br>Haga clic en **Detener**.<br><br>*¿Qué sucede si detengo la tarea?*<br><br>Por lo general, al detener la tarea se cancela su operación (copia de seguridad, recuperación, validación, exportación, conversión, migración). La tarea pasa en primer lugar al estado Deteniendo y después al estado Inactiva. La programación de la tarea, en caso de haberla creado, aún será válida. Para completar la operación deberá ejecutar nuevamente la tarea.<br><br>▪ Tarea de recuperación (desde la copia de seguridad del disco): El volumen de destino se eliminará y el espacio quedará no asignado. También obtendrá el mismo resultado si la recuperación no se realiza correctamente. Para recuperar el volumen "perdido", deberá ejecutar la tarea una vez más.<br><br>▪ tarea de recuperación (desde la copia de seguridad de archivos): La operación cancelada |

| | |
|---|---|
| | puede ocasionar cambios en la carpeta de destino. Es posible que algunos archivos se recuperen y otros no, según el momento en que se detuvo la tarea. Para recuperar todos los archivos deberá ejecutar la tarea una vez más. |
| Editar un plan o una tarea | **Plan de copia de seguridad**<br>Haga clic en **Editar**.<br>La edición del plan de copia de seguridad se realiza de la misma manera que la creación (pág. 207), excepto por las siguientes **limitaciones**:<br>No siempre es posible cambiar las propiedades del esquema de la copia de seguridad si el archivo comprimido creado no está vacío (es decir, si contiene copias de seguridad).<br>1. No es posible cambiar el esquema a "abuelo-padre-hijo" o Torres de Hanói.<br>2. Si se utiliza el esquema de la Torres de Hanói, no es posible cambiar la cantidad de niveles.<br>En todos los demás casos, el esquema puede modificarse y debe continuar utilizándose como si los archivos comprimidos existentes se hubieran creado a partir de un esquema nuevo. En los archivos comprimidos vacíos es posible realizar cualquier tipo de cambio.<br>*¿Por qué no puedo editar el plan de copia de seguridad?*<br>▪ El plan de copia de seguridad se encuentra en ejecución en ese momento.<br>La edición del plan de copia de seguridad actualmente en ejecución no está permitida.<br>▪ El plan de copia de seguridad posee un origen centralizado.<br>La edición directa de los planes de copia de seguridad centralizados no está permitida. Debe editar la política de copia de seguridad original.<br>**Tarea**<br>Haga clic en **Editar**.<br>*¿Por qué no puedo editar la tarea?*<br>▪ La tarea pertenece a un plan de copia de seguridad.<br>Solo las tareas que no pertenecen a un plan de copia de seguridad, tales como las tareas de recuperación, pueden modificarse mediante edición directa. Cuando deba modificar una tarea que pertenece a un plan de copia de seguridad local, edite el plan de copia de seguridad. Las tareas que pertenecen a un plan de copia de seguridad centralizado se pueden modificar al editar la política centralizada que generó el plan. |
| Eliminar un plan o una tarea | **Plan de copia de seguridad**<br>Haga clic en **Eliminar**.<br>*¿Qué sucede si elimino el plan de copia de seguridad?*<br>Si se elimina el plan, se eliminarán todas sus tareas.<br>*¿Por qué no puedo eliminar el plan de copia de seguridad?*<br>▪ El plan de copia de seguridad se encuentra en el estado "En ejecución"<br>El plan de copia de seguridad no podrá eliminarse si al menos una de sus tareas se encuentra en ejecución.<br>▪ El plan de copia de seguridad posee un origen centralizado.<br>El administrador del servidor de gestión puede eliminar un plan centralizado al revocar la política de copia de seguridad que dio origen al plan.<br>**Tarea** |

| | |
|---|---|
| | Haga clic en **Eliminar**.<br>*¿Por qué no puedo eliminar la tarea?*<br>▪ La tarea pertenece a un plan de copia de seguridad.<br>La tarea que pertenece a un plan de copia de seguridad no puede eliminarse por separado del plan. Edite el plan para quitar la tarea o elimine el plan completo. |
| Actualizar la tabla | Haga clic en **Actualizar**.<br>La consola de gestión actualizará la lista de los planes y las tareas de copia de seguridad presentes en el equipo con la información más reciente. Si bien la lista se actualiza automáticamente en función de los eventos, es posible que los datos no se recuperen inmediatamente del equipo gestionado debido a un breve periodo de latencia. La actualización manual garantiza la visualización de los datos más recientes. |

**Filtrado y clasificación**

El filtrado y la clasificación de las políticas de copia de seguridad se realiza de la misma manera que en la vista **Planes y tareas de copia de seguridad** para la gestión directa. Consulte la sección Filtrar y clasificar planes y tareas de copia de seguridad (pág. 200) para obtener más información.

## Miembro de

Esta pestaña aparece solo si se agrega el equipo seleccionado a uno o más grupos personalizados y muestra una lista de los grupos de los que el equipo forma parte.

**Operaciones**

| Para | Procedimiento |
|---|---|
| Ver los detalles de un grupo | Haga clic en **Ver detalles**.<br>Accederá a la ventana Detalles del grupo, donde podrá analizar la información relacionada con este grupo. |
| Ver tareas relacionadas con un grupo | Haga clic en **Ver tareas**.<br>Accederá a la sección Tareas, con tareas previamente filtradas relacionadas con el grupo de copia de seguridad seleccionado. |
| Ver registro relacionado con un grupo | Haga clic en **Ver registro**.<br>Se abrirá la sección Registro, con las entradas de registro previamente filtradas del grupo seleccionado. |
| Quitar un equipo de un grupo. | Haga clic en **Quitar**.<br>Los planes centralizados, implementados en el grupo principal, ya no afectarán a este equipo. |

## Máquinas virtuales guardadas en el servidor

La pestaña muestra una lista de equipos guardados en el servidor de virtualización seleccionado o gestionado por el dispositivo virtual especificado.

Puede crear un grupo dinámico basado en la lista de equipos virtuales guardados. Para hacerlo, haga clic en **Crear un grupo dinámico**. El grupo creado será accesible en Vista de equipos virtuales (pág. 339).

## Orden de la herencia

La ventana de **Orden de herencia** le permite examinar de donde proviene la política aplicada al equipo.

La política que se aplicó directamente al equipo se visualiza de la siguiente forma:
**Nombre del equipo**

La política que se aplica en el equipo mediante herencia se muestra como en el siguiente ejemplo:
Grupo1 > **Grupo2** > Grupo3 > Equipo1

El *Grupo1* contiene en la raíz al *Grupo2* al que la política se aplica directamente. El *Grupo2*, a su vez, contiene al *Grupo3* secundario que hereda la política del principal y aplica la política al *Equipo1* respectivamente.

El equipo (o grupo) al que se aplicó la política directamente aparecerá en negrita y marcado con un icono.

Todos los elementos son interactivos, es decir, cuando hace clic en un equipo o grupo, la vista de su grupo padre se abrirá.

## Filtrado y clasificación de equipos

| Para | Procedimiento |
|---|---|
| Clasificar equipos por columna | Haga clic en el encabezado de la columna para clasificar los equipos en orden ascendente.<br>Haga clic una vez más para clasificar los equipos en orden descendente. |
| Filtrar los equipos por nombre. | Ingrese el nombre de un equipo en el campo debajo del encabezado de la columna correspondiente.<br>Como resultado, podrá observar la lista de equipos cuyos nombres completos o parciales coinciden con el valor ingresado. |
| Filtrar los equipos por estado, última conexión, última copia de seguridad, disponibilidad. | En el campo debajo del encabezado de la columna correspondiente, seleccione el valor apropiado de la lista. |

### Configuración de la tabla de equipos

De manera predeterminada, la tabla incluye cinco columnas que se muestran y otras que están ocultas. También puede ocultar las columnas innecesarias y mostrar las ocultas, si fuera necesario.

#### *Mostrar u ocultar columnas*

1. Haga clic con el botón derecho en el encabezado de cualquier columna para abrir el menú contextual. Los elementos del menú que no estén seleccionados corresponden a los encabezados de las columnas presentadas en la tabla.
2. Haga clic sobre los elementos que quiera mostrar/ocultar.

## Acciones sobre grupos

Para acceder a las acciones seleccione la vista **Equipos físicos** en el árbol de **Navegación** y después haga clic sobre un grupo.

La siguiente es una guía que le ayudará a llevar a cabo las acciones en los grupos seleccionados.

| Operación | Procedimiento |
|---|---|
| Crear un grupo estático o dinámico personalizado | Haga clic en **Crear grupo**.<br>En la ventana **Crear grupo** (pág. 334), especifique los parámetros necesarios del grupo.<br>Los grupos personalizados se pueden crear en la carpeta raíz (**Equipos físicos**) o en otros grupos personalizados. |
| Aplicar una política de copia de seguridad a un grupo | Haga clic en **Aplicar política de copia de seguridad**.<br>En la ventana **Selección de política**, especifique la política de copia de seguridad que debe aplicar al grupo seleccionado. Si en el grupo seleccionado existen grupos secundarios, la política de copia de seguridad también se aplicará a ellos. |
| Ver información detallada sobre un grupo | Haga clic en **Ver detalles**.<br>En la ventana **Detalles del grupo** (pág. 337), examine la información sobre el grupo seleccionado. |
| Cambie el nombre de un grupo/subgrupo personalizado | Haga clic en **Cambiar nombre**.<br>En la columna **Nombre**, ingrese un nombre nuevo para el grupo seleccionado.<br>Los nombres de los grupos integrados no pueden modificarse. |
| Editar un grupo personalizado | Haga clic en **Editar**.<br>En la ventana **Editar grupo** (pág. 336), modifique los parámetros necesarios del grupo. |
| Mover un grupo personalizado hasta otro grupo | Haga clic en **Mover a**.<br>En la ventana **Mover a grupo** (pág. 336), especifique el que será el nuevo grupo principal del grupo seleccionado. |
| Eliminar un grupo personalizado | Haga clic en **Eliminar**.<br>Si se elimina un grupo principal también se eliminarán los grupos secundarios. Las políticas de copia de seguridad aplicadas al grupo principal y heredadas por los grupos secundarios se revocarán para todos los miembros de los grupos eliminados. Las políticas aplicadas de forma directa a los miembros se conservarán. |
| Actualizar una lista de grupos | Haga clic en **Actualizar**.<br>La consola de gestión actualizará la lista de los grupos desde el servidor de gestión con la información más reciente. Aunque la lista de grupos se actualiza automáticamente en función de los eventos, es posible que los datos no se puedan recuperar inmediatamente del servidor de gestión debido a un tiempo de latencia. La actualización manual garantiza que se muestren los datos más recientes. |

## Creación de un grupo estático o dinámico personalizado

***Para crear un grupo***

1. En el campo **Nombre del grupo**, ingrese un nombre para el grupo que se está creando.
2. Elija el tipo de grupo:
   a. **Estático**: para crear un grupo que contendrá equipos agregados manualmente.
   b. **Dinámico**: para crear un grupo que contendrá equipos agregados automáticamente de acuerdo con los criterios especificados.

      Haga clic en **Agregar criterios** y seleccione el patrón del criterio.

- **Sistema operativo**

  Todas los equipos que ejecutan el sistema operativo seleccionado serán miembros del grupo dinámico.
- **Unidad organizacional** (pág. 335)

  Todos los equipos que pertenecen a la unidad organizativa (UO) especificada serán miembros del grupo dinámico.
- **Rango de dirección IP**

  Todas los equipos cuyas direcciones IP se encuentran dentro del rango IP especificado serán miembros del grupo dinámico.
- **Enumerados en el archivo txt/csv** (pág. 336)

  Todos los equipos que se enumeren en el archivo .txt o .csv especificado serán miembros del grupo dinámico.

3. En el campo **Comentarios**, ingrese una descripción del grupo creado.
4. Haga clic en **Aceptar**.

### Incorporación de varios criterios

La incorporación de varios criterios establece una condición de acuerdo con las siguientes reglas:

a) Todas las entradas de los mismos criterios se combinan por adición lógica (O).

Por ejemplo, el siguiente conjunto de criterios

| | |
|---|---|
| Sistema operativo: | Windows Server 2008 |
| Sistema operativo: | Windows Server 2003 |

agregará al mismo grupo todas los equipos cuyo sistema operativo sea Windows 2000 O Windows 2003.

b) Las entradas de los diferentes criterios se combinan por multiplicación lógica (Y)

Por ejemplo, el siguiente conjunto de criterios

| | |
|---|---|
| Sistema operativo: | Windows Server 2008 |
| Sistema operativo: | Windows Server 2003 |
| Unidad organizativa: | SERVIDORES |
| Rango IP: | 192.168.17.0 - 192.168.17.55 |

agregará al mismo grupo todos los equipos cuyo sistema operativo sea Windows 2000 o Windows 2003 y que pertenezcan a la unidad organizativa SERVIDORES, y cuyas direcciones IP se incluyan dentro del rango 192.168.17.0 - 192.168.17.55.

### ¿Durante cuánto tiempo permanece en el grupo un grupo dinámico?

El miembro de un grupo dinámico permanecerá en el grupo mientras reúna los criterios necesarios. Dicho miembro se quitará automáticamente del grupo tan pronto como

- el miembro deje de cumplir con los criterios correspondientes
- el administrador cambie los criterios de manera que el miembro ya no reúna todos los criterios

No hay manera de eliminar manualmente un equipo de una grupo dinámico, excepto por la eliminación del equipo del management server.

## Criterio de unidad organizacional

El criterio de unidad organizacional se especifica para el dominio en el que se encuentra el servidor de gestión, de la siguiente manera: *OU=OU1*

Seleccione una unidad organizacional del árbol de Active Directory al hacer clic en **Examinar** o escribirla manualmente. Si las credenciales de acceso al dominio no se especificaron en las opciones del servidor de gestión, el programa le pedirá que las proporcione. Las credenciales se guardarán en la opción Credenciales de acceso al dominio (pág. 89).

Por ejemplo, supongamos que el dominio *us.corp.example.com* tiene a OU1 (que está en la raíz), OU1 tiene a OU2 y OU2 tiene a OU3. Y usted necesita añadir los equipos de OU3. Entonces, el criterio será: *OU=OU3, OU=OU2, OU=OU1*

Si OU3 tiene contenedores secundarios y también debe añadir los equipos de aquellos contenedores al grupo, seleccione la casilla de verificación **Incluir contenedores secundarios**.

## En lista en el criterio de archivos txt/csv

Cuando utiliza este criterio, el grupo dinámico incluirá equipos de la lista proporcionada en el archivo .txt o .csv especificado.

Si modifica el archivo más tarde, el contenido del grupo cambiará según corresponda. Se verifica el archivo cada 15 minutos.

Si más tarde elimina el archivo o no se encuentra disponible, el contenido del grupo corresponderá a la lista que se almacenó por última vez en el archivo.

### Requisitos del archivo de texto

El archivo debe contener los nombres o las direcciones IP de los equipos, un equipo por línea.

Ejemplo:

```
Nombre_equipo_1
Nombre_equipo_2
192.168.1.14
192.168.1.15
```

Un equipo registrado debe especificarse por su dirección de registro, es decir, debe proporcionar exactamente el mismo nombre de servidor, el nombre de dominio completamente cualificado (FQDN) o la dirección IP que se especificó cuando el equipo se añadió originalmente al servidor de gestión. De lo contrario, el equipo no se agregará al grupo. La dirección de registro de cada equipo puede encontrarse en la columna **Dirección de registro** en cualquier vista del servidor de gestión que contenga el equipo (la columna está oculta de manera predeterminada).

## Mover un grupo a otro

***Para mover el grupo seleccionado a otro grupo o a la raíz***

1. En el árbol de grupos, haga clic en el grupo al que moverá el grupo seleccionado. Puede mover cualquier tipo de grupo personalizado (ya sea estático o dinámico) a otro grupo personalizado de cualquier tipo o a la carpeta raíz.

   La carpeta raíz del árbol de equipos contiene los *grupos del primer nivel*. Los grupos que incluyen otros grupos se denominan *grupos principales*. Los grupos que están en grupos principales se denominan *grupos secundarios*. Todas las políticas de copia de seguridad aplicadas al grupo principal también se aplicarán a los grupos secundarios
2. Haga clic en **Aceptar**.

## Edición de grupos personalizados

La edición de un grupo personalizado se realiza de la misma manera que su creación (pág. 334).

El cambio del tipo de grupo producirá su conversión. Todos los grupos personalizados pueden convertirse en grupos dinámicos y viceversa.

- Cuando convierta un grupo estático en dinámico, proporcione los criterios de agrupación. Todos los miembros que existen en el grupo estático y que no reúnan los criterios proporcionados se quitarán del grupo dinámico.
- Al convertir un grupo dinámico en estático, existen dos opciones disponibles: conservar el contenido actual del grupo o vaciarlo.

## Detalles del grupo

Reúne en dos pestañas toda la información sobre el grupo seleccionado. Permite llevar a cabo operaciones con las políticas aplicadas al grupo.

Esta información también se duplica en el panel **Información**.

### Grupo

Muestra la siguiente información sobre el grupo:

- **Nombre:** nombre del grupo seleccionado
- **Grupo principal** (solo para subgrupos): nombre del grupo principal
- **Equipos**: cantidad de equipos en el grupo
- **Tipo**: tipo de grupo (estático o dinámico)
- **Criterios** (solo para grupos dinámicos): criterios de agrupación
- **Comentarios:** descripción del grupo (si se especifica)

### Políticas de copia de seguridad

Muestra una lista de las políticas de copia de seguridad relacionadas con el grupo y permite realizar las siguientes operaciones:

| Operación | Procedimiento |
|---|---|
| Ver los detalles de una política | Haga clic en **Ver detalles**.<br>En la ventana Detalles de la política (pág. 320), examine toda la información relacionada con la política seleccionada de copia de seguridad. |
| Ver las tareas de una política | Haga clic en **Ver tareas**.<br>La vista Tareas (pág. 347) mostrará una lista de las tareas relacionadas con la política seleccionada de copias de seguridad. |
| Ver registro de una política | Haga clic en **Ver registro**.<br>La vista Registro (pág. 349) mostrará una lista de las entradas del registro relacionadas con la política de copias de seguridad seleccionada. |
| Revocar una política desde el grupo. | Haga clic en **Revocar**.<br>El servidor de gestión revoca la política desde el grupo. Mientras los cambios se transfieren a los equipos y los agentes eliminan los planes de copia de seguridad, el estado de la política del grupo es **Revocación**. La política permanece en el servidor de gestión. |
| Determinar el origen de la política aplicada al grupo | Haga clic en **Explorar herencia**.<br>La ventana de **Orden de herencia** (pág. 338) mostrará el orden de herencia de la política aplicada al grupo. |

**Filtrado y clasificación**

El filtrado y la clasificación de las políticas de copia de seguridad se realiza de la misma manera que en la vista de las políticas de copia de seguridad. Consulte la sección Filtrado y clasificación de políticas de copia de seguridad (pág. 319) para obtener más información.

### Orden de la herencia

La ventana de **Orden de herencia** le permite examinar de donde proviene la política aplicada al grupo.

La política que se aplicó directamente al grupo se visualiza de la siguiente forma:
**Nombre del grupo**

La política que se aplica en el grupo mediante herencia se muestra como en el siguiente ejemplo:
Grupo1 > **Grupo2** > Grupo3

El *Grupo1* contiene en la raíz al *Grupo2* al que la política se aplica directamente. El *Grupo2*, a su vez, contiene al *Grupo3* secundario que hereda la política del principal.

El grupo al que se aplicó la política directamente aparecerá en negrita y marcado con un icono.

Todos los elementos son interactivos, es decir, cuando hace clic en un grupo, la vista de su grupo padre se abrirá.

## 7.1.4 Máquinas Virtuales

Puede gestionar centralmente máquinas virtuales con cualquiera de los siguientes métodos o con ambos:

**Incorporación de una máquina virtual como un equipo físico**

Instale Acronis Backup & Recovery 10 Agent for Windows o Agent for Linux en el equipo virtual y regístrelo (pág. 324) en el servidor de gestión. El equipo se tratará como un equipo físico. Aparecerá debajo de **Equipos con agentes** en el grupo **Todos los equipos con agentes**.

Este enfoque es práctico cuando:

- El equipo no está alojado en un servidor de virtualización.
- No tiene una licencia para Acronis Backup & Recovery 10 Virtual Edition.
- La Virtual Edition no es compatible con la copia de seguridad a nivel de hipervisor para este producto específico de virtualización.
- Debe superar las limitaciones de la copia de seguridad a nivel del hipervisor.

**Incorporación de una máquina virtual como una máquina virtual**

En Acronis Backup & Recovery 10 Management Server, se considera que un equipo es virtual si se puede realizar una copia de seguridad del servidor de virtualización sin instalar un agente en el equipo. Esto es posible cuando se utiliza Acronis Backup & Recovery 10 Advanced Server Virtual Edition.

Existen varias formas de añadir un equipo virtual al servidor de gestión:

- Habilite la integración (pág. 90) del servidor de gestión con vCenter Server

  **Resultado.** Los equipos virtuales gestionados por vCenter Server aparecerán debajo de **Equipos virtuales** en el grupo **Todos los equipos virtuales**. Los equipos parecen como no gestionables (en

gris), pero pueden incluirse en la copia de seguridad si se habilitó la implementación automática del agente durante la integración.

- Instale y configure Agente para ESX(i) VMware vSphere (Virtual Appliance) o Agente para ESX(i) VMware vSphere (Windows). Registre el agente en el servidor de gestión.

  **Resultado.** El equipo con el agente (el dispositivo virtual en el servidor de Windows) aparece debajo de **Equipos con agentes** en el grupo **Todos los equipos con agentes**. Los equipos virtuales gestionados por el agente aparecerán debajo de **Equipos virtuales** en el grupo **Todos los equipos virtuales**.
- Instale Agente para Hyper-V en un servidor Hyper-V o en todos los nodos de un clúster de Hyper-V. Registre los agentes en el servidor de gestión.

  **Resultado.** El servidor Hyper-V (nodos) aparece debajo de **Equipos con agentes** en el grupo **Todos los equipos con agentes**. Los equipos virtuales gestionados por los agentes aparecerán debajo de **Equipos virtuales** en el grupo **Todos los equipos virtuales**.

Las máquinas virtuales añadidas al servidor de gestión como máquina virtual se encuentran debajo de **Máquinas virtuales** en el árbol de **Navegación**. Esta sección describe todas las operaciones disponibles con estos equipos.

## Máquinas virtuales en un servidor de gestión

### Disponibilidad de máquinas virtuales

Las máquinas virtuales se muestran como disponibles cuando el agente está disponible para el servidor de gestión y los equipos están disponibles para el agente. La lista de máquinas virtuales se actualiza dinámicamente cada vez que el servidor de gestión se sincroniza con los agentes.

Cuando el servidor de virtualización o la máquina virtual está no disponible o se retira, las máquinas virtuales aparecen en gris.

Cuando las máquinas virtuales no están disponibles para el agente (esto sucede cuando los equipos se quitan del inventario del servidor de virtualización, se eliminan del disco o el almacenamiento del servidor está caído o desconectado), los equipos desaparecen de los grupos **Todas las máquinas virtuales** y los demás grupos se incluyen. Las tareas que realizan la copia de seguridad de estas máquinas virtuales fallarán con un registro de errores adecuado. Como resultado, la política tendrá un estado de Error.

El estado conectado o desconectado de una máquina virtual no afecta la copia de seguridad, ya que las máquinas virtuales se pueden incorporar en la copia de seguridad en ambos estados.

### Políticas para las máquinas virtuales

Cualquier política que realice la copia de seguridad de los discos y volúmenes puede aplicarse a las máquinas virtuales así como a los equipos físicos. Las políticas que realizan una copia de seguridad de nivel de archivos no pueden aplicarse a las máquinas virtuales. Para obtener más información sobre la copia de seguridad y recuperación de máquinas virtuales, sistemas operativos invitados compatibles y configuraciones de disco, consulte "Copia de seguridad de máquinas virtuales".

#### Qué sucede cuando una política se aplica a un grupo de máquinas virtuales

Se realizará la copia de seguridad de cada equipo como tarea separada en un archivo comprimido individual. El nombre predeterminado del archivo comprimido incluirá el nombre de la máquina virtual y el nombre de la política. Es aconsejable mantener el nombre predeterminado del archivo comprimido para que pueda encontrar las copias de seguridad de cada equipo fácilmente en la bóveda de almacenamiento.

### Agrupación de máquinas virtuales

La sección **Máquinas virtuales** de este árbol de navegación contiene un grupo incorporado llamado **Todas las máquinas virtuales**. No puede modificar, eliminar ni mover manualmente este grupo. Puede aplicar políticas que realicen copias de seguridad de los discos o volúmenes a este grupo.

Puede crear grupos estáticos y dinámicos de máquinas virtuales. Cualquier máquina virtual que está actualmente disponible puede agregarse a un grupo estático. No puede crear grupos que contengan máquinas virtuales y equipos físicos.

Los criterios de membresía dinámica para las máquinas virtuales son los siguientes:

- **Tipo de servidor de virtualización (Hyper-V, ESX/ESXi).**

Con este criterio, puede crear un grupo dinámico de máquinas virtuales alojadas en servidores registrados Hyper-V (o ESX/ESXi, respectivamente). Cualquier equipo agregado a los servidores aparecerá en este grupo. Cualquier equipo eliminado de los servidores desaparecerá de este grupo.

- **Servidor/VA**

Con este criterio, puede crear un grupo dinámico de máquinas virtuales alojadas en un servidor de virtualización especificado o gestionado por el dispositivo virtual específico.

## Integración de VMware vCenter

Si utiliza VMware vSphere, es recomendable que integre el servidor de gestión en su vCenter Server.

***Para integrar el servidor de gestión con un VMware vCenter Server:***

1. En el árbol de **Navegación**, haga clic con el botón derecho en **Máquinas virtuales** y seleccione **Integración de VMware vCenter**.
2. Haga clic en **Configurar integración**
3. Seleccione la casilla de verificación **Habilitar la integración de VMware vCenter**
4. Especifique la dirección IP o el nombre de vCenter Server y proporcione las credenciales de acceso para el servidor
5. Haga clic en **Aceptar**

Como resultado, un grupo que tiene el mismo nombre que el vCenter Server aparecerá en el servidor de gestión debajo de **Máquinas virtuales**. Para más información, consulte "Integración de VMware vCenter (pág. 90)".

***Para eliminar la integración con un VMware vCenter Server:***

1. En el árbol de **Navegación**, haga clic con el botón derecho en **Máquinas virtuales** y seleccione **Integración de VMware vCenter**.
2. Haga clic en **Configurar integración**
3. Borre la casilla de verificación **Habilitar la integración de VMware vCenter**
4. Haga clic en **Aceptar**

El grupo que tenga el mismo nombre que el vCenter Server se eliminará y las políticas aplicadas a este grupo o sus grupos secundarios se revocarán.

Las máquinas virtuales permanecen en el grupo **Todas las máquinas virtuales** y en otros grupos de sus servidores gestionados por Agent para ESX/ESXi. Las políticas aplicadas a estos grupos o directamente a los equipos continuarán funcionando en los equipos. De esta manera, al eliminar la integración solo elimina los equipos que no son gestionables.

## Implementación y actualización de Agente para ESX/ESXi.

Acronis Backup & Recovery 10 Management Server proporciona una forma fácil de implementar Agent para ESX/ESXi en cada servidor VMware ESX o ESXi cuyas máquinas virtuales desea incluir en la copia de seguridad.

Se creará un dispositivo virtual con un agente en cada servidor ESX/ESXi que especifique y esté registrado en el servidor de gestión. Las máquinas virtuales, agrupadas dinámicamente por sus servidores, aparecerán en el servidor de gestión y podrá aplicar las políticas de copias de seguridad a las máquinas virtuales o realizar una copia de seguridad de cada equipo individualmente.

La actualización de agentes que ya se han instalado se realiza de la misma manera que la implementación. Al seleccionar un servidor o clúster en el que el agente está instalado, se le sugerirá que actualice el agente en ese servidor.

Si utiliza VMware vSphere, es recomendable que integre (pág. 340) el servidor de gestión en su vCenter Server antes de comenzar con la implementación del agente. En este caso, no tendrá que especificar cada servidor manualmente.

### *Para implementar Agente para ESX/ESXi a los servidores VMware ESX/ESXi:*

1. En el árbol de **Navegación**, haga clic con el botón derecho en **Máquinas virtuales** o haga clic con el botón derecho en el grupo que tiene el mismo nombre que el vCenter Server.
2. Haga clic en **Implementar el agente de ESX**.
3. **Servidores ESX/ESXi**

   Para un vCenter Server, se mostrará una lista de servidores y clústeres ESX/ESXi obtenida a partir del vCenter Server. Seleccione los servidores y clústeres en los que implementar el agente o seleccione la casilla de verificación **Seleccionar todos**.

   *En un clúster vCenter, un único Agente para ESX/ESXi realiza la copia de seguridad de las máquinas virtuales alojadas en todos los alojadas del clúster. Para obtener más información, consulte "Asistencia para clústeres vCenter (pág. 343)".*

   Puede añadir un servidor único a la lista al especificar su dirección IP o nombre. Proporcione un nombre de usuario y contraseña para cada servidor que añada a la lista. No puede especificarse un vCenter Server en esta ventana.

   Cuando se selecciona un servidor o clúster en el que el agente ya se ha instalado, se muestra el panel derecho de la ventana de **Implementación de ESX Agente**: **Actualizar el agente de ESX en este servidor.** No hay otros ajustes disponibles. Si necesita únicamente la actualización, vaya directamente al paso 6.
4. [Opcional] **Configuraciones de los agentes**

   Puede implementar Agent para ESX/ESXi con la configuración predeterminada o especificar una configuración personalizada para cualquier agente. Estos ajustes son los siguientes:

   **Almacenamiento de datos:** este es el almacenamiento de datos en el host ESX/ESXi en donde se almacenará el dispositivo virtual. Este es el almacenamiento de datos compartido por todos los servidores, incluyendo el interior del clúster, al implementar el agente en un clúster vCenter. Para obtener más información, consulte "Asistencia para clústeres vCenter (pág. 343)".

   **Interfaz de red:** esta es la red interna del servidor en el que se incluirá el dispositivo virtual. Si existen varias redes en el servidor, el programa selecciona la que es más adecuada para la operación del agente y especifica esta red como **predeterminada**. Solo aquellas redes que tienen una conexión con la Consola de servicios (o Red de gestión, en términos de VMware Infrastructure) del servidor están disponibles para su selección. Esto es fundamental para el funcionamiento del agente.

   El próximo ajuste aparece de diferente manera, dependiendo de cómo implementará el agente.

Al implementar a través del vCenter server - **La cuenta que se utilizará para la conexión del agente al servidor vCenter.**

Al implementar directamente al servidor ESX/ESXi - **La cuenta que se utilizará para la conexión del agente al servidor ESX.**

El servidor de gestión utilizará esta cuenta para establecer una relación de confianza con el agente durante su registro. Los planes de copias de seguridad y tareas de recuperación centralizados que se originan en el servidor de gestión se ejecutarán con esta cuenta de manera predeterminada. Esto significa que la cuenta debe tener los privilegios necesarios en el vCenter Server.

De manera predeterminada, el software utilizará la cuenta que ha especificado previamente, ya sea para configurar la integración con el vCenter o para obtener acceso al servidor ESX/ESXi. Si es necesario, puede especificar credenciales para otra cuenta.

La **zona horaria** del dispositivo virtual se configurará automáticamente de acuerdo con la zona horaria del servidor de gestión. Puede cambiar la zona horaria directamente en la interfaz de usuario del dispositivo virtual como se describe en "Cómo instalar ESX/ESXi Virtual Appliance". Cambiar la cuenta o los ajustes de red también es posible pero no recomendable, a menos que sea absolutamente necesario.

5. **Licencias**

   Haga clic en **Proporcionar la licencia**.

   Cuando instale la versión de prueba del producto, seleccione **Utilizar la siguiente clave de licencia de prueba** e introduzca la clave de licencia de prueba. La desduplicación siempre está habilitada en la versión de prueba.

   Cuando instale el producto adquirido, seleccione **Utilizar una licencia del siguiente Acronis License Server** y especifique el servidor de licencias que tenga los números de licencia adecuados para Acronis Backup & Recovery 10 Advanced Server Virtual Edition. Necesita una licencia para cada host que seleccione.

   Para poder deduplicar copias de seguridad, un agente necesita una licencia para deduplicación que se vende por separado. Si ha importado dichas licencias en el servidor de licencias, puede seleccionar la casilla de verificación **Habilitar deduplicación...** para permitir que los agentes adquieran estas licencias.

   Al instalar el producto *solo* para la copia de seguridad en línea, seleccione **Solo copia de seguridad (no se necesita clave de licencia)**. Esta opción asume que posee u obtendrá una suscripción al servicio Acronis Backup & Recovery 10 Online al momento de realizar la primera copia de seguridad.

6. Haga clic en **Implementar el agente de ESX**.

### Comprobación del progreso de la implementación y el resultado

La creación o actualización de dispositivos virtuales puede demorar un tiempo. Mire el progreso de las operaciones en la parte inferior de las vistas de las máquinas virtuales debajo de la barra **Información**. Después de crear y registrar un dispositivo virtual, aparece un grupo de máquinas virtuales correspondientes en el servidor de gestión.

### Si la implementación finalizó pero no se encuentra el grupo de máquinas virtuales

Acceda a la consola del dispositivo virtual con el cliente vSphere/VMware Infrastructure y compruebe la configuración del agente. Configure el agente manualmente, si fuera necesario, como se describe en "Cómo instalar ESX/ESXi Virtual Appliance". Añada el dispositivo virtual al servidor de gestión manualmente como se describe en "Incorporación de un equipo en el servidor de gestión (pág. 324)".

### Asistencia para clústeres vCenter

En un clúster vCenter, un único Agent para ESX/ESXi realiza la copia de seguridad de los equipos virtuales alojados en todos los servidores del clúster.

#### Implementación de Agent para ESX/ESXi en un clúster

Al configurar la implementación del agente desde el servidor de gestión, puede seleccionar un clúster como un servidor ESX normal. El dispositivo virtual (DV) del agente se implementa en un almacenamiento compartido en todos los servidores del clúster. Por lo general, se trata de un NFS compartido o un SAN-LUN conectado a cada uno de los servidores.

Supongamos que el clúster contiene tres servidores.

- El servidor 1 utiliza los almacenamientos A, B, C, D.
- El servidor 2 utiliza los almacenamientos C, D, E.
- El servidor 3 utiliza los almacenamientos B, C, D.

El DV se puede implementar tanto en C como en D. Si no hay un almacenamiento compartido por todos los servidores, puede importar el DV manualmente a cualquiera de los servidores. Esto funcionará, pero el rendimiento de la copia de seguridad no será bueno.

Después de la implementación, el dispositivo virtual del agente puede aparecer en cualquiera de los servidores, incluso en el clúster, dependiendo de cómo se ha configurado el equilibrio de carga.

#### Movimiento del DV del agente entre los clústeres

El funcionamiento del agente no se ve afectado cuando el Programador de Recursos Distribuidos (DRS) migra el dispositivo virtual a otro servidor.

#### Creación de un clúster de servidores que ya tienen agentes

Le recomendamos que elimine los Agents para ESX/ESXi de todos los servidores, menos uno. Retenga el agente cuyo DV resida en el almacenamiento compartido. Reinicie el DV para que reconozca el clúster.

## 7.1.5 Nodos de almacenamiento

Acronis Backup & Recovery 10 Storage Node le ayuda a optimizar el uso de numerosos recursos necesarios para la protección de datos de la empresa. Este objetivo se logra al organizar las bóvedas gestionadas (pág. 402) que sirven de almacenes dedicados para los archivos comprimidos de copia de seguridad de la empresa.

El nodo de almacenamiento le permite:

- Evitar la carga innecesaria de la CPU de los equipos gestionados al usar la limpieza del lado de los nodos de almacenamiento (pág. 409) y la validación del lado del nodo de almacenamiento (pág. 414).
- Reducir drásticamente el tráfico de la copia de seguridad y el espacio de almacenamiento que ocupan los archivos al usar la desduplicación (pág. 69).
- prevenir que malhechores tengan acceso a los archivos de copias de seguridad, incluso en caso de robo del medio de almacenamiento, al usar bóvedas cifradas (pág. 402).

Para obtener más información sobre Acronis Backup & Recovery 10 Storage Node, consulte la sección Acronis Backup & Recovery 10 Storage Node (pág. 20).

### Elementos clave de la vista "Nodos de almacenamiento"

- **Lista de nodos de almacenamiento con barra de herramientas**

  La barra de herramientas le permite llevar a cabo operaciones (pág. 344) con el nodo de almacenamiento seleccionado. La lista de nodos de almacenamiento muestra los nodos en línea y fuera de línea que se han añadido al servidor de gestión. También le informa acerca del número total de copias de seguridad y archivos comprimidos en el nodo de almacenamiento.

- **Panel de información**

  Contiene información detallada sobre el nodo de almacenamiento seleccionado y permite gestionar la tarea de compactación. De manera predeterminada, el panel se encuentra minimizado. Para expandir el panel, haga clic en la flecha tipo  . El contenido del panel también se encuentra en la ventana **Detalles del nodo de almacenamiento** (pág. 346).

### Modo de trabajo con nodos de almacenamiento (flujo de trabajo típico)

1. Instale Acronis Backup & Recovery 10 Storage Node.
2. Cree una cuenta de usuario para cada uno de los usuarios a los que desee dar acceso al nodo de almacenamiento.

   ***Nota:*** *Puede omitir este paso si tanto el nodo de almacenamiento como los usuarios de los equipos se encuentran en el mismo dominio de Active Directory.*

   Para obtener información acerca de los permisos de usuario en un nodo de almacenamiento y en sus bóvedas gestionadas, consulte Permisos de usuario en un nodo de almacenamiento (pág. 76).
3. Añada (pág. 345) el nodo de almacenamiento a Acronis Backup & Recovery 10 Management Server.
4. Cree una bóveda personal (pág. 135): especifique la ruta de la bóveda, indique el nodo de almacenamiento que gestionará la bóveda y seleccione las operaciones de gestión como, por ejemplo, desduplicación o cifrado.
5. Cree una política de copias de seguridad (pág. 377) o un plan de copia de seguridad que la bóveda gestionada utilizará.

## Acciones en los nodos de almacenamiento

Todas las operaciones descritas a continuación se llevan a cabo haciendo clic en los botones correspondientes en la barra de herramientas. Se puede acceder a las operaciones desde la barra **Nodos de almacenamiento** (en el panel **Acciones y herramientas**) y desde el elemento **Nodo de almacenamiento** del menú principal.

Para realizar una operación con un nodo de almacenamiento añadido en el servidor de gestión, seleccione primero el nodo de almacenamiento.

A continuación, se muestra una guía para llevar a cabo operaciones con los nodos de almacenamiento.

| Operación | Procedimiento |
|---|---|
| Añadir un nodo de almacenamiento al servidor de gestión | Haga clic en **Añadir**.<br>En la ventana Añadir nodo de almacenamiento (pág. 345), especifique en qué equipo se encuentra instalado el nodo de almacenamiento.<br>Al añadir un nodo de almacenamiento se establece una relación de confianza entre el servidor de gestión y el nodo de almacenamiento, del mismo modo que cuando se añade un equipo al servidor. Una vez que se ha añadido el nodo de almacenamiento en el servidor de gestión, se podrán crear bóvedas |

| | |
|---|---|
| | gestionadas en el nodo. |
| Eliminar un nodo de almacenamiento del servidor de gestión | Haga clic en **Quitar**.<br>Una vez que se ha eliminado el nodo de almacenamiento del servidor de gestión, las bóvedas que se gestionaban por medio de ese nodo de almacenamiento desaparecen de la lista de bóvedas (pág. 130) y dejan de estar disponibles para realizar operaciones. Todos los planes y tareas que utilicen esas bóvedas fallarán. Todas las bases de datos y bóvedas de este nodo de almacenamiento permanecerán intactas.<br>Es posible añadir de nuevo al servidor de gestión el nodo de almacenamiento eliminado anteriormente. De esta manera, todas las bóvedas gestionadas por el nodo de almacenamiento aparecerán en la lista de bóvedas y volverán a estar disponibles todos los planes y tareas que usaban esas bóvedas. |
| Crear una bóveda gestionada centralizada en el nodo de almacenamiento seleccionado | Haga clic en **Crear bóveda**.<br>Se abrirá la página Crear bóveda gestionada (pág. 135) con el nodo de almacenamiento preseleccionado. Lleve a cabo los pasos restantes para crear la bóveda. |
| Cambiar la programación de tareas de compactación | Después de eliminar las copias de seguridad de las bóvedas de desduplicación, ya sea manualmente o durante una limpieza, podrían aparecer datos sin referencias en las bóvedas de desduplicación y sus bases de datos. El procedimiento de compactación elimina dichos datos para liberar espacio de almacenamiento. Solo se puede realizar una tarea de compactación por cada nodo de almacenamiento.<br>Haga clic en **Reprogramación de la compactación**.<br>En la ventana **Programación**, configure la programación para el procedimiento de compactación. Solo se pueden configurar los eventos de tiempo (programaciones diarias (pág. 174), semanales (pág. 176) y mensuales (pág. 178)).<br>El valor predeterminado: Comenzar la tarea cada **1 semana**, el **Domingo** a las **03:00:00 a. m**. Repetir **una vez**. |
| Ver información detallada sobre el nodo de almacenamiento | Haga clic en **Ver detalles**.<br>En la ventana **Detalles del nodo de almacenamiento** (pág. 346) (cuyo contenido se encuentra también en el panel **Información**), examine la información sobre el nodo de almacenamiento y las bóvedas gestionadas por este nodo. También puede gestionar la tarea de compactación: iniciando y deteniendo manualmente la tarea. |
| Actualizar la lista de nodos de almacenamiento. | Haga clic en **Actualizar**.<br>La consola de gestión actualizará la lista de nodos de almacenamiento del servidor de gestión con la información más reciente. Aunque la lista de nodos de almacenamiento se actualiza automáticamente en función de los eventos es posible que los datos no se puedan recuperar inmediatamente del servidor de gestión debido a un tiempo de latencia. La actualización manual garantiza la visualización de los datos más recientes. |

## Adición de un nodo de almacenamiento

***Para añadir un nodo de almacenamiento***

1. En el campo **IP/Nombre**, introduzca el nombre o la dirección IP del equipo donde se encuentra el nodo de almacenamiento, o haga clic en **Examinar...** para buscar el equipo dentro de la red.

Utilice el nombre de dominio totalmente cualificado (FQDN) del nodo de almacenamiento, es decir, un nombre de dominio totalmente especificado que finalice en un dominio de nivel alto. No introduzca “127.0.0.1” o “localhost” como el IP/nombre del nodo de almacenamiento. Estos ajustes no se aceptan ni siquiera si el servidor de gestión y el nodo de almacenamiento están en el mismo equipo ya que, después de haber implementado la política usando el nodo de almacenamiento, cada agente intentará acceder al nodo de almacenamiento como si estuviese instalado en el servidor del agente.

2. Para proporcionar una cuenta de usuario válida para el equipo, haga clic en **Opciones>>**, y especifique:
   - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio). La cuenta de usuario debe de ser un miembro del grupo de Administradores del equipo.
   - **Contraseña**. La contraseña de la cuenta.

   Seleccione la casilla de verificación **Guardar contraseña** para guardar la contraseña de la cuenta.
3. Haga clic en **Aceptar**.

El registro no se puede llevar a cabo cuando el equipo está fuera de línea, ya que necesita la participación del nodo de almacenamiento.

## Detalles del nodo de almacenamiento

La ventana **Detalles del nodo de almacenamiento** acumula en cuatro pestañas toda la información del nodo de almacenamiento de Acronis Backup & Recovery 10 seleccionado. Esta información se encuentra también en el panel **Información**.

### Propiedades del nodo de almacenamiento

Esta pestaña muestra la siguiente información sobre el nodo de almacenamiento seleccionado:

- **Nombre**: nombre del equipo donde se encuentra instalado el nodo de almacenamiento.
- **IP**: IP del equipo donde se encuentra instalado el nodo de almacenamiento.
- **Disponibilidad**:
  - **Desconocido**: este estado se muestra hasta que se establece la primera conexión entre el nodo de almacenamiento y el servidor de gestión, después de añadir el nodo de almacenamiento o poner en marcha el servicio del servidor de gestión.
  - **En línea**: indica que el nodo de almacenamiento se encuentra disponible para el servidor de gestión. Esto quiere decir que la última conexión entre el servidor de gestión y el nodo de almacenamiento se completó correctamente. Se establece una conexión cada 2 minutos.
  - **Fuera de línea**: indica que el nodo de almacenamiento no está disponible.
  - **Retirado**: indica que el nodo de almacenamiento se ha registrado en un servidor de gestión diferente. Por lo tanto, no es posible controlar el nodo desde el servidor de gestión actual.
- **Archivos comprimidos**: indica el número total de archivos comprimidos almacenados en todas las bóvedas gestionadas por el nodo de almacenamiento.
- **Copias de seguridad**: indica el número total de copias de seguridad almacenadas en todas las bóvedas gestionadas por el nodo de almacenamiento.

### Bóvedas

Esta pestaña muestra una lista de las bóvedas gestionadas por el nodo de almacenamiento.

Para abrir una bóveda gestionada para proceder a un examen detallado y realizar operaciones sobre ella, seleccione la bóveda y haga clic en **Ver bóveda** (en la barra de herramientas de la pestaña). En la vista **Bóveda centralizada** (pág. 131), realice las siguientes acciones.

### Servicios

Esta pestaña muestra los parámetros de programación de la tarea de compactación.

### Tareas de servicio

Esta pestaña permite al administrador del servidor de gestión configurar la tarea de compactación y revisar sus parámetros. En un nodo de almacenamiento solo puede existir una tarea de compactación.

## 7.1.6 Tareas

La vista **Tareas** le permite supervisar y gestionar las tareas existentes en los equipos registrados. Puede ver los detalles de las tareas, sus estados y resultados de ejecución, así como ejecutar, detener y eliminar tareas.

Para averiguar qué tarea está realizando un equipo en un determinado momento, compruebe el estado de ejecución de la tarea. El estado de una tarea le ayuda a determinar si la tarea se ha desarrollado correctamente.

Para obtener más información sobre los estados y estatus de las tareas, consulte las secciones Estados de las tareas (pág. 195) y Estatus de las tareas (pág. 196).

### Modo de trabajo con tareas

- Utilice las funciones de filtración y clasificación (pág. 349) de las entradas del registro que desee que se muestren en la tabla.
- Seleccione una tarea sobre la cual desee realizar una acción.

### Acciones en tareas

A continuación, se muestra una guía para llevar a cabo operaciones con las tareas.

| Operación | Procedimiento |
|---|---|
| **Creación de un nuevo plan de copia de seguridad o una tarea en un equipo registrado** | Haga clic en **Nuevo** y seleccione una de las siguientes opciones:<br>▪ Plan de copia de seguridad (pág. 207)<br>▪ Tarea de recuperación<br>▪ Tarea de validación (pág. 255)<br>Luego debe especificar el equipo registrado en el que se ejecutará la tarea seleccionada o el plan de copia de seguridad. |
| **Ver información detallada sobre una tarea** | Haga clic en **Ver detalles**.<br>En la ventana Detalles de tareas (pág. 201), examine toda la información relacionada con la tarea seleccionada. |
| **Vea el informe de la tarea** | Haga clic en **Ver registro**.<br>La vista Registro (pág. 349) mostrará una lista de las entradas del registro relacionadas con la tarea seleccionada. |

| | |
|---|---|
| **Ejecutar una tarea** | Haga clic en **Ejecutar**.<br>La tarea se ejecutará inmediatamente a pesar de su programación. |
| **Detener una tarea.** | Haga clic en **Detener**.<br>*¿Qué sucede si detengo la tarea?*<br>Por lo general, al detener la tarea se cancela su operación (copia de seguridad, recuperación, validación, exportación, conversión, migración). La tarea pasa en primer lugar al estado **Deteniendo** y después al estado Inactiva. La programación de la tarea, en caso de haberla creado, aún será válida. Para completar la operación, tendrá que ejecutar la tarea de nuevo.<br>▪ **Tarea de recuperación (desde la copia de seguridad del disco)**: Se eliminará el volumen de destino y su espacio quedará sin asignar. Obtendrá el mismo resultado que si la recuperación no se completara de manera correcta. Para recuperar el volumen "perdido", tendrá que volver a ejecutar la tarea nuevamente.<br>▪ **tarea de recuperación (desde la copia de seguridad de archivos)**: La operación cancelada puede ocasionar cambios en la carpeta de destino. Algunos archivos se pueden recuperar pero otros no, dependiendo del momento en el que se haya detenido la tarea. Para recuperar todos los archivos deberá ejecutar la tarea una vez más. |
| **Editar una tarea** | Haga clic en **Editar**.<br>*¿Por qué no puedo editar la tarea?*<br>▪ **La tarea pertenece a un plan de copia de seguridad.**<br>Solo las tareas que no pertenecen a un plan de copia de seguridad, tales como las tareas de recuperación, pueden modificarse mediante edición directa. Cuando deba modificar una tarea que pertenece a un plan de copia de seguridad local, edite el plan de copia de seguridad. Las tareas que pertenecen a un plan de copia de seguridad centralizado se pueden modificar al editar la política centralizada que generó el plan. Esto solo lo puede hacer el administrador del servidor de gestión.<br>▪ **No tiene el privilegio adecuado**<br>Un usuario no puede modificar tareas de otros usuarios sin poseer los privilegios de Administrador |
| **Eliminar una tarea.** | Haga clic en **Eliminar**.<br>*¿Por qué no puedo eliminar la tarea?*<br>▪ **La tarea pertenece a un plan de copia de seguridad.**<br>La tarea que pertenece a un plan de copia de seguridad no puede eliminarse por separado del plan. Edite el plan para quitar la tarea o elimine el plan completo.<br>▪ **No tiene el privilegio adecuado**<br>Un usuario no puede eliminar tareas de otros usuarios sin poseer los privilegios de Administrador.<br>▪ **Esta es una tarea de compactación integrada**<br>Cada nodo de almacenamiento posee una tarea de servicio integrada llamada tarea de compactación. Esta tarea no se puede eliminar. |

| | |
|---|---|
| **Actualizar la tabla de tareas** | Haga clic en **Actualizar**.<br>La consola de gestión actualizará la lista de tareas existentes en el equipo con la información más reciente. Aunque la lista de tareas se actualiza automáticamente en función de los eventos, es posible que los datos no se puedan recuperar inmediatamente debido a un tiempo de latencia. La actualización manual garantiza la visualización de los datos más recientes. |

### Filtrado y clasificación de tareas

A continuación, se muestra una guía para filtrar y ordenar las tareas.

| Para | Realizar |
|---|---|
| Configurar el número de tareas mostradas | Seleccione **Opciones > Opciones de consola > Cantidad de tareas** (pág. 86) y configure el valor deseado. La cantidad máxima de tareas que se pueden mostrar es 500. Si la cantidad excede dicho valor, utilice filtros para mostrar las tareas que no se han podido mostrar. |
| Ordenar tareas por columna | Haga clic en el encabezado de la columna para ordenar las tareas por orden ascendente.<br>Haga clic de nuevo para ordenar las tareas por orden descendente. |
| Filtrar las tareas por nombre, propietario o plan de copia de seguridad. | Escriba el nombre de la tarea (nombre del propietario o del plan de copias de seguridad) en el campo debajo del encabezado de la columna correspondiente.<br>De esta manera, verá la lista de tareas cuyos nombres (o los nombres de sus propietarios o de los planes de copia de seguridad) coinciden total o parcialmente con el valor introducido. |
| Filtrar tareas por tipo, estado de ejecución, estado, tipo, origen, último resultado o programación. | En el campo situado debajo del encabezado de cada columna respectiva, seleccione el valor que desee de la lista. |

#### Configuración de la tabla de tareas

De manera predeterminada, la tabla que se muestra se compone de ocho columnas, las demás se encuentran ocultas. También puede ocultar las columnas innecesarias y mostrar las ocultas.

***Mostrar u ocultar columnas***

1. Haga clic con el botón derecho en el encabezado de cualquier columna para abrir el menú contextual. Los elementos del menú que no estén seleccionados corresponden a los encabezados de las columnas presentadas en la tabla.
2. Haga clic sobre los elementos que quiera mostrar/ocultar.

## 7.1.7 Registro

El registro de Acronis Backup & Recovery 10 almacena el historial de acciones que el software realiza en un equipo o que un usuario lleva a cabo en un equipo utilizando dicho software. Por ejemplo, cuando un usuario edita una tarea, se añade una entrada al registro. Cuando el software ejecuta una tarea, añade varias entradas que revelan lo que está haciendo en ese momento.

#### Registro local y centralizado de Acronis Backup & Recovery 10

Acronis Backup & Recovery 10 posee un registro de eventos local y centralizado.

### Registro de eventos local

Un registro de eventos local conserva información sobre las operaciones de Acronis Backup & Recovery 10 en un equipo gestionado. Por ejemplo, al crear o ejecutar un plan de copia de seguridad, gestionar archivos comprimidos en bóvedas personales o ejecutar una tarea de recuperación, se generarán eventos registrados en el registro de eventos local. Físicamente, un registro de eventos local es una recopilación de archivos XML almacenados en el equipo. El registro local de eventos de un equipo gestionado es accesible cuando la consola está conectada al equipo. El registro local de eventos no se puede deshabilitar.

Las operaciones llevadas a cabo utilizando un dispositivo de inicio también se registran, pero la vida del registro se limita a la sesión actual. Aunque al reiniciar el equipo se elimina el registro, es posible guardar el registro en un archivo siempre que el equipo se inicie con el dispositivo.

Acronis Backup & Recovery 10 Storage Node tiene su propio registro local de eventos. Solo se puede acceder a este registro a través del registro centralizado.

### Registro de eventos centralizado

### Modo de trabajo con las entradas del registro

- El número máximo de entradas almacenadas en el registro de eventos centralizado es de 50.000. El número máximo de entradas que se puede mostrar es de 10.000. En el caso de que el número de entradas sea mayor que 10.000, utilice las funciones de filtración y clasificación de las entradas del registro que desee que se muestren en la tabla. También puede ocultar las columnas innecesarias y mostrar las ocultas. Para obtener más detalles, consulte la sección Filtrado y clasificación de las entradas del registro (pág. 351).
- Seleccione la(s) entrada(s) del registro sobre la(s) que desea llevar a cabo una acción. Para obtener más detalles, consulte la sección Acciones sobre las entradas del registro (pág. 351).
- Para revisar información detallada sobre la entrada del registro seleccionada, utilice el panel **Información**. De manera predeterminada, el panel se encuentra minimizado. Para expandir el panel, haga clic en la flecha tipo  . El contenido del panel también se puede encontrar en la ventana **Detalles de las entradas del registro** (pág. 352).

### Modos de abrir la vista "Registro" con entradas del registro prefiltradas.

Si ha seleccionado elementos en otras vistas de administración (Tablero, Equipos, Políticas de copia de seguridad, Tareas), puede abrir la vista Registro con entradas del registro filtradas previamente para ese elemento en cuestión. Por lo tanto, no hace falta que configure usted mismo los filtros en la tabla Registro.

| Vista | Acción |
|---|---|
| **Tablero** | En el calendario, haga clic con el botón derecho en cualquier fecha resaltada y seleccione **Ver registro**. La vista Registro mostrará la lista de las entradas del registro que ya se han filtrado por la fecha en cuestión. |
| **Equipos** | Seleccione un equipo o un grupo de equipos y haga clic en **Ver registro**. La vista Registro mostrará una lista de las entradas del registro relacionadas con el equipo o grupo de equipos seleccionado. |
| **Políticas de copia de seguridad** | Seleccione una política de copias de seguridad y haga clic en **Ver registro**. La vista Registro mostrará una lista de las entradas del registro relacionadas con la política seleccionada. |
| **Tareas** | Seleccione una tarea y haga clic en **Ver registro**. La vista Registro mostrará una lista de las entradas del registro relacionadas con la tarea seleccionada. |

## Acciones en las entradas del registro

Todas las operaciones descritas a continuación se llevan a cabo haciendo clic en los elementos correspondientes en la **barra de herramientas** del registro. Todas estas operaciones se pueden llevar a cabo con el menú contextual (haciendo clic con el botón derecho en la entrada del registro), o con la barra **acciones del registro** (en el panel **Acciones y herramientas**).

A continuación se muestra una guía para llevar a cabo acciones en las entradas del registro.

| Operación | Procedimiento |
|---|---|
| Seleccionar una entrada del registro | Haga clic en ella. |
| Seleccionar varias entradas del registro | ▪ *no contiguas*: mantenga pulsada la tecla **CTRL** y haga clic en las entradas una a una<br>▪ *contiguas*: seleccione una entrada, mantenga pulsada la tecla **MAYÚSCULAS** y haga clic en otra entrada. Así se seleccionarán todas las entradas entre la primera y la última selección. |
| Ver información sobre las entradas del registro | 1. Seleccione una entrada del registro<br>2. Realice uno de los siguientes procedimientos:<br>▪ Haga clic en **Ver detalles**. Los detalles de las entradas del registro se mostrarán en una ventana diferente.<br>▪ Expanda el Panel de información haciendo clic en la flecha tipo. |
| Guardar las entradas del registro seleccionadas en un archivo comprimido. | 1. Seleccione una o varias entradas del registro.<br>2. Haga clic en **Guardar la selección en archivo**.<br>3. En la ventana abierta, especifique la ruta y un nombre para el archivo. |
| Guardar todas las entradas del registro a un archivo. | 1. Asegúrese de que no se han configurado filtros.<br>2. Haga clic en **Guardar todo en archivo**.<br>3. En la ventana abierta, especifique la ruta y un nombre para el archivo. |
| Guardar todas las entradas filtradas del registro en un archivo comprimido. | 1. Configure los filtros para obtener una lista de las entradas del registro que satisfagan los criterios.<br>2. Haga clic en **Guardar todo en archivo**.<br>3. En la ventana abierta, especifique la ruta y un nombre para el archivo. Como consecuencia, se guardarán las entradas del registro de la lista. |
| Eliminar todas las entradas del registro. | Haga clic en **Limpiar registro**.<br>Todas las entradas del registro se eliminarán del mismo y se creará una nueva entrada. Esta contendrá información relacionada con quién eliminó las entradas y cuándo. |
| Configurar el nivel de registro | Haga clic en **Configurar el nivel de registro**.<br>En la ventana **Nivel de registro** (pág. 87), especifique si desea recopilar eventos de registro de equipos registrados al registro centralizado. |

## Filtrado y clasificación de entradas del registro

A continuación se muestra una guía para filtrar y ordenar las entradas del registro.

| Operación | Procedimiento |
|---|---|
| Mostrar las entradas del registro para un periodo de tiempo determinado | 1. En el campo **De**, seleccione la fecha a partir de la cual se mostrarán las entradas del registro.<br>2. En el campo **A**, seleccione la fecha hasta la cual se mostrarán las entradas del registro. |
| Filtrar las entradas del registro por tipo | Active o desactive los siguientes botones de la barra de herramientas:<br>  para filtrar mensajes de error<br>  para filtrar mensajes de advertencia<br>  para filtrar mensajes de información |
| Filtrar entradas del registro por tipo de plan de copia de seguridad original o entidad gestionada. | En el encabezado de la columna **Plan de copia de seguridad** (o **Tipo de entidad gestionada**), seleccione el plan de copia de seguridad o el tipo de entidad gestionada de la lista. |
| Filtrar entradas del registro por tarea, entidad gestionada, equipo, código o propietario. | Escriba el valor requerido (nombre de la tarea, del equipo, del propietario, etc.) en el campo situado debajo del encabezado de la columna respectiva.<br>Como consecuencia, verá la lista de las entradas del registro que coinciden total o parcialmente con el valor introducido. |
| Ordenar las entradas del glosario por fecha y hora | Haga clic en el encabezado de la columna para ordenar las entradas del registro por orden ascendente. Haga clic de nuevo para ordenar las entradas del registro por orden descendente. |

### Configurar la tabla del registro

De manera predeterminada, la tabla muestra siete columnas, las otras están ocultas. Si fuera necesario, puede ocultar las columnas visibles y mostrar las ocultas.

#### *Mostrar u ocultar columnas*

1. Haga clic con el botón derecho en el encabezado de cualquier columna para abrir el menú contextual. Los elementos del menú que no estén seleccionados corresponden a los encabezados de las columnas presentadas en la tabla.
2. Haga clic sobre los elementos que quiera mostrar/ocultar.

## Detalles de las entradas del registro centralizado

Muestra información detallada de la entrada del registro seleccionada y permite copiarla al portapapeles.

Para copiar los detalles, haga clic en el botón **Copiar al portapapeles**.

### Campos de datos de entrada del registro.

Una entrada del registro centralizado contiene los siguientes campos de datos:

- **Tipo**: tipo de evento (Error, Advertencia, Información)
- **Fecha**: fecha y hora en la que ha ocurrido el evento
- **Política**: la política de copias de seguridad con la que se relaciona el evento (si la hubiera)

- **Tarea**: tarea con la que se relaciona el evento (si la hubiera)
- **Tipo de entidad gestionada**: tipo de entidad gestionada donde ha ocurrido el evento (si la hubiera)
- **Entidad gestionada**: nombre de la entidad gestionada donde ha ocurrido el evento (si la hubiera)
- **Equipo**: nombre del equipo donde ha ocurrido el evento (si lo hubiera)
- **Código**: en blanco o el código de error del programa si el tipo de evento es de error. El código de error se compone de un número entero que puede utilizar el servicio de asistencia de Acronis para solucionar el problema.
- **Módulo**: en blanco o el número de módulo del programa en el que ha tenido lugar el error. Se trata de un número entero que puede utilizar el servicio de asistencia de Acronis para solucionar el problema.
- **Propietario**: nombre de usuario del propietario (pág. 33) del plan o la política de copias de seguridad
- **Mensaje**: la descripción textual del evento.

La información de la entrada del registro que se copiará tendrá el siguiente aspecto:

```
--------------------------Detalles de entrada del registro-------------------
-------
Tipo:                              Información
Fecha y hora:                      DD.MM.AAAA HH:MM:SS
Plan de copia de seguridad:        Nombre del plan de copias de seguridad
Tarea:                             Nombre de la tarea
Tipo de entidad gestionada:        Equipo
Entidad gestionada:                NOMBRE_DE_LA_ENTIDAD
Equipo:                            NOMBRE_DEL_EQUIPO
Mensaje:
Descripción de la operación
Código:                            12(3x45678A)
Módulo:                            Nombre del módulo
Propietario:                       Propietario del plan
------------------------------------------------------------------------
```

### 7.1.8 Generación de informes

La generación de informes le proporciona al administrador del management server información detallada y bien estructurada con respecto a las operaciones de protección de datos de una empresa . Los informes pueden utilizarse como instrumento para un análisis profundo de la infraestructura completa de la copia de seguridad dentro de una red corporativa.

El management server genera informes utilizando estadísticas y registros que se recolectan desde equipos registrados y se almacenan en base de datos especializadas.

Los informes se generan basados en una plantilla de informes. Las plantillas definen la información que se incluirá en el informe y la manera en la que se representa la información.

Acronis Backup & Recovery 10 Management Server ofrece plantillas de informes para:

- Equipos registrados
- Políticas de copias de seguridad existentes en servidor de gestión
- Planes de copias de seguridad locales y centralizadas existentes en los equipos registrados
- Tareas locales y centralizadas existentes en los equipos registrados
- Archivos comprimidos y copias de seguridad almacenados en las bóvedas centralizadas

- Estadísticas acerca de las bóvedas gestionadas centralizadas
- Historial de las actividades de la tarea

Los informes sobre los equipos, las políticas de copias de seguridad, los planes de copias de seguridad, las tareas y los Archivos comprimidos y copias de seguridad contienen información del momento actual.

Los informes sobre las estadísticas de las bóvedas y las actividades de la tarea se realizan a base de intervalos y proporcionan información histórica para el intervalo de tiempo especificado que puede durar de días a años, según la cantidad de datos almacenados en las bases de datos.

### Generación de informes

Para comenzar a generar un informe, seleccione una plantilla del informe en la vista **Informes** y después haga clic en **Generar** en la barra de herramientas.

Existen dos tipos de plantillas de informes: personalizables y predeterminadas. En una plantilla de informes personalizable puede especificar qué entradas incluir en el informe al utilizar los filtros. Una plantilla de informe predeterminada está predefinida para que pueda generar un informe con un clic.

El informe contendrá la información seleccionada, agrupada y clasificada de acuerdo a las configuraciones de las plantillas. Los informes aparecen en una ventana interactiva separada que permite expandir y reducir las tablas. Puede exportar el informe a un archivo XML y abrirlo después utilizando Microsoft Excel o Microsoft Access.

## Informe acerca de los equipos

En esta vista puede generar un informe acerca de los equipos que están registrados en el management server. Este informe consiste en una o más tablas.

### Filtro

En **Filtros**, seleccione qué equipos se deben incluir en el informe. Se incluyen solo las máquinas que cumplen con todos los criterios del filtro.

- **Equipos**: La lista de equipos. Seleccione ya sea equipos físicos o equipos virtuales.
- **Estado**: Los estados de los equipos: **Aceptar**, **Advertencia** y/o **Error**.
- **Última conexión** (solo equipos físicos): El periodo dentro del cual se estableció la última conexión entre los equipos y el management server.
- **Última copia de seguridad exitosa**: El periodo dentro del cual se finalizó la última copia de seguridad en cada uno de los equipos.
- **Siguiente copia de seguridad**: El periodo dentro del cual se iniciará la siguiente copia de seguridad programada en cada uno de los equipos.
- **Sistema operativo**: Los sistemas operativos que ejecutan los equipos.
- **Dirección IP** (solo equipos físicos): El rango de la última dirección IP conocida de los equipos.
- **Disponibilidad** (solo equipos físicos): El tipo de disponibilidad de los equipos, **En línea** o **Fuera de línea**.

Con la configuración de filtros predeterminada, el informe incluye todos los equipos físicos.

### Vista del informe

En **Vista del informe**, seleccione la forma de visualización del informe:

- Seleccione si desea mostrar todos los elementos en una única tabla o agruparlos en una columna en particular.
- Especifique qué columnas de la tabla mostrar y en qué orden.
- Especifique cómo ordenar la tabla.

## Informe acerca de las políticas de copias de seguridad

En esta vista, puede generar un informe acerca de las políticas de copias de seguridad existentes en el management server. Este informe consiste en una o más tablas.

### Filtro

En **Filtros**, seleccione qué políticas de copias de seguridad incluir en el informe. Se incluyen solo las políticas de copias de seguridad que cumplen con todos los criterios del filtro.

- **Políticas de copias de seguridad**: La lista de políticas de copias de seguridad.
- **Tipo de origen**: El tipo de datos incorporados en la copia de seguridad bajo las políticas de copias de seguridad— **Discos/volúmenes** y/o **Archivos**.
- **Estado de implementación**: Los estados de implementación de las políticas de copias de seguridad; por ejemplo, **Implementado**.
- **Estado**: Los estados de las políticas de copias de seguridad: **Aceptar**, **Advertencia** y/o **Error**.
- **Programación**: Los tipos de programación de las políticas de copias de seguridad: **Manual** y/o **Programada**. La programación manual significa que el plan de copia de seguridad centralizada correspondiente se ejecuta solo cuando lo inicia manualmente.
- **Propietario**: La lista de usuarios que crearon las políticas de copias de seguridad.

Con la configuración de filtros predeterminada, el informe incluye todas las políticas de copias de seguridad.

### Vista del informe

En **Vista del informe**, seleccione la forma de visualización del informe:

- Seleccione si desea mostrar todos los elementos en una única tabla o agruparlos en una columna en particular.
- Especifique qué columnas de la tabla mostrar y en qué orden.
- Especifique cómo ordenar la tabla.

## Informe acerca de los planes de copias de seguridad

En esta vista, puede generar un informe acerca de planes de copias de seguridad existentes en los equipos registrados. Este informe consiste en una o más tablas.

### Filtro

En **Filtros**, seleccione qué planes de copias de seguridad se deben incluir en el informe. Se incluyen solo los planes de copias de seguridad que cumplen con todos los criterios del filtro.

- **Origen**: Los tipos de origen de los planes de copias de seguridad: **Local** y/o **Centralizado**.
- **Políticas de copias de seguridad** (solo disponible para los planes de copias de seguridad centralizados): Las políticas de copias de seguridad en las que se basan los planes de copias de seguridad centralizados.

- **Equipos**: La lista de equipos donde existen planes de copias de seguridad.
- **Estado de ejecución**: Los estados de ejecución de los planes de copias de seguridad, por ejemplo, **Ejecutando**.
- **Estado**: Los estados de los planes de copias de seguridad: **Aceptar**, **Advertencia** y/o **Error**.
- **Última hora de finalización**: El periodo dentro del cual se finalizó la última copia de seguridad en cada uno de los planes de copias de seguridad.
- **Programación**: Los tipos de programación de los planes de copias de seguridad: **Manual** y/o **Programada**. La programación manual significa que un plan de copia de seguridad se ejecuta solo cuando lo inicia manualmente.
- **Propietario**: La lista de usuarios que crearon los planes de copias de seguridad.

Con la configuración de filtros predeterminada, el informe incluye todos los planes de copias de seguridad de todos los equipos.

### Vista del informe

En **Vista del informe**, seleccione la forma de visualización del informe:

- Seleccione si desea mostrar todos los elementos en una única tabla o agruparlos en una columna en particular.
- Especifique qué columnas de la tabla mostrar y en qué orden.
- Especifique cómo ordenar la tabla.

## Informe acerca de las tareas

En esta vista, puede generar un informe acerca de las tareas que se ejecutan en los equipos registrados. Este informe consiste en una o más tablas.

### Filtro

En **Filtros**, seleccione qué tareas se deben incluir en el informe. Se incluyen solo las tareas que cumplen con todos los criterios del filtro.

- **Origen**: Los tipos de orígenes de las tareas: **Centralizado**, **Local** y/o **Local sin plan de copias de seguridad**. Una tarea centralizada pertenece a un plan de copias de seguridad centralizada. Una tarea local puede no pertenecer a un plan de copias de seguridad (por ejemplo, una tarea de recuperación).
- **Políticas de copias de seguridad** (solo tareas centralizadas): Las políticas de copias de seguridad en las que se basan las tareas.
- **Equipos**: La lista de equipos donde existen tareas.
- **Tipo**: Los tipos de tareas, por ejemplo, tareas de copias de seguridad de discos.
- **Estado de ejecución**: Los estados de ejecución de las tareas, por ejemplo, **Ejecutando**.
- **Último resultado**: Los últimos resultados de las tareas, **Completado correctamente**, **Completado correctamente con advertencias** y/o **Fallido**.
- **Programación**: Los tipos de programación de las tareas: **Manual** o **Programada**. La programación manual significa que una tarea se ejecuta solo cuando lo inicia manualmente.
- **Propietario**: La lista de usuarios que crearon las tareas.
- **Duración**: Los límites del tiempo en el que cada una de las tareas fue ejecutada por última vez.

Con la configuración de filtros predeterminada, el informe incluye todas las tareas de todos los equipos.

### Vista del informe

En **Vista del informe**, seleccione la forma de visualización del informe:

- Seleccione si desea mostrar todos los elementos en una única tabla o agruparlos en una columna en particular.
- Especifique qué columnas de la tabla mostrar y en qué orden.
- Especifique cómo ordenar la tabla.

## Informe acerca de los archivos comprimidos y las copias de seguridad

En esta vista, puede generar un informe acerca de los archivos comprimidos que están almacenados en las bóvedas de gestión centralizada. Este informe consiste en una o más tablas.

### Filtro

En **Filtros**, seleccione qué archivos comprimidos se deben incluir en el informe. Se incluyen solo los archivos comprimidos que cumplen con todos los criterios del filtro.

- **Bóvedas**: La lista de bóvedas gestionadas centralmente que almacena los archivo comprimidos.
- **Equipos**: La lista de equipos registrados desde donde fueron creados los archivos comprimidos.
- **Tipo**: Los tipos de archivos comprimidos, archivos comprimidos a nivel del disco y/o archivos a nivel del archivo.
- **Propietario**: La lista de usuarios que crearon los archivos comprimidos.
- **Hora de creación**: El periodo en el cual se creó la copia de seguridad más nueva en cada uno de los archivos comprimidos.
- **Espacio ocupado**: Los límites para el espacio ocupado por cada uno de los archivos comprimidos.
- **Fecha de la copia de seguridad**: Los límites para el tamaño total de los datos que están actualmente almacenados en cada uno de los archivos comprimidos. El tamaño puede diferir del espacio ocupado debido a la compresión o deduplicación.
- **Cantidad de copias de seguridad**: Los límites para la cantidad de copias de seguridad que cada archivo comprimido contiene.

Con la configuración de filtros predeterminada, el informe incluye a todos los archivos que están almacenados en las bóvedas gestionadas centralmente.

### Vista del informe

En **Vista del informe**, seleccione la forma de visualización del informe:

- Seleccione si desea mostrar todos los elementos en una única tabla o agruparlos en una columna en particular.
- Especifique qué columnas de la tabla mostrar y en qué orden.
- Especifique cómo ordenar la tabla.

## Informe acerca de las estadísticas de las bóvedas

En esta vista, puede generar un informe acerca del uso de las bóvedas gestionadas centralizadas que actualmente están añadidas al servidor de gestión. Este informe consiste en una o más tablas y diagramas.

### Cobertura del informe

En **Cobertura del informe**, seleccione el intervalo de tiempo en el cual desea generar el informe. El informe mostrará el estado de las bóvedas seleccionadas a la hora especificada de cada día en el período del informe.

### Filtro

En **Filtros**, seleccione qué bóvedas gestionadas centralizadas se deben incluir en el informe y si desea incluir información acerca del total combinado de todas las bóvedas combinadas.

Un total combinado es el espacio total libre y ocupado, la cantidad total de datos copiados, la cantidad total de archivos comprimidos y copias de seguridad y la proporción promedio de las bóvedas seleccionadas.

Con la configuración de filtros predeterminada, el informe incluye información acerca de todas las bóvedas gestionadas centralizadas más el total combinado.

### Vista del informe

En **Vista del informe**, seleccione la forma de visualización del informe:

- Especifique qué columnas de la tabla mostrar y en qué orden.
- Seleccione qué diagramas se deben incluir en el informe. Los diagramas muestran el uso del espacio en las bóvedas.

## Informe acerca de las actividades de la tarea

En esta vista, puede generar un informe acerca de las tareas que existieron en los equipos registrados dentro de un período seleccionado. Este informe consiste en uno o más diagramas, un diagrama por equipo.

Los diagramas muestran cuántas veces finalizó cada tarea en un día en particular con cada uno de los resultados: “Completado”, “Completado con advertencias” y “Fallido”.

### Cobertura del informe

En **Cobertura del informe**, seleccione el intervalo de tiempo en el cual desea generar el informe.

### Filtro

En **Filtros**, seleccione qué tareas se deben incluir en el informe. Se incluyen solo las tareas que cumplen con todos los criterios del filtro.

- **Origen**: Los tipos de origen de las tareas: **Centralizado**, **Local** y/o **Local sin plan de copias de seguridad**. Una tarea centralizada pertenece a un plan de copias de seguridad centralizada. Una tarea local puede no pertenecer a un plan de copias de seguridad (por ejemplo, una tarea de recuperación).
- **Políticas de copias de seguridad** (solo tareas centralizadas): Las políticas de copias de seguridad en las que se basan las tareas. La configuración predeterminada incluye todas las políticas de copias de seguridad que alguna vez existieron durante el periodo del informe.
- **Equipos**: La lista de equipos en donde existen tareas.
- **Tipo**: Los tipos de tareas, por ejemplo, tareas de copias de seguridad de discos.
- **Propietario**: La lista de usuarios que crearon las tareas.

Con la configuración de filtros predeterminada, el informe incluye todas las tareas que existieron en los equipos registrados en cualquier momento durante el periodo del informe.

### Selección de columnas

En la ventana **Selección de columnas**, puede elegir qué columnas de la tabla incluir en el informe y en qué orden.

Las tablas en el informe contendrán columnas, de izquierda a derecha, como se establece en **Presentación del informe**. La columna superior en la lista será la primera columna a la izquierda en el informe.

Al elegir qué columna mostrar, utilice las flechas izquierda y derecha para incluir o excluir columnas y las flechas hacia arriba y abajo para cambiar el orden de las columnas.

Algunas columnas, como **Nombre del equipo** en un informe sobre equipos, no pueden excluirse de la lista o moverse hacia arriba o abajo en la misma.

### Vista del informe

Para que su navegador web muestre correctamente las fechas y demás información en los informes generados, habilite el contenido activo (JavaScript). Puede permitir que el contenido activo se ejecute temporalmente para la página web visualizada actualmente o habilitarlo permanentemente. Para permitir que el contenido activo se ejecute temporalmente en Internet Explorer, haga clic en la barra de información que aparece de manera predeterminada en la parte superior de la página web y después haga clic en **Permitir el contenido bloqueado**.

***Para habilitar el contenido activo de forma permanente***

en Internet Explorer

1. En el menú **Herramientas**, haga clic en **Opciones de Internet** y después en la pestaña **Avanzado**.
2. Seleccione la casilla de verificación **Permitir que el contenido activo se ejecute en los archivos en Mi PC** debajo de **Seguridad**.
3. Haga clic en **Aceptar**.

en Mozilla FireFox

1. En el menú **Opciones**, haga clic en **Contenido.**
2. Asegúrese de que la casilla de verificación **Habilitar JavaScript** esté seleccionada.
3. Haga clic en **Aceptar**.

## 7.2 Configuración de los componentes de Acronis Backup & Recovery 10

Existen tres maneras de configurar varios parámetros de los componentes de Acronis Backup & Recovery 10 en Windows:

- Utilizando la Plantilla Administrativa Acronis.
- Utilizando la interfaz gráfica de usuario (GUI).
- Modificando el registro de Windows.

En Linux, en vez de utilizar la plantilla administrativa y modificar el registro, los parámetros se configuran editando los archivos de configuración correspondientes.

Si los valores de cualquier de estos parámetros establecidos a través de la plantilla administrativa difieren de aquellos establecidos por la interfaz de usuario gráfico, los parámetros con base en la

plantilla toman precedente y se hacen efectivos de modo inmediato; los parámetros que se muestran en el GUI cambiarán en consecuencia..

Los siguientes subtemas describen todas las maneras de configuración y los parámetros que pueden configurarse a través de ellas.

### 7.2.1 Parámetros establecidos a través de la plantilla administrativa

Los siguientes son los parámetros de Acronis Backup & Recovery 10 los componentes que pueden establecerse utilizando Acronis la plantilla administrativa. Para obtener información sobre cómo solicitar la plantilla administrativa, ver cómo cargar Acronis la plantilla administrativa (pág. 360).

La plantilla administrativa contiene los parámetros de configuración del Acronis Backup & Recovery 10 Agente, el Acronis Backup & Recovery 10 Management Server y el Acronis Backup & Recovery 10 Storage Node, como se describe en los subtemas correspondientes a este tema.

#### Cómo cargar Acronis Administrative Template

La plantilla administrativa, proporcionada por Acronis, permite el ajuste de algunas funciones relacionadas con la seguridad, incluyendo ajustes de comunicación cifrada. A través del mecanismo de políticas de grupo de Microsoft, los ajustes de política de plantilla pueden aplicarse a un único equipo así como a un dominio.

***Para cargar Acronis Administrative Template***

1. Ejecute el editor de objetos de políticas de grupo de Windows (%windir%\system32\gpedit.msc.)
2. Abra el objeto de políticas de grupo (GPO) que desea editar.
3. Expanda **Configuración del equipo**.
4. Haga clic con el botón derecho en **Plantillas administrativas**.
5. Haga clic en **Agregar/Quitar plantillas**.
6. Haga clic en **Añadir**.
7. Buscando la plantilla administrativa Acronis (\Program files\Common Files\Acronis\Agent\Acronis_agent.adm o \Program files\Acronis\BackupAndRecoveryConsole\Acronis_agent.adm), y haga clic en **Abrir**.

Una vez que la plantilla está cargada, puede abrirla y editar los ajustes deseados. Tras cargar la plantilla o editar sus ajustes, deberá reiniciar el (los) componente(s) configurado(s) o algunos de sus servicios.

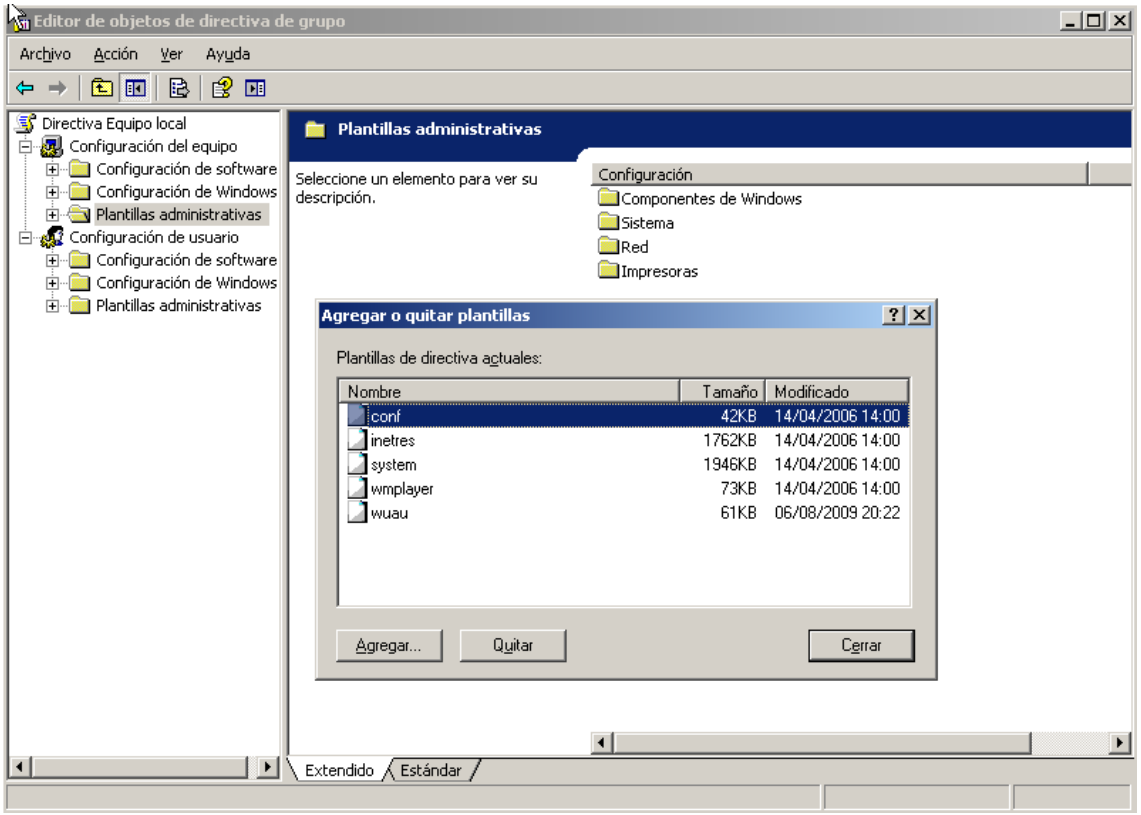
Para obtener información detallada sobre el Editor de objetos de políticas de grupo de Windows, consulte:

http://msdn2.microsoft.com/es-es/library/aa374163.aspx

Para obtener información detallada sobre las políticas de grupo, consulte:

http://msdn2.microsoft.com/es-es/library/aa374177.aspx




## Acronis Backup & Recovery 10 Storage Node

Los siguientes son los parámetros de Acronis Backup & Recovery 10 Storage Node que pueden establecerse por medio de Acronis Administrative Template.

**Límite de conexión del cliente**

*Descripción:*Especifica el número máximo de conexiones simultáneas para el nodo de almacenamiento por los agentes que realizan la copia de seguridad o recuperación.

*Valores posibles:* Cualquier número entero entre **1** y **2147483647.**

*Valor predeterminado:* **10.**

Los agentes Acronis Backup & Recovery 10 se conectan al nodo de almacenamiento para acceder a sus bóvedas de gestión durante la copia de seguridad o recuperación. El parámetro de **Límite de Conexión de Cliente** determina el número máximo de dichas conexiones que el nodo de almacenamiento puede manejar de manera simultanea.

Cuando se alcanza este límite, el nodo de almacenamiento utiliza la cola de copias de seguridad (consulte el siguiente parámetro) para los agentes que están a la espera de la conexión.

**Límite de cola de copia de seguridad**

*Descripción:* Especifica la cantidad máxima de los componentes de Acronis Backup & Recovery 10 en la cola de copia de seguridad del nodo de almacenamiento.

*Valores posibles:* Cualquier número entero entre **1** y **2147483647.**

*Valor predeterminado:* **50.**

La cola de copias de seguridad es una lista de componentes de Acronis Backup & Recovery 10 que están esperando una conexión al nodo de almacenamiento o están actualmente conectados a él (consulte el parámetro anterior).

Cuando la cantidad de componentes en la cola de copia de seguridad es igual al valor en **Límite de cola de copia de seguridad** y otro componente intenta establecer una conexión, el nodo de almacenamiento no pone al componente en la cola.

En este caso, la conexión del componente al nodo de almacenamiento fallará. Si el componente es un Acronis Backup & Recovery 10 Agent, la tarea de copia de seguridad o recuperación correspondiente se detendrá en el estado **Fallido.**

**Advertencias y límites de bóveda**

Especifique la cantidad de espacio libre en una bóveda (tanto como valor absoluto y porcentaje) debajo del cual una advertencia o error se registra.

Este parámetro contiene la siguiente configuración:

**Límite de advertencia de espacio libre de la bóveda**

*Descripción:* Especifica la cantidad de espacio libre en la bóveda gestionada, en megabytes, debajo de la cual se registra una advertencia en el registro del nodo de almacenamiento.

*Valores posibles:* cualquier número entero entre **0** y **2147483647.**

*Valor predeterminado:* **200.**

El espacio libre de una bóveda es la cantidad de espacio libre en el medio, como el volumen de un disco, que se almacena en la bóveda.

Cuando la cantidad de espacio libre en una bóveda es igual o menor al valor en **Límite de advertencia de espacio libre en la bóveda** se registra una advertencia en el registro del nodo de almacenamiento, que indica la bóveda en cuestión. Puede ver las advertencias del nodo de almacenamiento en el Tablero.

**Porcentaje de advertencia de espacio libre de la bóveda.**

*Descripción:* Especifica la cantidad de espacio libre en un bóveda gestionada, como un porcentaje de su tamaño total, por debajo de la cual se registra una advertencia en el registro del nodo de almacenamiento.

*Valores posibles:* cualquier número entero entre **0** y **100.**

*Valor predeterminado:* **10.**

El tamaño total de una bóveda el espacio libre de la bóveda más el tamaño de todos los archivos comprimidos que se encuentran en la bóveda.

Por ejemplo, supongamos que dos bóvedas, Bóveda A y Bóveda B, están ambas almacenadas en el volumen de un disco. Supongamos además que el tamaño de los archivos comprimidos en la Bóveda A es de 20 GB y el tamaño de los archivos comprimidos en la Bóveda B es de 45 GB.

Si el volumen es de 5 GB de espacio libre, entonces el tamaño total de la Bóveda A es de 20 GB + 5 GB = 25 GB, y el de la Bóveda B es 45 GB + 5 GB = 50 GB, sin importar el tamaño del volumen.

El porcentaje de espacio libre en una bóveda es el espacio libre de la bóveda dividido por el tamaño total de la bóveda. En el ejemplo anterior, la BóvedaA tiene 5 GB / 25 GB = 20% de espacio libre y la Bóveda B tiene 5 GB / 50 GB = 10% de espacio libre.

Cuando el porcentaje de espacio libre en una bóveda es igual o menor al valor en **Porcentaje de advertencia de espacio libre en la bóveda** se registra una advertencia en el registro del nodo de almacenamiento, que indica la bóveda en cuestión. Puede ver las advertencias del nodo de almacenamiento en el Tablero.

***Nota:*** *Los parámetros* ***Límite de advertencia de espacio libre de la bóveda*** *y el* ***Porcentaje de advertencia de espacio libre de una bóveda*** *son independientes de cada uno: se registrará una advertencia cada vez que se alcance cualquiera de los umbrales.*

**Límite de error de espacio libre de la bóveda**

*Descripción:* Especifica la cantidad de espacio libre en una bóveda gestionada, en megabytes, por debajo de la cual se registra un error en el registro de nodo de almacenamiento y queda prohibida toda copia de seguridad de la bóveda.

*Valores posibles:* cualquier número entero entre **0** y **2147483647.**

*Valor predeterminado:* **50.**

Cuando la cantidad de espacio libre en una bóveda es igual o menor al valor en **Límite de error de espacio libre en la bóveda** se registra un error en el registro del nodo de almacenamiento. Las copias de seguridad de la bóveda continuará fallando hasta que el espacio libre de la bóveda se encuentre por encima del límite.

**Límite de advertencia de espacio libre de la base de datos de la bóveda.**

*Descripción:* Especifica la cantidad de espacio libre, en megabytes, del volumen que contiene una base de datos de una bóveda gestionada, por debajo de la cual se registra una advertencia en el registro del nodo de almacenamiento.

*Valores posibles:* cualquier número entero entre **0** y **2147483647.**

*Valor predeterminado:* **20.**

Si la cantidad de espacio libre del volumen que contiene una base de datos de una bóveda gestionada es menor que el valor en **límite de advertencia de espacio libre de la base de datos de la bóveda**, se registra una advertencia en el registro del nodo de almacenamiento, indicando la bóveda en cuestión. Puede ver las advertencias del nodo de almacenamiento en el Tablero.

La base de datos se almacena en el nodo de almacenamiento en una carpeta local cuyo nombre está especificado en **Ruta de base de datos** cuando se crea la bóveda.

**Límite de error de espacio libre de la base de datos de la bóveda**

*Descripción:* Especifica la cantidad de espacio libre en el volumen que contiene la base de datos de una bóveda, en megabytes, por debajo de la cual se registra un error en el registro de nodo de almacenamiento y se prohíbe toda copia de seguridad de la bóveda.

*Valores posibles:* cualquier número entero entre **0** y **2147483647.**

*Valor predeterminado:* **10.**

Si la cantidad de espacio libre en el disco que contiene la base de datos de la bóveda gestionada es menor que el valor en **Límite de error de espacio libre de la base de datos de la bóveda**, se registra un error en el registro del nodo de almacenamiento. Las copias de seguridad de la bóveda continuará fallando hasta que la cantidad de espacio libre se encuentre por encima del límite.

Puede ver los errores del nodo de almacenamiento en el Tablero.

La base de datos se almacena en el nodo de almacenamiento en una carpeta local cuyo nombre se especifica en la **la ruta de la base de datos** al crearse la bóveda.

## Acronis Backup & Recovery 10 Management Server

Los siguientes son los parámetros de Acronis Backup & Recovery 10 Management Server que pueden configurarse con Acronis Administrative Template.

**Recopilación de registros**

Especifica cuándo recopilar las entradas del registro de los equipos gestionados por Acronis Backup & Recovery 10 Management Server.

Este parámetro tiene dos ajustes:

**Rastrear estado**

*Descripción:* Especifica si recopilar las entradas del registro acerca de los eventos de los componentes de los equipos registrados.

*Valores posibles:* **Verdadero** o **falso.**

*Valor predeterminado:* Verdadero.

**Rastrear nivel**

*Descripción:* Especifica el nivel mínimo de gravedad de las entradas recopiladas. solo se recopilarán las entradas de niveles más altos o iguales al valor de **Nivel del rastreo**.

*Valores posibles:* **0** (Evento interno), **1** (Información de depuración), **2** (Información), **3** (Advertencia), **4** (Error) o **5** (Error crítico).

*Valor predeterminado:* 0 (se recopilarán todos las entradas).

**Reglas de limpieza de los registros**

Especifica cómo limpiar el registro de eventos centralizado almacenado en la base de datos de informes del servidor de gestión.

Este parámetro contiene las siguientes configuraciones:

**Tamaño máximo**

*Descripción:* especifica el tamaño máximo del registro de eventos centralizado en kilobytes.

*Valores posibles:* Cualquier número entero entre **0** y **2147483647.**

*Valor predeterminado:* **1048576** (es decir, 1 GB).

**Porcentaje a conservar**

*Descripción:* especifica el porcentaje del tamaño máximo del registro para mantener durante la limpieza

*Valores posibles:* Cualquier número entero entre **0** y **100.**

*Valor predeterminado:* **95.**

Para obtener información sobre cómo se limpia el registro de eventos centralizado, consulte las Reglas de limpieza de los registros (pág. 87).

**Registro de sucesos de Windows**

Especifica cuándo registrar los eventos de Acronis Backup & Recovery 10 Management Server en el Registro de sucesos de aplicación en Windows.

Este parámetro tiene dos ajustes:

**Rastrear estado**

*Descripción:*Especifica si registrar los eventos de Acronis Backup & Recovery 10 Management Server en el registro de sucesos.

*Valores posibles:* **Verdadero** o **falso.**

*Valor predeterminado:* False.

**Rastrear nivel**

*Descripción:* Especifica el nivel mínimo de gravedad de los eventos que se registrarán en el registro de sucesos. Solo se registrarán los eventos de niveles más altos o iguales al valor de **Rastrear nivel**.

*Valores posibles:* **0** (Evento interno), **1** (Información de depuración), **2** (Información), **3** (Advertencia), **4** (Error) o **5** (Error crítico).

*Valor predeterminado:* **4** (solo se registrarán errores y errores críticos, si se establece que el **Estado del rastreo** es **Verdadero**).

**SNMP**

Especifica los tipos de eventos del servidor de gestión para enviar notificaciones por medio del Protocolo de administración de red simple (SNMP).

Este parámetro contiene la siguiente configuración:

**Rastrear estado**

*Descripción:* Especifica si enviar notificaciones SNMP.

*Valores posibles:* **Verdadero** o **falso.**

*Valor predeterminado:* False.

**Rastrear nivel**

*Descripción:* Especifica el nivel mínimo de gravedad de los eventos para enviar notificaciones SNMP al respecto. Solo se enviarán los eventos de niveles más altos o iguales al valor de **Rastrear nivel**.

*Valores posibles:* **0** (Evento interno), **1** (Información de depuración), **2** (Información), **3** (Advertencia), **4** (Error) o **5** (Error crítico).

*Valor predeterminado:* 4 (solo se enviarán errores y errores críticos, si se establece que **Rastrear estado** es **Verdadero**).

**Dirección SNMP**

*Descripción:* Especifica el nombre de red o dirección IP del servidor SNMP.

*Valores posibles:* cualquier cadena de 0 a 32765 caracteres de largo.

*Valor predeterminado:* cadena vacía.

**Comunidad SNMP**

*Descripción:* Especifica el nombre de la comunidad para las notificaciones SNMP.

*Valores posibles:* cualquier cadena de 0 a 32765 caracteres de largo.

*Valor predeterminado:* public.

**Sincronización**

Especifica cómo Acronis Backup & Recovery 10 Management Server se conecta a los equipos registrados para la implementación de políticas centralizadas, la recuperación de registros y estados de planes de copia de seguridad y acciones similares; conjuntamente llamados sincronización.

Este parámetro contiene las siguientes configuraciones:

**Conexiones máximas**

*Descripción:* Especifica la cantidad máxima de conexiones de sincronización simultáneas que se deben mantener.

*Valores posibles:* Cualquier número entero entre 1 y 500.

*Valor predeterminado:* 200.

si la cantidad total de equipos registrados en línea no excede el valor de **Conexiones máximas**, siempre se mantienen las conexiones con esos equipos y el servidor de gestión se sincroniza periódicamente con cada equipo.

De lo contrario, se conecta a una cantidad de equipos registrados dependiendo de la cantidad asignada de conexiones simultáneas. Después de que la sincronización con un equipo se haya completado, el servidor de gestión puede desconectarse de ese equipo y utilizar la conexión libre para sincronizarse con otro equipo, y así sucesivamente.

(Nota: Es probable que siempre se conserven las conexiones a equipos con alta prioridad de sincronización - Ver a continuación **Período-Prioridad alta** en este tema.)

Las conexiones de sincronización no están relacionadas con aquellas entre Acronis Backup & Recovery 10 Management Server y Acronis Backup & Recovery 10 Management Console.

**Trabajadores máximos**

*Descripción:* Especifica la cantidad máxima de cadenas que se utilizan para la sincronización.

*Valores posibles:* Cualquier número entero entre 1 y 100.

*Valor predeterminado:* 30.

El proceso del servidor de gestión utiliza subprocesos especiales (llamados subprocesos para trabajadores o trabajadores) para realizar la sincronización con un equipo registrado que está conectado para la sincronización.

Cada trabajador realiza la sincronización para exactamente un equipo al mismo tiempo.

Un equipo conectado para sincronizar espera a un trabajador disponible. Por esta razón, la cantidad real de trabajadores nunca excederá la cantidad máxima de conexiones (consulte **Conexiones máximas** descritas anteriormente).

**Período (en segundos)**

*Descripción:* Especifica con qué frecuencia, en segundos, realizar la sincronización de los equipos que poseen una prioridad de sincronización normal, normalmente los equipos sin tareas de copia de seguridad centralizadas actualmente en ejecución.

*Valores posibles:* Cualquier número entero entre 120 y 2147483647.

*Valor predeterminado:* 120.

Acronis Backup & Recovery 10 Management Server intenta realizar la sincronización para cada equipo con prioridad normal una vez en la cantidad de segundos estipulados por **Periodo** al utilizar la cadena de trabajadores disponible (consulte **Trabajadores máximos** descrito anteriormente).

Si hay menos subprocesos trabajadores que equipos de prioridad normal, el intervalo real entre las sincronizaciones puede ser más largo que el valor de este parámetro.

**Período- Alta Prioridad (en segundos)**

*Descripción:* Especifica con qué frecuencia, en segundos, realizar la sincronización de los equipos que poseen una prioridad de sincronización alta, normalmente los equipos con que tareas de copia de seguridad centralizadas actualmente en ejecución.

*Valores posibles:* Cualquier número entero entre 15 y 2147483647.

*Valor predeterminado:* 15.

Este parámetro es análogo con el parámetro de **Periodo** descrito anteriormente.

**Monitorización en tiempo real**

*Descripción:* Especifica si llevar a cabo la supervisión en tiempo real de los equipos registrados con el mecanismo de sondeo.

*Valores posibles:* **Verdadero** o **falso.**

*Valor predeterminado:* False.

De manera predeterminada, Acronis Backup & Recovery 10 Management Server se conecta a los equipos registrados para llevar a cabo la sincronización, en especial, para recuperar datos

como los registros de la copia de seguridad. Este método se conoce como mecanismo de sondeo.

Si la **Monitorización en tiempo real** es **Verdadero**, el servidor de gestión en cambio envía solicitudes a los equipos para proporcionar nuevos datos cuando aparezcan y luego introduce un modo de escucha. Este método se llama monitorización en tiempo real.

La monitorización en tiempo real puede reducir tráfico en la red; por ejemplo, cuando las tareas de copia de seguridad centralizadas se ejecutan con poca frecuencia. Sin embargo, es eficaz solamente cuando hay relativamente pocos equipos registrados.

Evite habilitar la monitorización en tiempo real si la cantidad de equipos registrados excede la cantidad máxima de conexiones simultáneas (consulte **Conexiones máximas** anteriormente en este tema).

**Segundo intento de conexión**

*Descripción:* Especifica si intentar conectarse a un equipo registrado al utilizar su último dirección IP conocida después de que fallara un intento de conectarse al utilizar su nombre de servidor.

*Valores posibles:* **Verdadero** o **falso.**

*Valor predeterminado:* False.

Al conectarse a un equipo registrado, Acronis Backup & Recovery 10 Management Server primero utiliza el nombre de red del equipo, siempre que ese equipo se hubiera añadido al servidor de gestión por nombre.

Si el **Según intento de conexión** es **Verdadero** y una conexión al equipo ha fallado utilizando su nombre de red, el servidor de gestión realiza un segundo intento de conexión, esta vez utilizando la último dirección IP que se asoció al nombre de esa red.

Recomendamos configurar el **Segundo intento de conexión** a **Verdadero** solo en redes que frecuentemente experimentan problemas con sus servidores DNS y que las direcciones IP de los equipos cambien con poca frecuencia; como en casos de direcciones IP fijas o largos tiempos de DHCP arrendados.

Este ajuste no tiene efecto en equipos que se han agregado al servidor de gestión por la dirección IP.

**Umbral de período fuera de línea (en segundos)**

*Descripción:* Especifica el intervalo máximo, en segundos, entre los intentos de conectarse a un equipo registrado que parece estar fuera de línea.

*Valores posibles:* Cualquier número entero entre 120 y 2147483647.

*Valor predeterminado:* 1800.

Normalmente, el servidor de gestión se conecta a cada equipo registrado cada cierto intervalo de tiempo (Ver anteriormente en esta sección **Período** y **Período- Prioridad alta**). Cuando el servidor de gestión descubre que el equipo está fuera de línea, duplica este intervalo; continúa duplicando el intervalo en cada intento a continuación hasta alcanzar el valor especificado en **Umbral de Período fuera de línea**. Si el equipo vuelve a estar en línea, el intervalo de tiempo vuelve a ser el normal.

Este enfoque tiene como objetivo el uso eficiente de los recursos del servidor de gestión y la reducción de la carga de la red.

**Crear copia de seguridad**

Especifica la ubicación y el tamaño inicial de almacenamiento de la instantánea (un archivo temporal que se utiliza al realizar copias de seguridad de datos al tomar una instantánea). Este archivo se elimina tan pronto finaliza la copia de seguridad.

Con la configuración predeterminada, se crea el almacenamiento de instantáneas en la carpetas de archivos temporales de Windows y esta ocupa el 50 por ciento del espacio disponible en el volumen que contiene esa carpeta. Este tamaño puede aumentar después si se necesita más espacio para la instantánea.

Puede aumentar el tamaño inicial del almacenamiento de la instantánea (o colocarla en un volumen diferente) cuando surjan problemas al realizar la copia de seguridad de los datos que cambian en gran medida durante la copia de seguridad.

Este parámetro se utiliza cuando se crea una política de copias de seguridad y se aplica a todos los planes de copias de seguridad centralizados que se basarán en esa póliza. Los cambios de este parámetro no afectan a las políticas de copia de seguridad ya existentes (y a sus planes de copias de seguridad centralizados).

Este parámetro contiene las siguientes configuraciones:

**Ruta de almacenamiento de la instantánea**

*Descripción:* especifica la carpeta en la que se ubica el almacenamiento de la instantánea.

*Valores posibles:* cualquier cadena de 0 a 32765 caracteres de longitude.

*Valor predeterminado:* Cadena vacía.

Una cadena vacía significa una carpeta de archivos temporales, que se da normalmente con la variable de entorno TMP o TEMP.

Puede especificar una carpeta local en cualquier volumen, incluso el volumen del que está realizando la copia de seguridad.

**Tamaño absoluto del almacenamiento de la instantánea**

*Descripción:* especifica el tamaño inicial del almacenamiento de la instantánea en megabytes.

*Valores posibles:* Cualquier número entero entre **0** y **2147483647.**

*Valor predeterminado:* **0.**

Si este ajuste es **0**, el servidor de gestión utiliza el ajuste **Tamaño relativo del almacenamiento de la instantánea**.

El tamaño inicial no debe exceder el espacio disponible menos 50 MB.

**Tamaño relativo del almacenamiento de la instantánea**

Esta configuración es eficaz solamente cuando el ajuste **Tamaño absoluto del almacenamiento de la instantánea** es **0**.

*Descripción:* especifica el tamaño inicial del almacenamiento de la instantánea en forma de porcentaje del espacio del disco que está disponible cuando se inicia la copia de seguridad.

*Valores posibles:* Cualquier número entero entre **0** y **100.**

*Valor predeterminado:* **50.**

Si este ajuste es **0**, no se creará el almacenamiento de la instantánea.

El tamaño inicial no debe exceder el espacio disponible menos 50 MB.

Es posible tomar instantáneas sin el almacenamiento de las instantáneas.

El tamaño del almacenamiento de las instantáneas no afecta al tamaño de la copia de seguridad.

## Acronis Backup & Recovery 10 Agente para Windows

Los siguientes son los parámetros de Acronis Backup & Recovery 10 Agent que pueden establecerse utilizando Acronis Administrative Template.

### Licencia

Especifique con qué frecuencia el agente comprueba la licencia en el servidor de licencias y cuánto tiempo puede funcionar sin un servidor de licencias.

**Intervalo de comprobación dela licencia (en días)**

*Descripción:* Especifica con qué frecuencia, en días, se ha de comprobar la disponibilidad de licencias en Acronis License Server.

*Valores posibles:* cualquier número entero entre **0** y **5.**

*Valor predeterminado:* 1.

Acronis Backup & Recovery 10 Agent comprueba periódicamente si su clave de licencia se encuentra en el servidor de licencias. La primero comprobación se realiza cada vez que Acronis Backup & Recovery 10 Agent arranca y las siguientes comprobaciones se realizan una vez en la número de días establecidos por **Intervalo de comprobación de la licencia**.

Cuando el agente no pueda conectarse al servidor de licencias, se registra una advertencia en el registro del agente. Puede ver esta advertencia en el tablero.

Si el valor es **0**, no se realizará ninguna comprobación de la licencia; sin una licencia, la funcionalidad de Acronis Backup & Recovery 10 se deshabilitará después de la número de días especificados en **Tiempo máximo sin servidor de licencias** (consulte el siguiente parámetro).

Consulte también el **Intervalo de reintento para la conexión al servidor de licencias** más adelante en este tema.

**Tiempo máximo sin servidor de licencias (en días)**

*Descripción:* Especifica cuánto tiempo, en días, Acronis Backup & Recovery 10 funcionará como normal hasta deshabilitar su funcionalidad.

*Valores posibles:* cualquier número entero entre **0** y **60.**

*Valor predeterminado:* 30.

Si Acronis License Server no está disponible, Acronis Backup & Recovery 10 continuará funcionando con su funcionalidad completa durante la número de días especificados en **Tiempo máximo sin servidor de licencias**, que se cuenta a partir de la instalación y desde la último comprobación correcta.

**Intervalode reintento de conexiónal servidor de licencias (en horas)**

*Descripción:* Especifica el intervalo, en horas, entre los intentos de conexión cuando Acronis License Server no está disponible.

*Valores posibles:* cualquier número entero entre **0** y **24.**

*Valor predeterminado:* 1.

Si, durante una comprobación de la clave de licencia (consulte **Intervalo de comprobación de la licencia** antes en este tema), Acronis Backup & Recovery 10 Agent no pudo conectarse con el servidor de licencias, intentará reconectarse una vez en la número de días especificado en **Intervalo de reintento de conexión al servidor de licencias**.

Si el valor es **0**, no se realizarán reintentos; el agente solo verificará las licencias como lo determina el **Intervalo de verificación de licencias**.

**Dirección del servidor de licencias**

*Descripción:* Especifica el nombre de red o dirección IP de Acronis License Server.

*Valores posibles:* cualquier cadena de 0 a 32765 caracteres de largo.

*Valor predeterminado:* cadena vacía.

**Reglas de limpieza de los registros**

Especifica cómo limpiar el registro del agente.

Este parámetro contiene las siguientes configuraciones:

**Tamaño máximo**

*Descripción:* especifica el tamaño máximo del registro del agente en kilobytes.

*Valores posibles:* cualquier número entero entre **0** y **2147483647.**

*Valor predeterminado:* **1048576** (es decir, 1 GB).

**Porcentaje a conservar**

*Descripción:* especifica el porcentaje del tamaño máximo del registro para mantener durante la limpieza.

*Valores posibles:* cualquier número entero entre **0** y **100.**

*Valor predeterminado:* **95.**

Para obtener información sobre cómo se limpia el registro del agente, consulte las Reglas de limpieza de los registros (pág. 94).

**Registro de sucesos de Windows**

Especifica cuándo registrar los eventos de Acronis Backup & Recovery 10 Agent en el Registro de sucesos de aplicación en Windows.

Este parámetro tiene dos ajustes:

**Rastrear estado**

*Descripción:* Especifica si registrar los eventos del agente en el registro de sucesos.

*Valores posibles:* **Verdadero** o **falso.**

*Valor predeterminado:* False.

**Rastrear nivel**

*Descripción:* Especifica el nivel mínimo de gravedad de los eventos que se registrarán en el registro de sucesos. Solo se registrarán los eventos de niveles más altos o iguales al valor de **Rastrear nivel**.

*Valores posibles:* **0** (Evento interno), **1** (Información de depuración), **2** (Información), **3** (Advertencia), **4** (Error) o **5** (Error crítico).

*Valor predeterminado:* **4** (solo se registrarán errores y errores críticos, si se establece que el **Estado del rastreo** es **Verdadero**).

**SNMP**

Especifica los tipos de eventos del agente para enviar notificaciones por medio del Protocolo simple de administración de red (SNMP).

Este parámetro contiene las siguientes configuraciones:

**Rastrear estado**

*Descripción:* Especifica si enviar notificaciones SNMP.

*Valores posibles:* **Verdadero** o **falso.**

*Valor predeterminado:* False.

**Rastrear nivel**

*Descripción:* Especifica el nivel mínimo de gravedad de los eventos para enviar notificaciones SNMP al respecto. Solo se enviarán los eventos de niveles más altos o iguales al valor de **Rastrear nivel**.

*Valores posibles:* **0** (Evento interno), **1** (Información de depuración), **2** (Información), **3** (Advertencia), **4** (Error) o **5** (Error crítico).

*Valor predeterminado:* **4** (solo se registrarán errores y errores críticos, si se establece que el **Estado del rastreo** es **Verdadero**).

**Dirección SNMP**

*Descripción:* Especifica el nombre de red o dirección IP del servidor SNMP.

*Valores posibles:* cualquier cadena de 0 a 32765 caracteres de largo.

*Valor predeterminado:* cadena vacía.

**Comunidad SNMP**

*Descripción:* Especifica el nombre de la comunidad para las notificaciones SNMP.

*Valores posibles:* cualquier cadena de 0 a 32765 caracteres de largo.

*Valor predeterminado:* público.

**Crear copia de seguridad**

Especifica la ubicación y el tamaño inicial de almacenamiento de la instantánea (un archivo temporal que se utiliza al realizar copias de seguridad de datos al tomar una instantánea). Este archivo se elimina tan pronto finaliza la copia de seguridad.

Con la configuración predeterminada, se crea el almacenamiento de instantáneas en la carpetas de archivos temporales de Windows y esta ocupa inicialmente el 50 por ciento del espacio disponible en el volumen que contiene esa carpeta. Este tamaño puede aumentar después si se necesita más espacio para la instantánea.

Puede aumentar el tamaño inicial del almacenamiento de la instantánea (o colocarla en un volumen diferente) cuando surjan problemas al realizar la copia de seguridad de los datos que cambian en gran medida durante la copia de seguridad.

Este parámetro se utiliza cuando se crea un plan de copias de seguridad. Los cambios de este parámetro no afectan a los planes de copias de seguridad ya existentes.

Este parámetro contiene las siguientes configuraciones:

**Ruta de almacenamiento de la instantánea**

*Descripción:* especifica la carpeta en la que se crea el almacenamiento de la instantánea.

*Valores posibles:* cualquier cadena de 0 a 32765 caracteres de longitude.

*Valor predeterminado:* Cadena vacía.

Una cadena vacía significa una carpeta de archivos temporales, que se da normalmente con la variable de entorno TMP o TEMP.

Puede especificar una carpeta local en cualquier volumen, incluso el volumen del que está realizando la copia de seguridad.

**Tamaño absoluto del almacenamiento de la instantánea**

*Descripción:* especifica el tamaño inicial del almacenamiento de la instantánea en megabytes.

*Valores posibles:* cualquier número entero entre **0** y **2147483647.**

*Valor predeterminado:* **0.**

Si este ajuste es **0**, el servidor de gestión utiliza el ajuste **Tamaño relativo del almacenamiento de la instantánea**.

El tamaño inicial no debe exceder el espacio disponible menos 50 MB.

**Tamaño relativo del almacenamiento de la instantánea**

Esta configuración es eficaz solamente cuando el ajuste **Tamaño absoluto del almacenamiento de la instantánea** es **0**.

*Descripción:* especifica el tamaño inicial del almacenamiento de la instantánea en forma de porcentaje del espacio del disco que está disponible cuando se inicia la copia de seguridad.

*Valores posibles:* cualquier número entero entre **0** y **100.**

*Valor predeterminado:* **50.**

Si este ajuste es **0**, no se creará el almacenamiento de la instantánea.

El tamaño inicial no debe exceder el espacio disponible menos 50 MB.

Es posible tomar instantáneas sin el almacenamiento de las instantáneas.

El tamaño del almacenamiento de las instantáneas no afecta al tamaño de la copia de seguridad.

## Acronis Backup & Recovery 10

Esta sección de la plantilla administrativa especifica los parámetros de conexión y los parámetros de seguimiento de evento para los siguientes componentes Acronis Backup & Recovery 10:

- Acronis Backup & Recovery 10 Management Server
- Acronis Backup & Recovery 10 Agent
- Acronis Backup & Recovery 10 Storage Node

### Parámetros de conexión

#### Puertos de agente remoto

Especifica el puerto que utilizará el componente para la comunicación entrante y saliente con otro componentes de Acronis.

Seleccione una de las siguientes opciones:

**No configurado**

El componente utilizará el número de puerto predeterminado TCP 9876.

**Habilitado**

El componente utilizará el puerto especificado; escriba el número de puerto en el cuadro de diálogo **Puerto TCP del servidor**.

**Deshabilitado**

Igual que **No configurado**.

#### Opciones de cifrado del cliente

Especifique si desea cifrar los datos transferidos cuando el componente actúa como aplicación cliente y si desea confiar en los certificados SSL autofirmados.

Seleccione una de las siguientes opciones:

**No configurado**

El componente utilizará los ajustes predeterminados, que se basan en la utilización del cifrado siempre que sea posible y en la confianza en los certificados SSL autofirmados (consulte la siguiente opción).

**Habilitado**

El cifrado está habilitado. En **Cifrado**, seleccione una de las siguientes opciones:

**Habilitado**

La transferencia de datos será cifrada si el cifrado se encuentra habilitado en la aplicación servidor, de otra manera, no se cifrará.

**Deshabilitado**

El cifrado está deshabilitado; no se establecerá ninguna conexión con una aplicación servidor que requiera cifrado.

**Obligatorio**

La transferencia de datos se llevará a cabo únicamente si el cifrado se encuentra habilitado en la aplicación servidor (consulte "Opciones de cifrado del servidor"); se cifrará.

*Parámetros de autenticación*

Activar la casilla de verificación **Confiar en certificados autofirmados** permite al cliente conectarse a las aplicaciones servidor que utilizan certificados SSL autofirmados tales como aquellos creados durante la instalación de los componentes de Acronis Backup & Recovery 10; consulte Certificados SSL (pág. 83).

Esta casilla de verificación deberá permanecer activada, a menos que disponga de una Infraestructura de clave pública (PKI) en su entorno.

En **Utilizar autenticación de certificado del agente**, seleccione una de las siguientes opciones:

**No utilizar**

La utilización de certificados SSL está deshabilitada. No se establecerá la conexión con ninguna aplicación servidor que requiera la utilización de certificados SSL.

**Utilizar si es posible**

La utilización de certificados SSL está habilitada. El cliente solo utilizará certificados SSL si su utilización está habilitada en la aplicación servidor.

**Siempre utilizar**

La utilización de certificados SSL está habilitada. La conexión se establecerá únicamente si la utilización de certificados SSL está habilitada en la aplicación servidor.

**Deshabilitado**

Igual que **No configurado**.

**Opciones de cifrado del servidor**

Especifica si desea cifrar los datos transferidos cuando el componente actúa como aplicación servidor.

Seleccione una de las siguientes opciones:

**No configurado**

El componente utilizará el ajuste predeterminado, el cual se basa en la utilización de cifrado siempre que sea posible (consulte la siguiente opción).

**Habilitado**

El cifrado está habilitado. En **Cifrado**, seleccione una de las siguientes opciones:

**Habilitado**

La transferencia de datos será cifrada solo si el cifrado se encuentra habilitado en la aplicación cliente.

**Deshabilitado**

El cifrado está deshabilitado; no se establecerá ninguna conexión con una aplicación cliente que requiera cifrado.

**Obligatorio**

La transferencia de datos se llevará a cabo solo si el cifrado está habilitado en la aplicación del cliente (consulte "Opciones de cifrado del cliente"); se encifrará.

*Parámetros de autenticación*

En **Utilizar autenticación de certificado del agente**, seleccione una de las siguientes opciones:

**No utilizar**

La utilización de certificados SSL está deshabilitada. No se establecerá ninguna conexión a la aplicación del cliente que requiera la utilización de certificados SSL.

**Utilizar si es posible**

La utilización de certificados SSL está habilitada. El servidor utilizará certificados SSL si su utilización está habilitada en la aplicación del cliente y no los utilizará de otra manera.

**Siempre utilizar**

La utilización de certificados SSL está habilitada. Se establecerá la conexión solo si la utilización de certificados SSL está habilitada en la aplicación del cliente.

**Deshabilitado**

Igual que **No configurado**.

### Parámetros de seguimiento de eventos

En Windows, los eventos que ocurren en Acronis Backup & Recovery 10 pueden guardarse en el registro de eventos, un archivo o en ambos.

Cada evento tiene un nivel de cero a cinco basado en la gravedad del evento, como muestra la siguiente tabla:

| Nivel | Nombre | Descripción |
|---|---|---|
| **0** | Desconocido | Evento cuyo grado de gravedad es desconocido o no aplicable |
| **1** | Depuración | Evento utilizado para fines de depuración |
| **2** | Información | Evento con fines informativos, como por ejemplo la finalización exitosa de una operación o el inicio de un servicio |
| **3** | Advertencia | Evento que sea probablemente un problema inminente, como una escasa cantidad de espacio libre en la bóveda |
| **4** | Error | Evento que tuvo por resultado una pérdida de datos o funcionalidad. |
| **5** | Crítico | Evento que resultó en la finalización de un proceso como el proceso del agente |

Los parámetros de seguimiento de eventos se especifican como los siguientes ajustes en la plantilla administrativa:

**Nivel mínimo de seguimiento de archivos**

*Descripción:* Especifica el nivel de gravedad mínimo de los eventos que se va a registrar en el archivo. Solo se registrarán los eventos de niveles mayores que o similares al **Nivel Mínimo de Seguimiento de Archivo**.

*Valores posibles:* Cualquier nivel de gravedad desde **Desconocido** a **Crítico**, o **Bloqueado** a no registrar evento alguno

*Valor predeterminado:* 2 (significa que se registrarán los niveles de gravedad dos a cinco)

Los archivos registrados se ubican dentro de la carpeta **%TODOSLOSPERFILESDEUSUARIO%\Application Data\Acronis**, en la subcarpeta **Registros** para un componente en particular.

**Nivel mínimo de seguimiento de archivo Win32**

*Descripción:* Especifica el nivel de gravedad mínimo de los eventos que se van a registrar en el registro de sucesos del sistema. Solo se registrarán los eventos de niveles mayores que o similares al **Nivel Mínimo de Seguimiento de Archivo**.

*Valores posibles:* Cualquier nivel de gravedad desde **Desconocido** a **Crítico**, o **Bloqueado** a no registrar evento alguno

*Valor predeterminado:* 4 (significa que se registrarán los eventos sobre errores o errores críticos).

**Programa de Experiencia del Cliente**

Especifica si el equipo en el que está instalado el componente de Acronis Backup & Recovery 10 participará en el Programa de Experiencia del Cliente.

Seleccione una de las siguientes opciones:

**No configurado**

De manera predeterminada, el equipo no participa en el Programa de Experiencia del Cliente.

**Habilitado**

En **Activar envío de informes a Acronis**, seleccione uno de los siguientes puntos:

**Habilitar**

La información sobre la configuración de hardware, las funciones que más y menos se utilizan, y cualquier tipo de problema se recopilarán automáticamente en el equipo y se enviarán a Acronis regularmente. Los resultados finales tienen como objetivo suministrar mejoras en el software y mayores funcionalidades para satisfacer mejor las necesidades de los clientes de Acronis. Acronis no recopila ningún dato personal. Puede ver los términos de participación en el sitio web de Acronis.

**Deshabilitar**

No se enviará la información.

**Deshabilitado**

Igual que **No configurado**.

## 7.2.2 Parámetros configurados a través de la GUI

Los siguientes parámetros pueden configurarse a través de la interfaz gráfica de usuario (GUI):

- Acronis Backup & Recovery 10 Management Server **Registros de información**, **Registros de eventos de Windows**, **SNMP**, **Dirección SNMP** y **Comunidad SNMP.**
- Acronis Backup & Recovery 10 Agent **Registro de eventos de Windows**, **SNMP**, **Dirección SNMP**, **Comunidad SNMP** y **Programa de Experiencia del Cliente.**

Encontrará la descripción de estos parámetros en el tema correspondiente sobre la configuración a través de la plantilla administrativa.

## 7.2.3 Parámetros establecidos a través del registro de Windows

Los siguientes son los parámetros de Acronis Backup & Recovery 10 Storage Node que puede configurarse únicamente editando el registro.

### Parámetro relacionado con la deduplicación

**Umbral delactivador decompatación**

*Descripción:* Especifica el porcentaje de elementos usados en el almacenamiento de datos por debajo del cual se lleva a cabo la compactación.

*Valores posibles:* cualquier número entero entre **0** y **100.**

*Valor predeterminado:* **80.**

*Clave de registro:*
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ASN\Configuration\StorageNode\CompactingTriggerThreshold

Según se van eliminando las copias de seguridad de una bóveda deduplicada, susalmacenamientos de datos deduplicados (pág. 70) pueden contener elementos no utilizados: archivos o bloques de disco que ya no hacen referencia a ninguna copia de seguridad. El nodo de almacenamiento procesa ambos almacenamientos de datos a la vez para eliminar los elementos no utilizados. Esta operación se denomina compactación.

Debido a que la compactación es una operación que consume recursos, debería darse únicamente cuando el número de elementos no utilizados sea significativo.

El parámetro del **UmbraldelActivadordeCompactación** le permite establecer un equilibrio entre el espacio extra requerido para almacenar elementos no utilizados y la frecuencia de compactación. Cuando más grande sea el valor de este parámetro, se permitirán menos elementos no utilizados en los almacenamientos de datos pero, en cambio, la compactación será más frecuente.

Este parámetro se aplica de forma separada a copias de seguridad de niveles de archivo y de niveles de disco. De manera que, la compactación se realizará para un almacenamiento de datos y será omitida para el otro.

### Parámetros relacionados con bases de datos de bóvedas.

Los dos siguientes parámetros determinan las rutas a las bases de datos internas de Acronis Backup & Recovery 10 Storage Node, las cuales contienen información acerca de las bóvedas gestionadas.

La base de datos ubicada en la carpeta especificada por el parámetro **DatabasePath** es generalmente pequeña. Sin embargo, la base de datos ubicada en la carpeta especificada por el parámetro **TapeDatabasePath** (denominada la base de datos de cintas), puede ser grande si la biblioteca de cintas contiene miles de archivos comprimidos. En este caso, puede almacenar la base de datos de cintas en un volumen diferente.

***Importante:*** *No recomendamos modificar estos parámetros. Si no necesita modificar ninguno de ellos, debe hacer esto antes de crear cualquier bóveda gestionada correspondiente (de cinta o no). De lo contrario, el nodo de almacenamiento perderá el acceso a esas bóvedas hasta que las adjunte nuevamente y volver a adjuntar una bóveda, especialmente una de desduplicación, puede tomar una cantidad de tiempo considerable.*

**Ruta de la base de datos**

*Descripción:* Especifica la carpeta donde el Acronis Backup & Recovery 10 nodo de almacenamiento almacena su base de datos de bóvedas que no son de cinta.

Esta base de datos contiene una lista de bóvedas que son gestionadas por el nodo de almacenamiento, diferentes a las bóvedas de cinta (consulte el siguiente parámetro). Su tamaño típico no excede unos cuantos kilobytes.

*Valores posibles:* cualquier cadena de 0 a 32765 caracteres de largo.

*Valor predeterminado:* C:\Program Files\Acronis\StorageNode.

*Clave de registro:*
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ASN\Configuration\StorageNode\DatabasePath.

**Ruta de la base de datos de cinta**

*Descripción:* Especifica la carpeta donde el Acronis Backup & Recovery 10 Storage Node almacena su base de datos de bóvedas que son de cinta.

Esta base de datos contiene una lista de bóvedas de cinta que son gestionadas por el nodo de almacenamiento. Su tamaño depende del número de archivos comprimidos almacenados en las bibliotecas de cinta y es aproximadamente igual a 10 MB por cada cien archivos comprimidos.

*Valores posibles:* cualquier cadena de 0 a 32765 caracteres de largo.

*Valor predeterminado:* C:\Documents and Settings\All Users\Application Data\Acronis\BackupAndRecovery\TapeLocation\.

*Clave de registro:* HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\TapesDatabasePath.

## 7.3 Creación de una política de copias de seguridad

Una política de copias de seguridad puede aplicarse a equipos Windows y Linux.

Para crear una política de copias de seguridad, siga los siguientes pasos.

### General

**Nombre de la política**

[Opcional] Introduzca un nombre único para la política de copias de seguridad. Un nombre pensado a conciencia le permitirá identificar una política entre las demás.

**Tipo de fuente**

Seleccione el tipo de elementos de los cuales realizará la copia de seguridad: **Disco/volúmenes** o **Archivos**.

**Credenciales de la política** (pág. 379)

[Opcional] Puede cambiar las credenciales de la cuenta de la política de ser necesario. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

**Comentarios de la política**

[Opcional] Escriba una descripción de la política de copias de seguridad. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

**Etiqueta**

[Opcional] Marque una etiqueta de texto para el equipo/s al que va a realizar la copia de seguridad. La etiqueta puede usarse para identificar el equipo o el grupo de equipos en diversos escenarios. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

### Qué incorporar en la copia de seguridad

**Elementos de los cuales realizará la copia de seguridad** (pág. 380)

Especifique los elementos de datos de los que desea realizar la copia de seguridad en los equipos donde se esté implementando la política. En cada equipo, el agente encontrará los elementos de datos que utilizan las reglas que especificó. Por ejemplo, si la regla de selección es [Todos los volúmenes], se incluirá todo el equipo en la copia de seguridad.

**Credenciales de acceso** (pág. 385)

[Opcional] Proporcione credenciales para los datos de origen si la cuenta de política de copias de seguridad no tiene permisos de acceso a los datos. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

**Exclusiones** (pág. 386)

[Opcional] Establezca exclusiones para los tipos de archivos específicos de los cuales no desea realizar una copia de seguridad. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

## Dónde realizar copias de seguridad

**Archivo comprimido** (pág. 387)

Especifique la ruta de la ubicación donde se almacenará el archivo de copia de seguridad y el nombre del archivo comprimido. Se recomienda que el nombre del archivo comprimido sea único dentro de la ubicación. La ubicación debe estar disponible en un momento en el que servidor de gestión comience a implementar la política.

**Credenciales de acceso** (pág. 388)

[Opcional] Proporcione credenciales para la ubicación si la cuenta de política de copias de seguridad no tiene permisos de acceso a los datos. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

**Comentarios de archivo comprimido**

[Opcional] Escriba comentarios para el archivo comprimido. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

## ¿Cómo crear copias de seguridad?

**Esquema de copias de seguridad** (pág. 389)

Especifique cuándo y cada cuánto tiempo realizará las copias de seguridad de sus datos, establezca el período durante el cual mantendrá los archivos de copia de seguridad en la ubicación seleccionada y establezca una programación para el procedimiento de limpieza del archivo comprimido. Utilice esquemas de copia de seguridad optimizados y conocidos, como Abuelo-padre-hijo (GFS) y Torres de Hanói, cree un esquema de copias de seguridad personalizado o realice copias de seguridad de una sola vez.

## Validación de archivos comprimidos

**Cuándo validar**

[Opcional] Defina cuándo y cada cuánto tiempo realizará la validación y si se desea validar todo el archivo comprimido o la última copia de seguridad del archivo.

## Opciones de la copia de seguridad

**Configuraciones**

[Opcional] Configure los parámetros de la operación de copia de seguridad, como los comandos pre/post copia de seguridad, el ancho de banda de red máximo asignado para el flujo de copia de seguridad o el nivel de compresión del archivo de copia de seguridad. Si no realiza ninguna acción en esta sección, se usarán los valores predeterminados (pág. 96) según lo establecido en servidor de gestión.

Después de que se modifique cualquiera de las configuraciones con respecto al valor predeterminado, aparecerá una nueva línea que mostrará el valor recientemente establecido. El estado de la configuración cambia de **Predeterminada** a **Personalizada**. Si modifica nuevamente la configuración, la línea mostrará el nuevo valor, a menos que el nuevo valor sea el predeterminado. Cuando se establece el valor predeterminado, la línea desaparece, de modo que siempre verá únicamente la configuración que difiere de los valores predeterminados en esta sección de la página **Crear política de copia de seguridad**.

Para restablecer toda la configuración a los valores predeterminados, haga clic en **Restablecer a los valores predeterminados**.

Durante la operación de copia de seguridad, se omitirán las opciones de copia de seguridad predeterminadas de los equipos registrados.

### Conversión a VM

Se aplica a: Copia de seguridad de **disco/volumen.**

No eficaz para equipos cuyo sistema operativo es de Linux.

Al configurar una conversión normal, se obtiene una copia del servidor o estación de trabajo en un equipo virtual que puede encenderse fácilmente si el equipo original falla. La conversión se puede realizar en cualquier equipo que esté registrado en el servidor de gestión y cuente con Acronis Backup & Recovery 10 Agent con la funcionalidad correspondiente. Debe almacenar el archivo comprimido en una ubicación compartida, como una carpeta de red o una bóveda gestionada, para que el otro equipo tenga acceso al mismo.

**Cuándo convertir** (pág. 232)

[Opcional] Especifique si deben convertirse todas las copias de seguridad completas, incrementales o diferenciales o la última copia de seguridad que se creó según la programación. Si es necesario, especifique la programación de la conversión.

**Servidor** (pág. 233)

Especifique el equipo que realizará la conversión. El equipo debe tener instalado Acronis Backup & Recovery 10 Agent para Windows, Agent para ESX/ESXi o Agent para Hyper-V.

**Servidor de virtualización** (pág. 233)

Aquí debe seleccionar el tipo y la ubicación del equipo virtual resultante. Las opciones disponibles dependerán del servidor que haya seleccionado en el paso anterior.

**Almacenamiento** (pág. 233)

Escoja el almacenamiento en el servidor de virtualización o la carpeta en la que deben colocarse los archivos del equipo virtual.

**VMs resultante**

Especifique un nombre para los equipos virtuales que se crearán. El nombre predeterminado consiste en variables que reflejan el nombre de la política y el nombre del equipo desde el cual se realizará la copia de seguridad. Puede añadir sufijos al nombre pero nunca eliminar variables, ya que cada equipo virtual debe tener un nombre distintivo y único.

**Carpeta en VMware vCenter**

Si es servidor de gestión está integrado con vCenter Server, las máquinas virtuales resultantes aparecerán en la carpeta de **Acronis Backups** en vCenter. Puede especificar una subcarpeta para los equipos resultantes de la ejecución de la política.

Después de haber llevado a cabo todos los pasos necesarios, haga clic en **Aceptar** para crear la política de copias de seguridad.

## 7.3.1 Credenciales de la política

Proporcione las credenciales con las que se ejecutarán las tareas centralizadas.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Utilice las credenciales de servicio de Acronis.**

     Las tareas se ejecutarán con la cuenta de servicio de Acronis, ya sea que se hayan iniciado manualmente o ejecutado según la programación.

- **Utilice las siguientes credenciales.**

  Las tareas se ejecutarán con las credenciales que especifique, ya sea que se hayan iniciado manualmente o ejecutado según la programación.

  Especifique:

  - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio).
  - **Contraseña**. La contraseña de la cuenta.

2. Haga clic en **Aceptar**.

Para obtener más información sobre las credenciales de servicio de Acronis, consulte la sección Permisos para los servicios de Acronis. (pág. 77)

Para obtener más información sobre las operaciones disponibles según los privilegios de usuario, consulte la sección Privilegios de usuario en un equipo gestionado (pág. 33).

## 7.3.2 Elementos de los cuales realizará la copia de seguridad

Especifique las reglas de selección para realizar una copia de seguridad de los elementos, seleccionadas en el campo **Tipo de origen** de la sección General.

Reglas de selección para los volúmenes de los cuales realizará la copia de seguridad (pág. 380).

Reglas de selección para los archivos de los cuales realizará la copia de seguridad (pág. 384).

### Reglas de selección para los volúmenes de los cuales realizará la copia de seguridad

Defina las reglas de selección de volúmenes, de acuerdo con las cuales los volúmenes se incluirán en las copias de seguridad en los equipos donde se aplicará la política.

***Para definir las reglas de selección de volúmenes***

En la primera línea, seleccione la regla de la lista o escríbala de forma manual. Para añadir otra regla, haga clic en la siguiente línea vacía y seleccione la regla de la lista, o escríbala de forma manual. El programa recuerda las reglas que escribió de forma manual y, la próxima vez que abra la ventana, estas reglas estarán disponibles en la lista.

En la siguiente tabla se explican las reglas predefinidas que pueden seleccionarse de la lista.

| Para incluir | En la columna Volúmenes: | Comentarios |
|---|---|---|
| **Volúmenes en Windows y Linux** | | |
| Todos los volúmenes | Escriba o seleccione: **[All Volumes]** | Se refiere a todos los volúmenes de los equipos que ejecutan Windows y todos los volúmenes montados en equipos que ejecutan Linux. |
| **Volúmenes en Windows** | | |
| Volumen C: | Escriba **C:** o selecciónelo de la lista | |
| Volumen del sistema | Escriba o seleccione: | El volumen del sistema contiene los archivos específicos de hardware que son necesarios para iniciar Windows, como Ntldr, |

| | | |
|---|---|---|
| | **[SYSTEM]** | Boot.ini y Ntdetect.com.<br>Únicamente habrá un volumen del sistema, incluso si están instalados varios sistemas operativos de Windows en el equipo.<br>Para obtener más detalles, consulte "Nota sobre equipos de Windows", a continuación. |
| Volumen de inicio | Escriba o seleccione: **[BOOT]** | Hace referencia al volumen de inicio del equipo registrado.<br>El volumen de inicio contiene la carpeta Windows y los archivos de compatibilidad del sistema operativo de Windows (por lo general, ubicados en la carpeta Windows\System32). Es posible que no sea lo mismo que el volumen del sistema.<br>Si el equipo tiene varios sistemas operativos instalados, este es el volumen de inicio del sistema operativo en que el agente está trabajando.<br>Para obtener más detalles, consulte "Nota sobre equipos de Windows", a continuación. |
| Todos los volúmenes fijos | Escriba o seleccione: **[Fixed Volumes]** | Se refiere a todos los volúmenes que no sean medios extraíbles. Los volúmenes fijos incluyen dispositivos SCSI, ATAPI, ATA, SSA, SAS y SATA, y conjuntos RAID. |
| **Volúmenes Linux** | | |
| Primera partición del primer disco duro IDE de un equipo Linux | Escriba o seleccione: **/dev/hda1** | hda1 es el nombre estándar del dispositivo para la primera partición de la primera unidad de disco duro IDE. Para obtener más detalles, consulte "Nota sobre equipos de Linux", a continuación. |
| Primera partición del primer disco duro SCSI de un equipo Linux | Escriba o seleccione: **/dev/sda1** | sda1 es el nombre estándar del dispositivo para la primera partición de la primera unidad de disco duro SCSI. Para obtener más detalles, consulte "Nota sobre equipos de Linux", a continuación. |
| Primera partición del primer disco duro RAID de software de un equipo Linux | Escriba o seleccione: **/dev/md1** | md1 es el nombre estándar del dispositivo para la primera partición de la primera unidad de RAID de software. Para obtener más detalles, consulte "Nota sobre equipos de Linux", a continuación. |

Los nombres de las plantillas distinguen entre mayúsculas y minúsculas.

**¿Qué almacena una copia de seguridad de un disco o volumen?**

Para los sistemas de archivos compatibles, una copia de seguridad de un disco o volumen almacena solo los sectores que contienen datos. Esto reduce el tamaño de la copia de seguridad resultante y acelera las operaciones de copia de seguridad y recuperación.

**Windows**

Las copias de seguridad no incluyen el archivo de intercambio (pagefile.sys) ni el archivo que mantiene el contenido de la memoria RAM cuando el equipo está en estado de hibernación (hiberfil.sys). Después de la recuperación, los archivos se pueden volver a crear en el lugar apropiado con el tamaño cero.

Una copia de seguridad de volúmenes almacena todos los archivos y las carpetas del volumen seleccionado, independientemente de sus atributos (incluidos los archivos ocultos y del sistema), el registro de inicio, la tabla de asignación de archivos (FAT) si existe, la raíz y la pista cero del disco duro con el registro de inicio maestro (MBR). El código de inicio de los volúmenes GPT no se incluye en la copia de seguridad.

Un copia de seguridad del disco almacena todos los volúmenes del disco seleccionado (incluidos volúmenes ocultos como las particiones de mantenimiento del proveedor) y la pista cero con el registro de inicio maestro.

**Linux**

Una copia de seguridad de volúmenes almacena todos los archivos y las carpetas del volumen seleccionado independientemente de sus atributos, un registro de inicio y el superbloque del sistema de archivos.

Una copia de seguridad del disco almacena todos los volúmenes del disco y también la pista cero junto con el registro de inicio maestro.

Los volúmenes con sistemas de archivos no compatibles se incluyen en la copia de seguridad sector por sector.

**Nota sobre equipos de Windows**

Los sistemas operativos de Windows anteriores a Windows 7 y Windows Server 2008 R2 conservan los archivos del sistema y el cargador en el mismo volumen, a menos que se haya especificado un volumen diferente durante la instalación del sistema. Si los archivos de Windows y el cargador están en el mismo volumen, seleccione **[SISTEM]** o **[BOOT]** para crear una copia de seguridad del sistema operativo completo. De lo contrario, seleccione ambos, **[SISTEM]** e **[BOOT]**.

Los sistemas operativos a partir de Windows 7 y Windows Server 2008 R2 crean un volumen de sistema específico, denominado **Sistema reservado**. Si selecciona **[SISTEM]**, sólo se creará una copia de seguridad de este volumen específico. Seleccione siempre tanto **[SISTEM]** como **[BOOT]** para crear copias de seguridad de estos sistemas operativos.

Dado que las políticas de copia de seguridad normalmente se aplican a múltiples equipos con diversos sistemas operativos, Acronis recomienda que siempre seleccione los volúmenes de sistema e inicio para la creación de copias de seguridad, con el fin de garantizar la integridad de cada sistema operativo.

**Nota sobre equipos Linux**

Se pueden incluir volúmenes Windows y Linux (particiones) en una política de copia de seguridad centralizada.

Por ejemplo, es posible establecer una política para que realice una copia de seguridad del volumen **C:** en equipos Windows y la partición **/dev/hda1** en equipos Linux.

A diferencia de Windows, en Linux no hay una distinción precisa entre un volumen (partición) y una carpeta (directorio). Linux tiene la partición raíz (representada por /) a la que se conectan (montan) elementos de varios tipos —incluidos discos duros, directorios y dispositivos del sistema— lo que forma un árbol similar a la estructura de archivos y carpetas en Windows.

Por ejemplo, supongamos que un equipo Linux contiene un disco duro que se divide en tres volúmenes o particiones: la primera, la segunda y la tercera partición. Estas particiones están disponibles en el árbol como /dev/hda1, /dev/hda2 y /dev/hda3, respectivamente. Para realizar una copia de seguridad de un disco, digamos, de la tercera partición, se puede escribir /dev/hda3 en la fila del cuadro de diálogo **Reglas de selección para los volúmenes de los cuales se realizará la copia de seguridad**.

Además, una partición en Linux puede montarse en cualquier lugar dentro del árbol. Es decir, /dev/hda3 puede montarse como un “subdirectorio” dentro del árbol, como /home/usr/docs. En

este caso, se puede escribir /dev/hda3 o /home/usr/docs en el campo Volumen para realizar una copia de seguridad de la tercera partición de un disco.

En general, al configurar una política centralizada para realizar copias de seguridad del volumen en equipos Linux, compruebe que las rutas que introduce en el campo Volumen correspondan a las particiones (como /dev/hda2 o /home/usr/docs en el ejemplo anterior) y no a los directorios.

### Nombres estándares para particiones en Linux

Los nombres como /dev/hda1 reflejan la manera estándar de nombrar las particiones de disco duro IDE en Linux. El prefijo "hd" representa el tipo de disco (IDE), "a" significa que es el primer disco duro IDE en el sistema y "1" denota la primera partición en el disco.

En general, el nombre estándar para una partición en Linux consiste en tres componentes:

- Tipo de disco: hd para dispositivos IDE, sd para dispositivos SCSI, md para dispositivos RAID de software (por ejemplo, volúmenes dinámicos);
- Número del disco: a para el primer disco, b para el segundo disco, etc.;
- Número de partición en el disco: 1 para la primera partición, 2 para la segunda partición, etc.

Para garantizar que se realice la copia de seguridad de los discos seleccionados, independientemente de su tipo, considere incluir tres entradas en el cuadro de diálogo **Reglas de selección para los volúmenes de los cuales se realizará la copia de seguridad**, una de cada tipo posible. Por ejemplo, para realizar una copia de seguridad del primer disco duro de cada equipo Linux con una política centralizada, podría escribir las siguientes líneas en el campo Volumen:

/dev/hda1

/dev/sda1

/dev/mda1

### Nombres para volúmenes lógicos

Para hacer copias de seguridad de volúmenes lógicos, conocidos como volúmenes LVM, especifique sus nombres completos en las reglas de selección. El nombre completo de un volumen lógico incluye el grupo de volumen al cual pertenece el volumen.

Por ejemplo, para realizar la copia de seguridad de dos volúmenes lógicos, **lv_root** y **lv_bin**, los cuales pertenecen al mismo grupo de volumen **vg_mymachine**, especifique las siguientes reglas de selección:

```
/dev/vg_mymachine/lv_root
/dev/vg_mymachine/lv_bin
```

Para ver la lista de volúmenes lógicos en un equipo, ejecute la utilidad **lvdisplay** . En nuestro ejemplo, la salida será parecida a como sigue a continuación:

```
--- Logical volume ---
LV Name          /dev/vg_mymachine/lv_root
VG Name          vg_mymachine
…

--- Logical volume ---
LV Name          /dev/vg_mymachine/lv_bin
VG Name          vg_mymachine
…
```

***Consejo:*** *Para poder crear de forma automática la información de estructura de volumen durante la recuperación, asegúrese de que el volumen con el directorio* ***/etc/Acronis*** *de cada equipo esté seleccionado para la copia de seguridad. Para obtener más información, vea "Guardar la información de estructura del volumen".*

## Reglas de selección para los archivos de los cuales realizará la copia de seguridad

Defina las reglas de selección de archivos, de acuerdo con las cuales se incluirán archivos y carpetas en las copias de seguridad en el equipo donde se aplicará la política.

### *Para definir las reglas de selección de archivos*

En la primera línea, seleccione la regla de la lista o escríbala manualmente. Para añadir otra regla, haga clic en la siguiente línea vacía y seleccione la regla de la lista, o escríbala manualmente.

El programa recuerda las reglas que escribió manualmente y, la próxima vez que abra la ventana, estas reglas estarán disponibles en la lista junto con las predeterminadas.

### Windows

#### Ruta completa

Vaya a las carpetas y los archivos que desea incluir en la copia de seguridad. Si especificó una ruta de un archivo o carpeta explícitamente, la política realizará una copia de seguridad de este elemento en todos los equipos donde se encuentre esta misma ruta.

| Para incluir | En la columna Archivos y carpetas, escriba o seleccione: |
|---|---|
| Archivo Texto.doc en la carpeta D:\Trabajo | **D:\Trabajo\Texto.doc** |
| Carpeta C:\Windows | **C:\Windows** |

#### Variables de entorno

Algunas variables de entorno apuntan a las carpetas de Windows. El uso de estas variables, en lugar de la carpeta completa y las rutas de los archivos, garantiza que se incluyan las carpetas de Windows adecuadas en las copias de seguridad, independientemente de dónde esté ubicado Windows en un equipo en particular.

| Para incluir | En la columna Archivos y carpetas, escriba o seleccione | Comentarios |
|---|---|---|
| Carpeta Archivos de programa | **%PROGRAMFILES%** | Señala la carpeta Archivos de programa (por ejemplo, C:\Archivos de programa) |
| Carpeta Windows | **%WINDIR%** | Señala la carpeta donde se encuentra Windows (por ejemplo, C:\Windows) |
| ▪ Carpetas comunes a todos los perfiles de usuario (para Windows XP)<br>▪ Todos los perfiles de usuario para Windows Vista | **%ALLUSERSPROFILE%** | ▪ *Windows XP*: Señala la carpeta donde se encuentran los datos comunes a todos los perfiles de usuario (por ejemplo, C:\Documents and Settings\All Users)<br>▪ *Windows Vista*: Señala la carpeta donde se encuentran todos los perfiles de usuario (por ejemplo, C:\ProgramData) |

Puede utilizar otras variables de entorno o una combinación de variables de entorno y texto. Por ejemplo, para hacer referencia a la carpeta de Acronis en la carpeta Archivos de programa del equipo, escriba: **%PROGRAMFILES%\Acronis**

**Plantillas**

Las plantillas son similares a las variables de entorno, pero ya están personalizadas de antemano.

| Para incluir | En la columna Archivos y carpetas, escriba o seleccione: | Comentarios |
|---|---|---|
| Todos los archivos de todos los volúmenes de un equipo | **[All Files]** | Señala todos los archivos de todos los volúmenes del equipo. |
| Todos los perfiles de usuario de un equipo | **[All Profiles Folder]** | Señala la carpeta donde se encuentran todos los perfiles de usuario (por ejemplo, C:\Documents and Settings\ en Windows XP y C:\ProgramData en Windows Vista). |

**Linux**

| Para incluir | En la columna Archivos y carpetas, escriba o seleccione: |
|---|---|
| El archivo de texto, archivo.txt, en el volumen /dev/hda3 montado en /home/usr/docs | **/dev/hda3/archivo.txt**<br>o<br>**/home/usr/docs/archivo.txt** |
| Directorio principal para los usuarios comunes | **/home** |
| El directorio principal del usuario raíz | **/root** |
| Directorio de todos los programas relacionados con el usuario | **/usr** |
| Directorio de los archivos de configuración del sistema | **/etc** |

## 7.3.3 Credenciales de acceso al origen

Especifique las credenciales necesarias para acceder a los datos de los cuales realizará la copia de seguridad.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Utilice las credenciales de la política.**

     El programa accederá a los datos de origen mediante las credenciales de la política de copia de seguridad especificada en la sección General.
   - **Utilice las siguientes credenciales.**

     El programa accederá a los datos de origen mediante las credenciales que especifique. Utilice esta opción si las credenciales de la política no tienen permiso de acceso a los datos.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

### 7.3.4 Exclusiones

[Opcional] Configure exclusiones para tipos de archivo específicos para los cuales no desea realizar copias de seguridad. Por ejemplo, quizá desee que los archivos y carpetas ocultos y del sistema, así como los archivos con extensiones específicas, no se almacenen en el archivo comprimido.

***Para especificar los archivos y carpetas que desea excluir:***

Configure alguno de los siguientes parámetros:

- **Excluir todos los archivos y carpetas ocultos**

  Esta opción está vigente sólo para sistemas de archivos compatibles con Windows. Seleccione esta casilla de verificación para omitir archivos y carpetas con el atributo **Oculto**. Si una carpeta está **Oculta**, se excluirán todos sus contenidos, incluso los archivos que no se encuentran **Ocultos**.
- **Excluir todos los archivos y carpetas del sistema**

  Esta opción está vigente sólo para sistemas de archivos compatibles con Windows. Seleccione esta casilla de verificación para omitir archivos y carpetas con el atributo **Sistema**. Si una carpeta tiene el atributo **Sistema**, se excluirán todos sus contenidos, incluso los archivos que no tengan el atributo **Sistema**.

*Puede ver los atributos del archivo o de la carpeta en las propiedades del archivo/carpeta o mediante el comando **atrib**. Para obtener más información, consulte el Centro de Servicio Técnico y Ayuda de Windows.*

- **Excluir los archivos que coincidan con los siguientes criterios**

  Seleccione esta casilla de verificación para omitir los archivos y las carpetas cuyos nombres en la lista coincidan con alguno de los criterios, llamados máscaras del archivo; utilice los botones **Agregar**, **Editar**, **Eliminar** y **Eliminar todos** para crear la lista de máscaras del archivo.

  Puede utilizar uno o más caracteres comodín * y ? en una máscara de archivo:

  El asterisco (*) sustituye de cero a más caracteres del nombre del archivo; por ejemplo, la máscara de archivo Doc*.txt genera archivos Doc.txt y Document.txt

  El signo de interrogación (?) substituye a un único carácter; por ejemplo, la máscara de archivo Doc?.txt genera archivos Doc1.txt y Docs.txt, pero, por el contrario, no general archivos Doc.txt o Doc11.txt

Para excluir una carpeta especificada por una ruta que contiene la letra de unidad, agregue una barra invertida (\) al nombre de carpeta en el criterio; por ejemplo: C:\Finance\

**Ejemplos de exclusión**

| Criterio | Ejemplo | Descripción |
|---|---|---|
| **Windows y Linux** | | |
| Por nombre | F.log<br>F | Excluye todos los archivos denominados "F.log"<br>Excluye todas las carpetas denominadas "F" |
| Por máscara (*) | *.log<br>F* | Excluye todos los archivos con la extensión .log<br>Excluye todos los archivos y carpetas cuyos nombres comiencen con "F" (como carpetas F, F1 y archivos F.log, F1.log) |

| | | |
|---|---|---|
| Por máscara (?) | F???.log | Excluye todos los archivos .log cuyos nombres contengan cuatro símbolos y comiencen con "F" |
| **Windows** | | |
| Por ruta de archivo | C:\Finance\F.log | Excluye el archivo denominado "F.log" ubicado en la carpeta C:\Finance |
| Por ruta de carpeta | C:\Finance\F\ | Excluye la carpeta C:\Finance\F (asegúrese de especificar la ruta completa, comenzando por la letra de unidad) |
| **Linux** | | |
| Por ruta de archivo | /home/user/Finance/F.log | Excluye el archivo denominado "F.log", ubicado en la carpeta /home/user/Finance |
| Por ruta de carpeta | /home/user/Finance/ | Excluye la carpeta /home/user/Finance |

## 7.3.5 Archivo comprimido

Especifique si desea almacenar los archivos comprimidos y definir los nombres de los archivos nuevos de copia de seguridad.

### 1. Selección del destino de los archivos comprimidos

Elija dónde almacenar los archivos comprimidos del equipo:

- Almacenar todos los archivos comprimidos de los equipos en una única ubicación
  - Para hacer una copia de seguridad de datos en Acronis Online Backup Storage, haga clic en **Iniciar sesión** y especifique las credenciales de acceso al almacenamiento en línea. Después, expanda el grupo **Almacenamiento de copia de seguridad en línea** y seleccione la cuenta.

    Antes de hacer una copia de seguridad del almacenamiento en línea, necesitará comprar una suscripción para el servicio de almacenamiento en línea y activar la suscripción en el(los) equipo(s) de los que desea realizar una copia de seguridad. La opción de copia de seguridad en línea no está disponible en Linux.

  *Acronis Backup & Recovery 10 Online es posible que no esté disponible en su región. Para obtener más información, haga clic aquí: http://www.acronis.es/my/backup-recovery-online/.*

  - Para almacenar archivos comprimidos en una bóveda centralizada, expanda el grupo Centralizada y haga clic en la bóveda.
  - Para almacenar archivos comprimidos en una red compartida, expanda el grupo Carpetas de red, luego seleccione el equipo en red necesario y haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.
  - Para almacenar archivos comprimidos en un servidor FTP o SFTP, expanda el grupo correspondiente y vaya al servidor apropiado, luego seleccione la carpeta que usará para almacenar los archivos comprimidos.

  *Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

- Almacenar cada archivo comprimido de cada equipo en la carpeta especificada en el equipo

  Escriba la ruta completa para acceder a la carpeta en el campo Ruta. Esta ruta se creará en todos los equipos donde se haya aplicado la política.

- Almacene el archivo comprimido de cada equipo en Acronis Secure Zone

  Acronis Secure Zone debe crearse en cada equipo en el que se aplicará la política. Para obtener más información sobre cómo crear Acronis Secure Zone, consulte la sección Creación de Acronis Secure Zone (pág. 271).

**2. Nombres de los archivos comprimidos**

Los datos de cada equipo se incluirán en una copia de seguridad en un archivo comprimido diferente. Especifique los nombres de los archivos comprimidos.

El programa genera un nombre común para los nuevos archivos comprimidos y lo muestra en el campo Nombre. El nombre es similar a: [NombrePolítica]_[NombreEquipo]_ArchivoComprimido1. Si no está satisfecho con los nombres generados automáticamente, cree otro nombre.

Si seleccionó Almacenar todos los archivos comprimidos de los equipos en una única ubicación, deberá utilizar variables a fin de proporcionar los nombres de archivos comprimidos únicos dentro de la ubicación.

1. Haga clic en Añadir variables, luego seleccione
   - [Nombre del equipo]: sustitución del nombre del equipo
   - [Nombre de la política]: sustitución del nombre de la política de copias de seguridad

   Como resultado, en el campo Nombre aparecerán las siguientes reglas: [Nombre del equipo]_[Nombre de la política]_ArchivoComprimido1

   Por lo tanto, si la política de copias de seguridad nombrada, digamos, COPIA SEG_EQUIPO, se aplicará a los tres equipos (por ejemplo, DEPFIN1, DEPFIN2, DEPFIN3), los siguientes tres archivos comprimidos se crearán en la ubicación:

   DEPFIN1_COPIA SEG_EQUIPO_ArchivoComprimido1

   DEPFIN2_COPIA SEG_EQUIPO_ArchivoComprimido1

   DEPFIN3_COPIA SEG_EQUIPO_ArchivoComprimido1
2. Haga clic en Aceptar.

El nombre se parece a ArchivoComprimidoN, en el que N es un número de secuencia. Si el programa descubre que el archivo ArchivoComprimido1 ya está almacenado en la ubicación, sugerirá el nombre ArchivoComprimido2.

### 7.3.6 Credenciales de acceso a la ubicación

Especifique las credenciales necesarias para acceder a la ubicación donde se almacenará el archivo de copia de seguridad. El nombre de usuario de estas credenciales se considerará como propietario del archivo comprimido.

***Para especificar las credenciales***

1. Seleccione una de las siguientes opciones:
   - **Utilice las credenciales de la política.**

     El programa accederá a la ubicación mediante las credenciales de la política de copia de seguridad especificada en la sección General.
   - **Utilice las siguientes credenciales.**

     El programa accederá a la ubicación mediante las credenciales que especifique. Utilice esta opción si las credenciales de la política no cuentan con permiso de acceso a la ubicación. Es posible que tenga que proporcionar credenciales especiales para una red compartida o un nodo de almacenamiento.

Especifique:

- **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
- **Contraseña**. La contraseña de la cuenta.

2. Haga clic en **Aceptar**.

***Advertencia:*** *Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

## 7.3.7 Selección del esquema de copia de seguridad

Elija uno de los esquemas de copia de seguridad disponibles:

- **Copia de seguridad ahora** – para crear una tarea de copia de seguridad para un inicio manual y ejecutar la tarea inmediatamente después de crearla.
- **Copia de seguridad más tarde** – para crear una tarea de copia de seguridad para un inicio manual O programar que la tarea se ejecute más tarde una vez.
- **Simple** – para programar cuándo y con qué frecuencia realizar copias de seguridad de los datos y especificar reglas de retención.
- **Abuelo-Padre-Hijo** – para utilizar el esquema de copia de seguridad Abuelo-Padre-Hijo. Este esquema sólo permite realizar copias de seguridad de los datos una vez al día.. Puede configurar los días de la semana en los que se llevará a cabo la copia de seguridad y seleccionar de entre esos días, la fecha para la copia de seguridad semanal o mensual. Después, debe ajustar los periodos de retención para las copias de seguridad diarias (llamadas "hijos"), semanales (llamadas "padres") y mensuales (llamadas "abuelos"). Las copias de seguridad caducadas se borrarán automáticamente.
- **Torre de Hanoi** – para utilizar el esquema de copia de seguridad Torre de Hanoi, en el que se programa cuándo y con qué frecuencia realizar copias de seguridad (sesiones) y se selecciona el número de niveles de copia de seguridad (hasta 16). Con este esquema, se puede realizar más de una copia de seguridad de los datos al día. Al configurar el calendario de copia de seguridad y seleccionar los niveles de copia de seguridad, se obtiene automáticamente el periodo de recuperación, es decir, el número garantizado de sesiones que se pueden a las que se puede volver en cualquier momento. El mecanismo de limpieza automático mantiene el periodo de recuperación necesario, borrando las copias de seguridad caducadas y conservando las copias de seguridad más recientes de cada nivel.
- **Personalizada** – para crear una copia de seguridad personalizada, en la que se puede configurar libremente la estrategia que mejor convenga a las necesidades de su empresa: especificar diferentes programaciones para diferentes tipos de copias de seguridad, añadir condiciones y especificar las reglas de retención.
- **Inserción inicial** - para guardar localmente una copia de seguridad completa cuyo destino final es Acronis Online Backup Storage.

### Esquema Realizar copia de seguridad ahora

Con el esquema **Copia de seguridad ahora**, la copia de seguridad se llevará a cabo inmediatamente después de que haga clic en el botón **Aceptar** en la parte inferior de la página.

En el campo **Tipo de copia de seguridad**, seleccione si desea crear una copia de seguridad completa, incremental o diferencial (pág. 31).

## Esquema Realizar copia de seguridad más tarde

Con el esquema Copia de seguridad más tarde, la copia de seguridad se llevará a cabo una sola vez, en la fecha y hora que especifique.

Especifique los ajustes adecuados de la siguiente manera

| | |
|---|---|
| **Tipo de copia de seguridad** | Seleccione el tipo de copia de seguridad: completo, incremental o diferencial. Si no existe una copia de seguridad completa en el archivo comprimido, se creará una independientemente de su elección. |
| **Fecha y hora** | Especifique cuándo desea iniciar la copia de seguridad. |
| **La tarea se iniciará manualmente** | Seleccione esta casilla de verificación si no necesita colocar la tarea de copia de seguridad en una programación y desea iniciarla manualmente más tarde. |

## Esquema simple

Con el esquema simple de copia de seguridad, simplemente debe programar cuándo y con qué frecuencia realizar copias de seguridad de los datos y configurar la regla de retención. La primera vez se creará una copia de seguridad completa. Las siguientes copias de seguridad serán incrementales.

Para configurar el esquema simple de copia de seguridad, especifique los ajustes apropiados de la siguiente manera.

| | |
|---|---|
| **Crear copia de seguridad** | Configure la programación de la copia de seguridad: cuándo y con qué frecuencia realizar copias de seguridad de los datos.<br>Para obtener más información sobre cómo configurar el calendario, consulte la sección Programación (pág. 173). |
| **Regla de retención** | Con el esquema simple, solo se dispone de una regla de retención (pág. 42). Configure el periodo de retención para las copias de seguridad. |

## Esquema Abuelo-padre-hijo

### De un vistazo

- Copias de seguridad incrementales diarias, diferenciales semanales y completas mensuales
- Día personalizado para las copias de seguridad semanales y mensuales
- Periodos de retención personalizados para las copias de seguridad de cada tipo

### Descripción

Supongamos que queremos configurar un plan de copias de seguridad que produzca una serie de copias de seguridad regulares diarias (D), semanales (S) y mensuales (M). Este es el modo más normal para hacerlo: la siguiente tabla muestra un ejemplo de un periodo de dos meses para dicho plan.

| | Lu | Ma | Mi | Ju | Vi | Sa | Do |
|---|---|---|---|---|---|---|---|
| 1 Ene—7 Ene | D | D | D | D | S | - | - |
| 8 Ene—14 Ene | D | D | D | D | S | - | - |
| 15 Ene—21 Ene | D | D | D | D | S | - | - |
| 22 Ene—28 Ene | D | D | D | D | M | - | - |
| 29 Ene—4 Feb | D | D | D | D | S | - | - |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 5 Feb—11 Feb | D | D | D | D | S | - | - |
| 12 Feb—18 Feb | D | D | D | D | S | - | - |
| 19 Feb—25 Feb | D | D | D | D | M | - | - |
| 26 Feb—4 Mar | D | D | D | D | S | - | - |

Las copias de seguridad diarias se ejecutan todos los días laborables excepto los viernes, que se reservan para las copias de seguridad semanales y mensuales. Las copias de seguridad mensuales se llevan a cabo el cuarto viernes de cada mes y las semanales, los demás viernes del mes.

- Las copias de seguridad mensuales ("Abuelo") son completas;
- Las copias de seguridad semanales ("Padre") son diferenciales;
- Las copias de seguridad diarias ("Hijo") son incrementales.

### Parámetros

Puede configurar los siguientes parámetros de un esquema Abuelo-Padre-Hijo (GFS).

| | |
|---|---|
| **Comienzo de la copia de seguridad en:** | Especifica cuándo se inicia una copia de seguridad. El valor predeterminado son las 12:00. |
| **Copia de seguridad en:** | Especifica los días en los que se lleva a cabo la copia de seguridad. El valor predeterminado es el viernes. |
| **Semanalmente/mensualmente:** | Especifica cuál de los días elegidos en el campo **Realizar copias de seguridad el** desea reservar para las copias de seguridad semanales y mensuales. El cuarto día especificado del mes se llevará a cabo una copia de seguridad mensual. El valor predeterminado es el viernes. |
| **Mantener copias de seguridad:** | Especifica durante cuánto tiempo desea que se almacenen las copias de seguridad en el archivo comprimido. Se puede configurar en horas, días, semanas, meses o años. Para copias de seguridad mensuales, puede seleccionar también **Mantener indefinidamente** si desea que se almacenen para siempre.<br><br>Los valores predeterminados para cada tipo de copia de seguridad son los siguientes.<br><br>Diariamente: 7 días (mínimo recomendado)<br><br>Semanalmente: 4 semanas<br><br>Mensualmente: indefinidamente<br><br>El periodo de retención para las copias de seguridad semanales debe ser mayor al establecido para las diarias. Del mismo modo, el periodo de retención para las copias de seguridad mensuales debe ser mayor al de las copias semanales.<br><br>Le recomendamos configurar un periodo de retención de al menos una semana para las copias de seguridad diarias. |
| **Configuraciones avanzadas:** | Para especificar Configuraciones de programación avanzadas |

| | |
|---|---|
| | (pág. 181), haga clic en **Cambiar** en el área **Configuraciones avanzadas**. |

*Nunca se elimina una copia de seguridad hasta que todas las copias de seguridad que dependen directamente de ella se puedan eliminar. Por esta razón, puede que observe que una copia de seguridad semanal o mensual permanece en el archivo comprimido incluso unos días después de la fecha de caducidad esperada.*

*Si la programación comienza con una copia de seguridad diaria o semanal, en su lugar se crea una copia de seguridad completa.*

### Ejemplos

### Cada día de la semana pasada, cada semana del mes pasado

Permítanos sugerir un esquema de copia de seguridad GFS que podría encontrar útil.

- Realizar copias de seguridad cada día, fines de semana incluidos
- Tener la posibilidad de recuperar los archivos de cualquier fecha dentro de los últimos siete días
- Tener acceso a las copias de seguridad semanales del mes anterior.
- Mantener copias de seguridad mensuales indefinidamente.

Los parámetros del esquema de copia de seguridad se pueden configurar de la siguiente manera.

- Comienzo de la copia de seguridad en: **23:00**
- Copia de seguridad en: **Todos los días**
- Semanalmente/mensualmente: **Sábado** (por ejemplo)
- Mantener copias de seguridad:
  - Diariamente: **1 semana**
  - Semanalmente: **1 mes**
  - Mensualmente: **indefinidamente**

Por lo tanto, se creará un archivo comprimido de copias de seguridad diarias, semanales y mensuales. Las copias de seguridad diarias estarán disponibles durante siete días a partir de la fecha de creación. Por ejemplo, una copia de seguridad diaria con fecha de domingo, 1 de enero, permanecerá disponible hasta el próximo domingo, 8 de enero; la primera copia de seguridad semanal, con fecha de sábado, 7 de enero, se almacenará en el sistema hasta el 7 de febrero. Las copias de seguridad mensuales no se eliminarán nunca.

### Almacenamiento limitado

Si no desea fijar una gran cantidad de espacio para almacenar un archivo comprimido muy grande, debería configurar un esquema GFS para limitar la vida media de sus copias de seguridad, a la vez que garantiza que su información pueda recuperarse en caso de una pérdida de datos accidental.

Suponga que necesita:

- Realizar copias de seguridad al final de cada día laborable
- Tener la posibilidad de recuperar un archivo modificado o eliminado de manera accidental si se ha detectado relativamente pronto
- Tener acceso a una copia de seguridad semanal durante 10 días después de su creación.
- Conservar copias de seguridad mensuales durante 6 meses.

Los parámetros del esquema de copia de seguridad se pueden configurar de la siguiente manera.

- Comienzo de la copia de seguridad a las: **18:00**

- Copia de seguridad el: **Días hábiles**
- Semanalmente/mensualmente: **Viernes**
- Mantener copias de seguridad:
  - Diaria: **1 semana**
  - Semanal: **10 días**
  - Mensual: **6 meses**

Con este esquema, dispondrá de una semana para recuperar una versión anterior de un archivo dañado a partir de una copia de seguridad diaria, así como de 10 días de acceso a las copias de seguridad semanales. Las copias de seguridad completas mensuales estarán disponible durante 6 meses a partir de la fecha de creación.

### Programación laboral

Supongamos que es consultor financiero y trabaja media jornada en una empresa los martes y jueves. Durante estos días, por lo general, realiza cambios en documentos financieros y declaraciones, y actualiza hojas de cálculo, etc. en su portátil. Para realizar copias de seguridad de estos datos, es conveniente que:

- Rastree los cambios en las declaraciones financieras, hojas de cálculo, etc. realizados los martes y jueves (copia de seguridad incremental diaria).
- Tenga un resumen semanal de los cambios en los archivos desde el mes pasado (copia de seguridad diferencial semanal).
- Tenga una copia de seguridad completa mensual de todos los archivos.

Además, supongamos que desea mantener el acceso a todas las copias de seguridad, incluidas las diarias, durante al menos seis meses.

El siguiente esquema GFS cumple estos fines:

- Iniciar copia de seguridad a las: **23:30.**
- Realizar copias de seguridad el: **Martes, Jueves, Viernes**
- Semanalmente/mensualmente: **Viernes**
- Mantener copias de seguridad:
  - Diariamente: **6 meses**
  - Semanalmente: **6 meses**
  - Mensualmente: **5 años**

Aquí, las copias de seguridad incrementales diarias se crearán los martes y jueves, con copias de seguridad semanales y mensuales que se realizarán los viernes. Tenga en cuenta que, para elegir **Viernes** en el campo **Semanalmente/mensualmente**, deberá seleccionarlo primero en el campo **Realizar copias de seguridad el**.

Ese archivo comprimido le permitirá comparar los documentos financieros a partir del primer y último día hábil, y tener un historial de cinco años de todos los documentos, etc.

### Sin copias de seguridad diarias

Considere un esquema GFS diferente:

- Iniciar copia de seguridad a las: **12:00.**
- Realizar copias de seguridad el: **Viernes**
- Semanalmente/mensualmente: **Viernes**

- Mantener copias de seguridad:
  - Diariamente: **1 semana**
  - Semanalmente: **1 mes**
  - Mensualmente: **indefinidamente**

La copia de seguridad, por lo tanto, se realiza solo los viernes. Esto hace que el viernes sea la única opción para realizar copias de seguridad semanales y mensuales, sin que haya otra fecha para las copias de seguridad diarias. El archivo comprimido "Abuelo-padre" resultante, por lo tanto, consistirá solo de copias de seguridad diferenciales semanales y completas mensuales.

Si bien se puede utilizar el esquema GFS para crear dicho archivo comprimido, el esquema personalizado es más flexible para esta situación.

## Esquema Torres de Hanói

### De un vistazo

- Hasta 16 niveles de copias de seguridad completas, diferenciales e incrementales
- La frecuencia de las copias de seguridad del nivel siguiente es exactamente la mitad de la de las copias de seguridad de los niveles anteriores.
- Solo se almacena una copia de seguridad de cada nivel al mismo tiempo
- La cantidad de copias de seguridad recientes es mayor que la de las antiguas.

### Parámetros

Puede configurar los siguientes parámetros de un esquema Torres de Hanói.

| | |
|---|---|
| **Programación** | Configurar una programación diaria (pág. 174), semanal (pág. 176) o mensual (pág. 178). Se pueden crear programaciones simples al configurar los parámetros de la programación (ejemplo de una programación simple diaria: se realizará una tarea de copia de seguridad cada día 1 a las 10:00), así como programaciones más complejas (ejemplo de una programación compleja diaria: se realizará una tarea cada 3 días, comenzando a partir del 15 de enero. En los días especificados, la tarea se repetirá cada 2 horas desde las 10 hasta las 22 horas). De este modo, las programaciones complejas especifican las sesiones en las que el esquema debería ejecutarse. En los comentarios siguientes, se puede reemplazar por "sesiones programadas". |
| **Número de niveles** | Seleccione los niveles de copia de seguridad entre 2 a 16. Para obtener más información, consulte el siguiente ejemplo. |
| **Periodo de recuperación** | El número garantizado de sesiones a las que se puede volver en el archivo comprimido en cualquier momento. Se calcula automáticamente, dependiendo de los parámetros de programación y de los niveles que seleccione. Para obtener más información, consulte el siguiente ejemplo. |

### Ejemplo

Los parámetros de **Programación** se configuran de la siguiente manera

- Repetir: Cada día
- Frecuencia: Por primera vez a las 18:00

**Número de niveles**: 4

Para los 14 días siguientes (o 14 sesiones), este esquema de programación se verá de la siguiente manera: Los números sombreados indican los niveles de copia de seguridad.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |

| 4 | 1 | 2 | 1 | 3 | 1 | 2 | 1 | 4 | 1 | 2 | 1 | 3 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Las copias de seguridad de niveles diferentes son de diferentes tipos:

- Las copias de seguridad de *último nivel* (en este caso, nivel 4) son completas;
- Las copias de seguridad de *niveles intermedios* (2, 3) son diferenciales;
- Las copias de seguridad de *primer nivel* (1) son incrementales.

Un mecanismo de limpieza garantiza que solo se mantienen las copias de seguridad más recientes de cada nivel. Este es el aspecto del archivo comprimido en el día 8, un día antes de crear una nueva copia de seguridad completa.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 1 | 3 | 1 | 2 | 1 |

El esquema permite un almacenamiento eficiente de los datos: Se acumulan más copias de seguridad cuanto más cerca nos encontramos de la fecha actual. Con 4 copias de seguridad, se pueden recuperar datos de hoy, de ayer, de media semana o de una semana atrás.

### Periodo de recuperación

El número de días a los que se puede volver en el archivo comprimido es diferente en función del día. El número mínimo de días garantizados se llama periodo de recuperación.

La siguiente tabla muestra los periodos de copia de seguridad completos y los periodos de recuperación para esquemas de diferentes niveles.

| **Número de niveles** | **Copia de seguridad completa cada** | **En días diferentes, puede volver atrás** | **Periodo de recuperación** |
|---|---|---|---|
| 2 | 2 días | De 1 a 2 días | 1 día |
| 3 | 4 días | De 2 a 5 días | 2 días |
| 4 | 8 días | De 4 a 11 días | 4 días |
| 5 | 16 días | De 8 a 23 días | 8 días |
| 6 | 32 días | De 16 a 47 días | 16 días |

Al aumentar un nivel, la duración de los periodos de copia de seguridad completa y de recuperación se multiplican por dos.

Para ver por qué varía el número de los días de recuperación, consulte el ejemplo siguiente.

A continuación se encuentran las copias de seguridad que tenemos en el día 12 (los números en gris indican las copias de seguridad eliminadas).

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 1 | 3 | 1 | 2 | 1 | 4 | 1 | 2 | 1 |

Todavía no se ha creado una copia de seguridad diferencial de nivel 3, por lo que la copia de seguridad del día 5 aún se encuentra almacenada. Esta copia de seguridad sigue estando disponible ya que depende de la copia de seguridad completa del día 1. Esto nos permite retroceder hasta 11 días, lo cual constituye el mejor de los casos posibles.

El día siguiente, sin embargo, se crea una nueva copia de seguridad diferencial de nivel 3 y se elimina la copia de seguridad completa antigua.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 1 | 3 | 1 | 2 | 1 | 4 | 1 | 2 | 1 | 3 |

Esto nos proporciona solo un intervalo de recuperación de 4 días, lo que representa la peor situación posible.

En el día 14, el intervalo es de 5 días. En los días siguientes, este intervalo va aumentando hasta volver a reducirse, sucesivamente.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 1 | 3 | 1 | 2 | 1 | 4 | 1 | 2 | 1 | 3 | 1 |

El periodo de recuperación muestra el número de días que están garantizados incluso en el peor de los casos. Para un esquema de cuatro niveles, es de 4 días.

## Esquema personalizado de copia de seguridad

### De un vistazo

- Programación personalizada y condiciones de copia de seguridad de cada tipo
- Programación personalizada y reglas de retención

### Parámetros

| Parámetro | Significado |
|---|---|
| **Copia de seguridad completa** | Especifica con qué programación y bajo qué condiciones realizar una copia de seguridad completa.<br>Por ejemplo, la copia de seguridad completa puede configurarse para que se ejecute cada domingo a la 01:00, tan pronto como todos los usuarios hayan cerrado sus sesiones. |
| **Incremental** | Especifica con qué programación y bajo qué condiciones realizar una copia de seguridad incremental.<br>Si el archivo comprimido no contiene copias de seguridad cuando se ejecute la tarea, se llevará a cabo una copia de seguridad completa en lugar de una incremental. |
| **Diferencial** | Especifica con qué programación y bajo qué condiciones realizar una copia de seguridad diferencial.<br>Si el archivo comprimido no contiene copias de seguridad cuando se ejecute la tarea, se llevará a cabo una copia de seguridad completa en lugar de una diferencial. |
| **Limpie el archivo comprimido** | Especifica cómo eliminar copias de seguridad antiguas: ya sea aplicando reglas de retención (pág. 42) regularmente o limpiando el archivo durante la realización de una copia de seguridad cuando la ubicación de destino se queda sin espacio.<br>De manera predeterminada, las reglas de retención no se especifican, lo cual significa que las copias de seguridad más antiguas no se eliminarán de forma automática.<br>**Utilización de reglas de retención**<br>Especifique las reglas de retención y cuándo aplicarlas.<br>Se recomienda esta configuración para destinos de copias de seguridad como carpetas compartidas o bóvedas centralizadas.<br>**Cuando no hay espacio suficiente mientras se realiza la copia de seguridad**<br>El archivo comprimido se limpiará únicamente durante la realización de la copia de seguridad y sólo si no hay espacio suficiente para crear una copia de seguridad nueva. |

| | |
|---|---|
| | En este caso, el programa actuará de la siguiente manera:<br>▪ Eliminará la copia de seguridad más antigua y todas las copias de seguridad incrementales/diferenciales dependientes.<br>▪ Si queda sólo una copia de seguridad completa y otra está en progreso, eliminará la última copia de seguridad completa y todas las copias de seguridad incrementales/diferenciales dependientes<br>▪ Si queda sólo una copia de seguridad completa y hay una copia de seguridad incremental o diferencial en progreso, se producirá un error que le indicará que no hay espacio disponible<br>Se recomienda esta configuración para realizar copias de seguridad en una unidad USB o Acronis Secure Zone. Esta configuración no se aplica a bóvedas gestionadas.<br>Esta configuración permite la eliminación de la última copia de seguridad en el archivo comprimido, en caso de que su dispositivo de almacenamiento no pueda incluir más de una copia de seguridad. Sin embargo, si por alguna razón el programa no puede crear la copia de seguridad nueva, podría quedarse sin copias de seguridad. |
| **Aplicar las reglas**<br>(solo si las reglas de retención están configuradas) | Especifica cuándo aplicar las reglas de retención (pág. 42).<br>Por ejemplo, el procedimiento de limpieza puede configurarse para que se ejecute después de cada copia de seguridad y según la programación.<br>Esta opción estará disponible únicamente si ha configurado al menos una regla de retención en **Reglas de retención**. |
| **Programación de limpieza**<br>(solo si la opción **Según programación** está seleccionada) | Especifica una programación para la limpieza del archivo comprimido.<br>Por ejemplo, la limpieza puede programarse para que comience el último día de cada mes.<br>Esta opción estará disponible únicamente si ha seleccionado **Según programación** en **Aplicar las reglas**. |

## Ejemplos

### Copia de seguridad completa semanal

El siguiente esquema genera una copia de seguridad completa que se realiza todos los viernes por la noche.

**Copia de seguridad completa**: **Programación: Semanalmente**, todos los **viernes**, a las **22:00.**

Aquí, todos los parámetros de **Copia de seguridad completa** quedan vacíos, excepto **Programar**. Todas las copias de seguridad se conservan indefinidamente en el archivo comprimido (no se realizan limpiezas del archivo).

### Copia de seguridad incremental y completa más limpieza

Con el siguiente esquema, el archivo comprimido constará de copias de seguridad completas semanales e incrementales diarias. Más allá de eso, necesitamos que una copia de seguridad completa tenga lugar únicamente una vez que todos los usuarios hayan cerrado sesión.

**Copia de seguridad completa: Programación: Semanal**, cada **viernes** a las **22:00**

**Copia de seguridad completa: Condiciones: El usuario ha cerrado sesión**

**Incremental: Programación: Semanal, cada día laborable** a las **21:00**

Permita también que todas las copias de seguridad que tengan más de un año se eliminen del archivo comprimido, así como la realización de una limpieza que finalice con la creación de una nueva copia de seguridad.

**Reglas de retención:** Eliminar las copias de seguridad que tengas más de **12 meses**

**Aplicar las reglas: Después de realizar la copia de seguridad**

De manera predeterminada, no se eliminará una copia de seguridad completa a menos que se eliminen todas las copias de seguridad incrementales que dependen de ella. Para obtener más información, consulte Reglas de retención (pág. 42).

### Copias de seguridad mensuales completas, semanales diferenciales y diarias incrementales más limpieza

Este ejemplo demuestra el uso de todas las opciones disponibles en el esquema personalizado.

Supongamos que necesitamos un esquema para generar copias de seguridad completas mensuales, diferenciales semanales e incrementales diarias. La programación de copia de seguridad podría ser la siguiente:

Copia de seguridad completa: **Programación: Mensualmente**, todos los **últimos domingos** del mes, a las **21:00.**

**Incremental: Programación: Diariamente**, todos los **días hábiles**, a las **19:00.**

**Diferencial: Programación: Semanalmente**, todos los **sábados**, a las **20:00.**

Además, queremos añadir condiciones que deben cumplirse para que se inicie una tarea de copia de seguridad. Estas opciones se establecen en los campos **Condiciones** de cada tipo de copia de seguridad.

**Copia de seguridad completa**: **Condiciones**: **Ubicación disponible**

**Incremental**: **Condiciones**: **El usuario cerró la sesión**

**Diferencial**: **Condiciones**: **El usuario está inactivo**

Por ese motivo, la copia de seguridad completa. originalmente programada para las 21:00, podría comenzar más tarde: en cuanto la ubicación de la copia de seguridad esté disponible. Del mismo modo, las tareas de copia de seguridad para copias incrementales y diferenciales no se iniciarán hasta que todos los usuarios hayan cerrado sesión y estén inactivos, respectivamente.

Por último, creamos reglas de retención para el archivo comprimido: que se conserven solo las copias de seguridad que tengan menos de seis meses y que se realice una limpieza después de cada tarea de copia de seguridad y también el último día de cada mes.

**Reglas de retención**: Eliminar las copias de seguridad con más de **6 meses**

**Aplicar las reglas**: **Después de realizar la copia de seguridad**, **Según la programación**

**Programación de limpieza**: **Mensualmente**, el **Último día** de **Todos los meses**, a las **22:00.**

De manera predeterminada, una copia de seguridad no se eliminará siempre que tenga otras copias dependientes que deban conservarse. Por ejemplo: si una copia de seguridad completa puede eliminarse, pero hay otras copias incrementales o diferenciales que dependen de ella, la eliminación se pospone hasta que también se puedan eliminar todas las copias de seguridad dependientes.

Para obtener más información, consulte Reglas de retención (pág. 42).

### Tareas resultantes

Todos los esquemas personalizados originan siempre tres tareas de la copia de seguridad y, en caso de que se especifiquen las reglas de retención, una tarea de limpieza. Cada tarea se detalla en la lista de tareas como **Programada** (si se ha configurado la programación) o como **Manual** (si no se ha configurado la programación).

Puede ejecutar cualquier tarea de copia de seguridad o limpieza en cualquier momento, sin importar si se encuentra programada.

En el primero de los ejemplos anteriores, configuramos una programación únicamente para copias de seguridad completas. Sin embargo, el esquema seguirá originando tres tareas de copia de seguridad, permitiéndole así realizar manualmente una copia de seguridad de cualquier tipo:

- Copia de seguridad completa, se ejecuta cada viernes a las 22:00
- Copia de seguridad incremental, se ejecuta manualmente
- Copia de seguridad diferencial, se ejecuta manualmente

Puede ejecutar cualquiera de estas tareas de copia de seguridad al seleccionarlas en la lista de tareas en la sección **Planes y tareas de la copia de seguridad** situada en el panel izquierdo.

Si también ha especificado las reglas de retención en su esquema de copia de seguridad, el esquema originará cuatro tareas: tres tareas de copia de seguridad y una tarea de limpieza.

## 7.3.8 Validación de archivos comprimidos

Configure la validación de la tarea para comprobar si los datos de la copia de seguridad pueden recuperarse. Si la copia de seguridad no finaliza la validación correctamente, la tarea de validación falla y el plan de copias de seguridad establecerá su estado en Error.

Para configurar la validación, especifique los siguientes parámetros

1. **Cuándo validar**: seleccione cuándo realizar la validación. Ya que la validación es una operación que utiliza muchos recursos, puede ser conveniente **programar** la validación en el periodo de menor actividad del equipo gestionado. Por otro lado, si la validación es uno de los elementos clave de su estrategia de protección de datos y prefiere que se le notifique inmediatamente en el caso de que los datos de la copia de seguridad no estén dañado y puedan recuperarse correctamente, considere la posibilidad de comenzar la validación inmediatamente después de la creación de la copia de seguridad.
2. **Qué validar**: seleccione validar el archivo comprimido al completo o su última copia de seguridad en el archivo comprimido. La validación de la copia de seguridad de un archivo simula la recuperación de todos los archivos de la copia de seguridad a un destino ficticio La validación de la copia de seguridad del volumen calcula la suma de comprobación para cada bloque de datos guardados en la copia de seguridad. La validación del archivo comprimido validará todas las copias de seguridad de los archivos comprimidos y podría llevar un tiempo considerable y agotar muchos recursos.
3. **Programación de la validación** (aparece únicamente si ha seleccionado según programación en el paso 1): configure la programación de la validación. Para obtener más información, consulte la sección Programación (pág. 173).

# 8 Glosario

## A

### Acronis Active Restore

La tecnología propietaria de Acronis que pone un sistema en línea inmediatamente después de que comience la recuperación del sistema. El sistema se inicia desde la copia de seguridad (pág. 404) y el equipo queda funcional y listo para proporcionar los servicios necesarios. Se recupera con la más alta prioridad a los datos requeridos para que se utilizarán para las solicitudes entrantes; todo lo demás se recupera en segundo plano. Limitaciones:

- La copia de seguridad se ubica en la unidad local (cualquier dispositivo disponible a través de BIOS, a excepción del inicio de red)
- No funciona con imágenes de Linux.

### Acronis Secure Zone

Un volumen seguro para almacenar archivos comprimidos (pág. 401) de copias de seguridad dentro de un equipo gestionado (pág. 405). Ventajas:

- Permite la recuperación de un disco en el mismo disco en donde se encuentra la copia de seguridad del disco
- Ofrece un método rentable y útil para la protección de datos por fallos del software, virus, ataques o errores del operador
- Elimina la necesidad de medios o conexión de red diferentes para realizar copias de seguridad o recuperar los datos. Es especialmente útil para los usuarios móviles
- Puede utilizarse como la ubicación primaria para copias de seguridad de destino doble.

Limitaciones: Acronis Secure Zone no se puede organizar en un disco dinámico (pág. 404) o un disco que utilice el estilo de partición GPT.

Acronis Secure Zone se considera una bóveda personal (pág. 403).

### Acronis Startup Recovery Manager (ASRM)

Una modificación del agente reiniciable (pág. 401), que reside en el disco del sistema y está configurado para iniciarse al momento del inicio al presionarse F11. Acronis Startup Recovery Manager elimina la necesidad de un dispositivo de rescate o conexión de red para iniciar la utilidad de rescate de inicio.

Acronis Startup Recovery Manager es muy útil para los usuarios móviles. En caso de fallo, el usuario reinicia el equipo, pulsa F11 cuando aparezca el aviso "Press F11 for Acronis Startup Recovery Manager..." y realiza recuperación de datos en la misma manera que con un medio de inicio común.

Limitación: requiere la reactivación de cargadores que no sean los de Windows ni GRUB.

### Agente (Agente Acronis Backup & Recovery 10)

Una aplicación que realiza copias de seguridad de datos y recuperación, y que permite otras operaciones de gestión en el equipo (pág. 405), como gestión de tareas y operaciones con discos duros.

El tipo de datos con los que se puede realizar una copia de seguridad depende del tipo de agente. Acronis Backup & Recovery 10 incluye los agentes para realizar copias de seguridad de discos y archivos, y los agentes para copias de seguridad para máquinas virtuales que se encuentran en los servidores de virtualización.

## Agente de inicio

Es una herramienta de rescate de inicio que incluye la mayor parte de la funcionalidad del agente Acronis Backup & Recovery 10 (pág. 400). El agente de inicio está basado en un núcleo de Linux. Se puede iniciar un equipo (pág. 405) desde un agente de inicio utilizando medios de inicio (pág. 410) o Acronis PXE Server. Las operaciones se pueden configurar y controlar tanto de manera local, por medio de una interfaz de usuario, como de manera remota, por medio de la consola (pág. 403).

## Archivo comprimido

Consulte el archivo de copia de seguridad (pág. 401).

## Archivo comprimido cifrado

Es un archivo cifrado de copias de seguridad (pág. 401) de acuerdo con Advanced Encryption Standard (AES). Cuando se establece la opción de cifrado y contraseña del archivo en las opciones de copia de seguridad (pág. 410), el agente (pág. 400) cifra cada copia de seguridad que pertenece al archivo antes de guardar la copia de seguridad a su destino.

El algoritmo criptográfico AES funciona en el modo Cipher-block chaining (CBC) y utiliza una clave generada de manera aleatoria con un tamaño definido por el usuario de 128, 192 ó 256 bits. Entonces se cifra la clave de cifrado con AES-256 con un hash SHA-256 de la contraseña como clave. No se almacena la contraseña en el disco o en el archivo de copia de seguridad, el hash de la contraseña se usa para verificación. Con esta seguridad con dos niveles, los datos de copia de seguridad están protegidos contra el acceso no autorizado.

## Archivo de copia de seguridad (Archivo)

Un conjunto de copias de seguridad (pág. 404) creadas y gestionadas por un plan de copias de seguridad (pág. 411). Un archivo puede tener varias copias de seguridad completas (pág. 403), como también copias de seguridad diferenciales (pág. 404) e incrementales. (pág. 404) Las copias de seguridad que pertenecen al mismo archivo se guardan siempre en la misma ubicación. Los planes de copias de seguridad múltiples pueden copiar la misma ubicación en el mismo archivo, pero el modelo dominante es "un plan, un archivo".

Las copias de seguridad en un archivo son manejadas por completo por el plan de copia de seguridad. Las operaciones manuales con archivos (validación (pág. 414), visualización de contenidos, montaje y eliminación de copias de seguridad) se debería realizar con Acronis Backup & Recovery 10. No modifique sus archivos con herramientas incompatibles con Acronis, como Windows Explorer o gestores de terceros.

# B

## Bóveda

Es un lugar para almacenar archivos de copia de seguridad (pág. 401). Se puede organizar una bóveda en una unidad o medio extraíble local o de red, como una unidad USB externa. No hay configuración para el límite del tamaño de la bóveda o el número de copias de seguridad en una

bóveda. Puede limitar el tamaño de cada archivo con una limpieza (pág. 408), pero el tamaño total de los archivos almacenados en la bóveda sólo está limitado por el tamaño de almacenamiento.

## Bóveda centralizada

Es una ubicación de red asignada por el administrador de management server (pág. 409) para que funcione como almacenamiento de archivos de copias de seguridad (pág. 401). Una bóveda centralizada puede ser gestionada por el nodo de almacenamiento (pág. 410) o quedar sin gestión. El tamaño y cantidad total de archivos almacenados en una bóveda centralizada están limitados solamente por el tamaño de almacenamiento.

Tan pronto como el administrador del management server crea una bóveda centralizada, el nombre y la ruta de la bóveda se distribuyen por todos los equipos registrados (pág. 405) en el servidor. El vínculo a la bóveda aparece en los equipos en la lista de bóvedas centralizadas. Cualquier plan de copia de seguridad (pág. 411) existente en los equipos, incluidos los planes locales, puede usar la bóveda centralizada.

En un equipo que no está registrado en el servidor de administración, un usuario que tiene privilegios para realizar copias de seguridad en la bóveda centralizada puede hacerlo al especificar la ruta completa a la bóveda. Si es una bóveda gestionada, los archivos del usuario serán gestionados por el nodo de almacenamiento como también los archivos almacenados en la bóveda.

## Bóveda cifrada

Es una bóveda gestionada (pág. 402) en la que se cifra todo lo que se guarda y en donde el nodo de almacenamiento (pág. 410) descifra de modo claro todo lo que se lee, por medio de una clave de cifrado específica de la bóveda guardada en el nodo. En el caso de robo o acceso por una persona no autorizada, el malhechor no podrá descifrar los contenidos de la bóveda si no tiene acceso al nodo de almacenamiento. Los archivos cifrados (pág. 401) serán cifrados por encima de lo cifrado por el agente (pág. 400).

## Bóveda de deduplicación

Es una bóveda gestionada (pág. 402) en la que se habilita la deduplicación (pág. 404).

## Bóveda gestionada

Es una bóveda centralizada (pág. 402) gestionada por un nodo de almacenamiento (pág. 410). Se puede acceder a los archivos (pág. 401) en una bóveda gestionada de la siguiente manera:

bsp://node_address/vault_name/archive_name/

Físicamente, las bóvedas gestionadas pueden residir en una red compartida, SAN, NAS, en un disco duro local conectado al nodo de almacenamiento, o en una biblioteca de cintas conectada de manera local al nodo de almacenamiento. El nodo de almacenamiento realiza limpieza del lado del nodo de almacenamiento (pág. 409) y validación del lado del nodo de almacenamiento (pág. 414) por cada archivo almacenado en la bóveda gestionada. El administrador puede especificar las operaciones adicionales que el nodo de almacenamiento realizará (cifrado, deduplicación (pág. 404)).

Todas las bóvedas administradas son autónomas, es decir, contienen todos los metadatos que el nodo de almacenamiento necesita para administrar la bóveda. En caso de pérdida del nodo de almacenamiento o de daño de su base de datos, el nuevo nodo de almacenamiento recupera los metadatos y crea nuevamente la base de datos. Cuando la bóveda está conectada a otro nodo de almacenamiento, se realiza el mismo proceso.

## Bóveda personal

Es una bóveda (pág. 401) local o de red creada por gestión directa (pág. 406). Una vez que se crea una bóveda personal, aparece un vínculo debajo del elemento **Bóvedas personales** del panel de **Navegación**. Varios equipos pueden usar la ubicación física, por ejemplo, una red compartida como una bóveda personal.

## Bóveda sin gestionar

Es cualquier bóveda (pág. 401) que no esté gestionada (pág. 402).

# C

## Complemento de Acronis para WinPE

Una modificación del agente para Windows de Acronis Backup & Recovery 10 que puede ejecutarse en el entorno de preinstalación. Es posible añadir el complemento a una imagen WinPE (pág. 415) con el generador de dispositivos de inicio. El medio de inicio (pág. 410) resultante se puede usar para iniciar cualquier equipo compatible con PC y realizar,con ciertas limitaciones, la mayoría de las operaciones de gestión directa (pág. 406) sin la ayuda de un sistema operativo. Las operaciones se pueden configurar y controlar tanto de manera local, por medio de una interfaz de usuario, como de manera remota, por medio de la consola (pág. 403).

## Consola (Acronis Backup & Recovery 10 Management Console)

Una herramienta para el acceso local o remoto de agentes Acronis (pág. 400) y Acronis Backup & Recovery 10 Management Server (pág. 409).

Una vez que se establece la conexión de la consola con el management server, el administrador establece y gestiona las políticas de copias de seguridad (pág. 412) y acceder a otra funcionalidad del servidor de gestión, es decir, realiza la gestión centralizada (pág. 406). El uso de la conexión directa de la consola y el agente, el administrador realiza gestión directa (pág. 406).

## Consolidación

La combinación de dos o más copias de seguridad (pág. 404) subsecuentes que pertenecen al mismo archivo comprimido (pág. 401) en una sola copia de seguridad.

Se puede necesitar la consolidación cuando se elimina copias de seguridad, tanto de manera manual o durante la limpieza (pág. 408). Por ejemplo, las reglas de retención requiere la eliminación de una copia de seguridad completa (pág. 403) que caducó pero guarda la siguiente copia incremental (pág. 404). Las copias de seguridad serán combinadas en una sola copia de seguridad que tendrá la fecha del copia de seguridad incremental. Debido a que mover los archivos puede demorar mucho tiempo e implicar el uso de recursos del sistema, las reglas de retención proporcionan una opción para no eliminar las copias de seguridad con dependencias. En nuestro ejemplo, se conservará la copia de seguridad completa hasta que la copia incremental también sea obsoleta. Después, se eliminarán las copias de seguridad.

## Copia de seguridad completa

Es una copia de seguridad (pág. 404) autosuficiente que contiene todos los datos seleccionados para la copia de seguridad. No necesita acceso a otra copia de seguridad para recuperar los datos de cualquier copia de seguridad completa.

## Copia de seguridad del disco (Imagen)

Una copia de seguridad (pág. 404) que contiene una copia basada en un sector del disco o un volumen en una forma compacta. Por lo general, se copian sólo los sectores que contienen datos. Acronis Backup & Recovery 10 proporciona la opción de tomar una imagen sin procesar, es decir, copia todo los sectores del disco, lo que permite imágenes de sistemas de archivos no compatibles.

## Copia de seguridad diferencial

La copia de seguridad diferencial almacena los cambios de los datos a partir de la última copia de seguridad completa (pág. 403). Necesita acceso a la copia de seguridad completa correspondiente para recuperar los datos de una copia de seguridad diferencial.

## Copia de seguridad incremental

Es una copia de seguridad que almacena los cambios de los datos a partir de la última copia de seguridad (pág. 404). Necesita tener acceso a otras copias de seguridad del mismo archivo (pág. 401) para restaurar los datos de una copia de seguridad incremental.

## Crear copia de seguridad

Una copia de seguridad es el resultado de una única operación de copia de seguridad (pág. 411). Físicamente, es un archivo o un registro de cinta que contiene una copia de los datos en una fecha y hora específica. Los archivos de copia de seguridad creados con Acronis Backup & Recovery 10 tienen la extensión TIB. Los archivos TIB que son el resultado de una exportación (pág. 406) o consolidación (pág. 403) de una copia de seguridad también se denominan copias de seguridad.

# D

## Deduplicación

Es un método diferente de almacenamiento que duplica la misma información sólo una vez.

Acronis Backup & Recovery 10 puede aplicar la tecnología de desduplicación a los archivos de copia de seguridad (pág. 401) almacenados en los nodos de almacenamiento (pág. 410). Esto minimiza el espacio de almacenamiento de los archivos, el tráfico de copias de seguridad y el uso de la red durante las copias de seguridad.

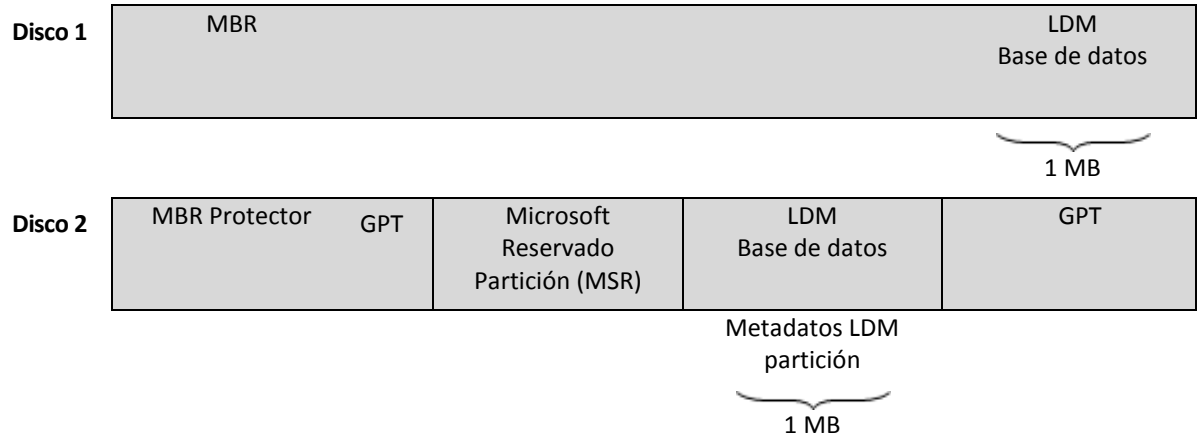
## Disco dinámico

Los discos duros gestionados con el Administrador de discos lógicos (LDM) disponible en Windows desde Windows 2000. LDM ayuda a asignar flexiblemente los volúmenes en un dispositivo de almacenamiento para una mejor tolerancia a fallos, mejor rendimiento o mayor tamaño de volumen.

Un disco dinámico puede usar tanto el estilo de partición Registro de inicio maestro (MBR) o Tabla de partición GUID (GPT). Además de MBR o GPT, cada disco dinámico tiene una base de datos oculta en donde LDM almacena la configuración de volúmenes dinámicos. Cada disco dinámico retiene toda la

información sobre los volúmenes dinámicos existentes en el grupo de discos, lo que mejora la confiabilidad del almacenamiento. La base de datos ocupa al menos 1 MB de un disco MBR. En un disco GPT, Windows crea una partición dedicada de metadatos LDM, lo que toma espacio de la partición reservada de Microsoft (MSR).




**Los discos dinámicos organizados con discos MBR (Disco 1) y GPT (Disco 2).**

Para obtener más información sobre los grupos de discos dinámicos, consulte el siguiente artículo de la Base de Conocimiento de Microsoft:

Gestión del disco (Windows XP Professional Resource Kit) http://technet.microsoft.com/en-us/library/bb457110.aspx.

816307 Mejores prácticas para el uso de los discos dinámicos en equipos con Windows Server 2003 http://support.microsoft.com/kb/816307/es.

# E

## Equipo

Es un equipo físico o virtual identificado por la instalación del sistema operativo. Los equipos con varios sistemas operativos (sistemas con múltiples inicios) son considerados como equipos múltiples.

## Equipo físico

En el Acronis Backup & Recovery 10 Management Server, un equipo físico es lo mismo al equipo registrado (pág. 405). Se considera que una máquina virtual es física si hay un agente de Acronis Backup & Recovery 10 instalado en el equipo y el equipo está registrado en el management server.

## Equipo gestionado

Es un equipo (pág. 405), tanto físico como virtual cuando al menos tiene un agente instalado de Acronis Backup & Recovery 10. (pág. 400)

## Equipo registrado

Un equipo (pág. 405) gestionado por el management server (pág. 409). Se puede registrar un solo equipo a la vez en un management server. Un equipo se encuentra registrado como resultado del proceso de registro (pág. 412).

## Equipo virtual

En el Acronis Backup & Recovery 10 Management Server, se considera que es una máquina (pág. 405) es virtual si se puede realizar una copia de seguridad del servidor de virtualización sin instalar un agente (pág. 400) en el equipo. Una máquina virtual aparece en el management server después del registro del servidor de virtualización que alberga el equipo, ya que el agente Acronis Backup & Recovery 10 para máquinas virtuales está instalado en dicho servidor.

## Esquema de copias de seguridad

Una parte del plan de copia de seguridad (pág. 411) que incluye el programa de copia de seguridad y (de manera opcional) las reglas de retención del programa de limpieza (pág. 408). Por ejemplo, realice una copia de seguridad completa (pág. 403) mensualmente en el último día del mes a las 10:00 h y una copia de seguridad incremental (pág. 404) los domingos a las 22:00 h. Elimina copias de seguridad que tienen más de tres meses. Verifica dichas copias de seguridad cada vez que se completa una operación de respaldo.

Acronis Backup & Recovery 10 ofrece la capacidad de usar programas conocidos y optimizados para copias de seguridad, como GFS y Torre de Hanói, para crear un esquema de copias de seguridad personalizado o hacer copias de seguridad solo una vez.

## Exportar

Una operación que crea una copia de un archivo comprimido (pág. 401) o una copia parcial de un archivo comprimido en la ubicación especificada. La operación de exportación se puede aplicar a un único archivo comprimido, una única copia de seguridad (pág. 404) o a su selección de copias de seguridad que pertenecen al mismo archivo comprimido. Se puede exportar una bóveda (pág. 401) completa utilizando la interfaz de línea de comandos.

# G

## Generador de dispositivos

Es una herramienta dedicada a la creación de medios de inicio (pág. 410).

## Gestión centralizada

La gestión de la infraestructura Acronis Backup & Recovery 10 por medio de una unidad de gestión central conocida como Acronis Backup & Recovery 10 Management Server (pág. 409). Las operaciones de gestión centralizada incluyen:

- Creación, aplicación y gestión de políticas de copias de seguridad (pág. 412)
- Creación y gestión de grupos dinámicos (pág. 408) y estáticos (pág. 408) de equipos (pág. 405)
- Gestión de las tareas (pág. 413) existentes en los equipos
- Creación y gestión de las bóvedas centralizadas (pág. 402) para el almacenamiento de archivos
- Gestión de nodos de almacenamiento (pág. 410)
- Actividades de supervisión de componentes de Acronis Backup & Recovery 10 , visualización del registro centralizado y más.

## Gestión directa

Cualquier operación de gestión que se realice en un equipo gestionado (pág. 405) por medio de la conexión entre consola (pág. 403) y agente (pág. 400) (a diferencia de la gestión centralizada (pág. 406) en donde se configura las operaciones en el management server (pág. 409) y se propaga por el servidor de los equipos gestionados).

Las operaciones de gestión directa incluyen:

- La creación y gestión de planes de copias de seguridad locales (pág. 412)
- La creación y gestión de tareas locales (pág. 413), como tareas de recuperación
- La creación y gestión de la bóveda personal (pág. 403) y los archivos almacenados allí
- La visualización del estado, progreso y propiedades de las tareas centralizadas (pág. 413) que existen en el equipo
- Visualización y gestión del registro de las operaciones del agente
- Operaciones de gestión de disco, como la clonación del disco, creación del volumen, conversión de volumen.

Se realiza un tipo de gestión directa cuando se usa medios de inicio (pág. 410). También se pueden realizar algunas de las operaciones de gestión directa por medio de la interfaz del management server. Sin embargo, esto implica tanto una conexión explícita como implícita del equipo seleccionado.

## GFS (Abuelo-padre-hijo)

Un popular esquema de copia de seguridad (pág. 406) que permite el mantenimiento de un equilibrio óptimo entre el tamaño del archivo de copia de seguridad (pág. 401) y el número de los puntos de recuperación (pág. 412) disponibles del archivo. GFS permite la recuperación con resolución diaria para los últimos días, una resolución semanal por las últimas semanas y una resolución mensual para cualquier momento en el pasado.

Para más información, consulte esquema de copias de seguridad GFS (pág. 35).

## Grupo de disco

Es una variedad de discos dinámicos (pág. 404) que almacenan los datos comunes de configuración en sus bases de datos LDM y por lo tanto se pueden gestionar como uno solo. Por lo general, todos los discos dinámicos creados dentro del mismo equipo (pág. 405) son miembros del mismo grupo de discos.

Tan pronto como se cree el primer disco dinámico con LDM u otra herramienta de gestión de discos, el nombre del grupo de discos se encuentra en la clave del registro HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmio\Boot Info\Primary Disk Group\Name.

Los discos creados o importados a continuación son agregados al mismo grupo de discos. El grupo existe siempre que exista al menos uno de sus miembros. Una vez que se desconecta el último disco dinámico o se lo convierte a básico, el grupo queda suspendido, si bien su nombre queda en la clave de registro que se nombró antes. En el caso de que se conecte o se cree de nuevo un disco, se crea un grupo de discos con un nombre incremental.

Cuando se mueva un grupo de discos a otro equipo, se lo considerará como "externo" y no se podrá usar hasta que se lo importe al grupo de discos existentes. El proceso de importación actualiza los datos de configuración tanto de los discos locales como externos para que puedan formar una sola

entidad. Los grupos externos se importan tal como están (tendrán el nombre original) si no existe el grupo de discos en el equipo.

Para obtener más información sobre los grupos de discos, consulte el siguiente artículo de la Base de Conocimiento de Microsoft:

222189 Descripción de Grupos de Discos en Administrador de discos de Windows http://support.microsoft.com/kb/222189/es.

## Grupo dinámico

Es un grupo de equipos (pág. 405) que el management server (pág. 409) completa automáticamente de acuerdo a los criterios de pertenencia que especifica el administrador. Acronis Backup & Recovery 10 ofrece los siguientes criterios de pertenencia:

- Sistema operativo
- Unidad organizativa de Active Directory
- Rango de dirección IP.

Un equipo sigue siendo parte de un grupo dinámico siempre que el equipo cumpla con los criterio del grupo. Se elimina automáticamente al equipo del grupo tan pronto como

- las propiedades del equipo cambian para que el equipo deje de cumplir con los criterios ó
- el administrador cambia los criterios para que el equipo deje de cumplir con los criterios.

No hay manera de eliminar manualmente un equipo de una grupo dinámico, excepto por la eliminación del equipo del management server.

## Grupo estático

Es un grupo de equipos que el administrador del management server (pág. 409) poblará manualmente al cargar los equipos al grupo. Un equipo permanece en un grupo estático hasta que el administrador elimina del grupo o del management server.

## Grupo incorporado

Es un grupo de equipos que siempre existe en un management server (pág. 409).

Un management server tiene dos grupos integrados que contienen dos equipos de cada tipo: Todos los equipos físicos (pág. 405), todas las máquinas virtuales (pág. 405).

No se pueden eliminar, ni mover a otros grupos o modificar manualmente a los grupos integrados. Los grupos personalizados no pueden ser creados dentro de grupos integrados. No hay manera de quitar un equipo físico del grupo integrado, salvo por la eliminación del equipo del management server. Las máquinas virtuales son eliminadas como resultado de la eliminación del servidor.

Se puede aplicar una política de copia de seguridad (pág. 412) en un grupo integrado.

# I

## Imagen

El mismo que en Copia de seguridad del disco (pág. 404).

# L

## Limpieza

Es la eliminación de copias de seguridad (pág. 404) de un archivo de copia de seguridad (pág. 401) para eliminar las copias de seguridad desactualizadas o prevenir que el archivo exceda el tamaño deseado.

La limpieza incluye la aplicación a un archivo de reglas de retención establecidas por el plan de copia de seguridad (pág. 411) que produce el archivo. Esta operación verifica si el archivo excede su tamaño máximo o para las copias de seguridad caducadas. Esto puede eliminar las copias de seguridad, dependiendo de si se exceden las reglas de retención.

Para obtener más información, consulte: Reglas de retención (pág. 42).

## Limpieza del lado del agente

La limpieza (pág. 408) realizada por un agente (pág. 400) de acuerdo al plan de copia de seguridad (pág. 411) que produce el archivo (pág. 401). La limpieza del lado del agente la realizan las bóvedas sin gestionar (pág. 403).

## Limpieza del lado del nodo de almacenamiento

La limpieza (pág. 408) realizada por un nodo de almacenamient (pág. 410)o de acuerdo a los planes de copias de seguridad (pág. 411) que guarda los archivos (pág. 401) en una bóveda gestionada (pág. 402). Como es una alternativa a la limpieza del lado del agente (pág. 409), la limpieza del lado del nodo de almacenamiento evita la carga innecesaria de la CPU de los servidores de producción.

Puesto que el programa de limpieza existe en el equipo (pág. 405) en donde está el agente (pág. 400), y por lo tanto usa la hora y sucesos del equipo, el agente debe iniciar la limpieza del lado del nodo de almacenamiento cada vez que sucede el momento o suceso programado. Para hacerlo, el agente debe estar en línea.

La siguiente tabla resume los tipos de limpieza usados en Acronis Backup & Recovery 10.

| | **Limpieza** | |
|---|---|---|
| | **Del lado del agente** | **Almacenamiento del lado del nodo** |
| **Se aplica a:** | Archivo comprimido | Archivo comprimido |
| **Iniciado por:** | Agente | Agente |
| **Realizado por:** | Agente | Nodo de almacenamiento |
| **Programación establecida por:** | Plan de copia de seguridad | Plan de copia de seguridad |
| **Reglas de retención establecidas por:** | Plan de copia de seguridad | Plan de copia de seguridad |

# M

## Management server (Acronis Backup & Recovery 10 Management Server)

Es un servidor central que gestiona la protección de datos dentro de la red empresarial. Acronis Backup & Recovery 10 Management Server le proporciona al administrador lo siguiente:

- un punto de acceso a la infraestructura Acronis Backup & Recovery 10
- Una manera fácil de proteger los datos en varios equipos (pág. 405) con políticas de copia de seguridad (pág. 412) y agrupación
- Funcionalidad de supervisión en toda la empresa
- La capacidad de crear bóvedas centralizadas (pág. 402) para guardar los archivos de copias de seguridad (pág. 401) de la empresa.
- La capacidad de gestionar los nodos de almacenamiento (pág. 410).

Si hay varios management server en la red, funcionan independientemente, gestionan diferentes equipos y utilizan las bóvedas centralizadas para almacenamiento de archivos.

## Medio de inicio

Es un medio físico (CD, DVD, unidad de memoria flash USB u otros medios admitidos por el BIOS del equipo (pág. 405) que se usa como dispositivo de inicio) que contienen el agente de inicio (pág. 401) o en el entorno de preinstalación de Windows (WinPE) (pág. 415) con el complemento Acronis para WinPE (pág. 403). Se puede iniciar un equipo en los entornos antedichos que se usan el inicio por red de Acronis PXE Server o Servicio de Instalación Remota (RIS). Estos servidores con componentes de inicio cargados también pueden ser medios de inicio.

Los dispositivos de arranque se usan con frecuencia para:

- recuperar de un sistema operativo que no puede iniciar
- acceder a los datos que sobrevivieron en un sistema dañado y realizar copias de seguridad de éstos
- implementar un sistema operativo desde cero
- Creación completa de volúmenes básicos o dinámicos (pág. 414)
- Copia de seguridad sector por sector de un disco que tiene un sistema de archivos incompatible.
- realizar copias de seguridad fuera de línea de cualquier dato que no se puede incluir en la copia de seguridad en línea por acceso restricto, con un bloqueo permanente por las aplicaciones en ejecución o por cualquier otra razón.

# N

## Nodo de almacenamiento (Acronis Backup & Recovery 10 Nodo de almacenamiento)

Es un servidor que permite optimizar el uso de diversos recursos necesarios para la protección de los datos de una empresa. Este objetivo se logra al organizar las bóvedas gestionadas (pág. 402). El nodo de almacenamiento le permite al administrador:

- Evita la carga innecesaria de la CPU de los equipos gestionados (pág. 405) al usar la limpieza del lado de los nodos de almacenamiento (pág. 409) y la validación del lado del nodo de almacenamiento (pág. 414)
- Reduce drásticamente el tráfico de la copia de seguridad y el espacio de almacenamiento que ocupan los archivos (pág. 401) al usar la deduplicación (pág. 404)
- Previene que malhechores tengan acceso a los archivos de copias de seguridad, incluso en caso de robo del medio de almacenamiento, al usar bóvedas cifradas (pág. 402).

# O

## Opciones de copia de seguridad

Son los parámetros de configuración de una operación de copia de seguridad (pág. 411) como comandos pre/post de copia de seguridad, asignación del máximo ancho de banda de la red para el flujo de la copia de seguridad o del nivel de compresión de datos. Las opciones de copia de seguridad son parte del plan de copia de seguridad (pág. 411).

## Operación de copia de seguridad

Es una operación que crea una copia de los datos que existen en el disco duro del equipo (pág. 405) para la recuperación o reversión de los datos a una fecha y hora específicos.

# P

## Plan

Consulte el plan de copia de seguridad (pág. 411).

## Plan de copia de seguridad (Plan)

Es un conjunto de reglas que especifican como se protegerán los datos en algún equipo. Un plan de copia de seguridad especifica:

- Los datos para incluir en la copia de seguridad
- La ubicación en donde se almacenará el archivo de copia de seguridad (pág. 401) (el nombre y ubicación del archivo de copia de seguridad)
- El esquema de copia de seguridad (pág. 406) incluye el programa de copia de seguridad y de manera opcional las reglas de retención
- De manera opcional, el archivo de validación de reglas (pág. 413)
- Las opciones de copia de seguridad (pág. 410).

Por ejemplo, un plan de copia de seguridad puede contener la siguiente información:

- Copia de seguridad del volumen C: **(estos son los datos que el plan protegerá)**
- Nombre al archivo como MySystemVolume y ubíquelo en \\server\backups\ (**es el nombre y la ubicación del archivo**)
- Realiza una copia de seguridad completa por mes en el último día del mes a las 10:00 y copias de seguridad incrementales los domingos a las 22:00. Elimina la copias de seguridad que tienen más de tres meses **(es el esquema de copia de seguridad)**
- Valida la última copia de seguridad inmediatamente después de su creación **(es una regla de validación)**
- Protege el archivo con una contraseña **(es una opción).**

Físicamente, un plan de copia de seguridad es un paquete de tareas (pág. 413) configuradas para la ejecución en un equipo gestionado (pág. 405).

Se puede crear un plan de copia de seguridad directamente en el equipo (plan local) o puede aparecer en el equipo como resultado de la implementación de una política de copia de seguridad (pág. 412) (plan centralizado (pág. 411)).

## Plan de copia de seguridad centralizado

Un plan de copia de seguridad (pág. 411) que parece en el equipo gestionado (pág. 405) como resultado de la implementación de la política de la copia de seguridad (pág. 412) del management server (pág. 409). Dicho plan se puede modificar sólo al editar la política de copia de seguridad.

## Plan de copia de seguridad local

Es un plan de copia de seguridad (pág. 411) creado en un equipo gestionado (pág. 405) por medio de la gestión directa (pág. 406).

## Política

Consulte la política de copias de seguridad (pág. 412).

## Política de copia de seguridad (Política)

El administrador de Management server (pág. 409) crea las plantillas del plan de copia de seguridad y las almacena en el management server. Una política de copias de seguridad tiene las mismas reglas que un plan de copias de seguridad, pero no se pueden especificar los datos a respaldar explícitamente. En cambio, se pueden usar las reglas de selección (pág. 413), como las variables de entorno. Debido a la flexibilidad de la selección, una política de copias de seguridad se puede aplicar centralmente a varios equipos. Si se especifica explícitamente un elemento de datos (p. ej. /dev/sda o C:\Windows), la política realizará copias de seguridad del elemento en cada equipo en donde existe la ruta exacta.

Al aplicar la política a un grupo de equipos, el administrador implementa varios planes de copias de seguridad con una sola acción.

El flujo de trabajo cuando se usan políticas es las siguiente:

1. El administrador crea la política de seguridad.
2. El administrador aplica la política a un grupo de equipos o a un solo equipo (pág. 405).
3. El management server implementa la política en los equipos.
4. En cada equipo, el agente (pág. 400) instalado en el equipo encuentra los elementos de datos por medio de las reglas de selección. Por ejemplo, si la regla de selección es [Todos los volúmenes], se hará una copia de seguridad de todo el equipo.
5. En cada equipo, el agente instalado crea un plan de copias de seguridad (pág. 411) por medio de otras reglas especificadas por la política. A este plan de copia de seguridad se lo denomina plan centralizado (pág. 411).
6. En cada equipo, el agente instalado crea un conjunto de tareas centralizadas (pág. 413) que lleva a cabo el plan.

## Punto de recuperación

Es la hora y fecha a la que se puede revertir los datos de la copia de seguridad.

# R

## Registro

Es un proceso que agrega un equipo gestionado (pág. 405) a un management server (pág. 409).

El registro establece una relación de confianza entre el agente (pág. 400) del equipo y el servidor. Durante el registro, la consola recupera el certificado del cliente de management server y lo pasa al agente que lo usa después para autenticar los clientes que intentan establecer una conexión. Esto evita intentos de ataques a la red que consisten en establecer una conexión falsa de parte de un miembro de confianza (management server).

## Regla de selección

Es una parte de la política de copias de seguridad (pág. 412). Le permite al administrador del management server (pág. 409) la selección de los datos a respaldar dentro de un equipo.

## Reglas de validación

Es una parte de la política de copias de seguridad (pág. 411). Las reglas que definen cómo y la asiduidad para realizar la validación y si la validación (pág. 414) de todo el archivo (pág. 401) o la última copia de seguridad del archivo.

# T

## Tarea

En AcronisBackup & Recovery 10, una tarea es un conjunto de acciones secuenciales que deben realizarse en un equipo gestionado (pág. 405) cuando se llega a un tiempo o sucede cierto suceso. Las acciones se describen en un archivo de secuencia de comandos xml. La condición de inicio (programa) existe en las claves protegidas del registro.

## Tarea centralizada

Es una tarea (pág. 413) que pertenece a un plan de copia de seguridad centralizada (pág. 411). Dicha tarea aparece en el equipo gestionado (pág. 405) como resultado de la implementación de la política de copia de seguridad (pág. 412) del management server (pág. 409) y se puede modificar sólo por la edición de la política de copia de edición.

## Tarea local

Es una tarea (pág. 413) que pertenece al plan local de copias de seguridad (pág. 412) o tarea que no pertenece a un plan, como una tarea de recuperación. Sólo se puede modificar una tarea local que pertenece a una plan de copia de seguridad al editar el plan; otras tareas locales se pueden modificar directamente.

## Torres de Hanói

Un popular esquema de copia de seguridad (pág. 406) que permite el mantenimiento de un equilibrio óptimo entre el tamaño del archivo de copia de seguridad (pág. 401) y el número de los puntos de recuperación (pág. 412) disponibles del archivo comprimido. A diferencia del esquema GFS (pág. 407) que posee solo tres niveles de resolución de recuperación (resolución diaria, semanal y mensual), el esquema Torres de Hanói reduce continuamente el intervalo de tiempo entre los puntos de recuperación a medida que incrementa la antigüedad de la copia de seguridad. Esto permite un uso muy eficaz del almacenamiento de las copias de seguridad.

Para obtener más información, consulte "Esquema de copias de seguridad Torres de Hanói" (pág. 39).

# U

## Universal Restore (Acronis Backup & Recovery 10 Universal Restore)

La tecnología propia de Acronis ayuda a iniciar Windows en hardware diferente o una máquina virtual. Universal Restore maneja diferentes dispositivos que son críticos para el inicio del sistema operativo, como controladores de almacenamiento, placa madre o conjunto de chips.

Universal Restore no está disponible:

- Cuando se inicia el equipo con Acronis Startup Recovery Manager (pág. 400) (con F11) o
- la imagen que se recupera se encuentra en Acronis Secure Zone (pág. 400) o
- Cuando se usa Acronis Active Restore (pág. 400),

debido a que estas funciones fueron especialmente diseñadas para la recuperación instantánea de datos en el mismo equipo.

Universal Restore no está disponible cuando se recupera Linux.

# V

## Validación

Una operación que verifica la posibilidad de recuperación de datos en una copia de seguridad (pág. 404).

La validación de la copia de seguridad de un archivo imita la recuperación de todos los archivos de la copia de seguridad a un destino  Las versiones previas del producto consideraban que la copa de seguridad de un archivo era válida cuando los metadatos del encabezado era consistente. El método actual lleva tiempo pero es mucho más confiable. La validación de la copia de seguridad del volumen calcula la suma de comprobación por cada bloque de datos guardados en la copia de seguridad. Este proceso también usa más recursos.

Si bien la validación satisfactoria significa una gran probabilidad de tener una recuperación exitosa, no verifica todos los factores que influencian el proceso de recuperación. Si realiza una copia de seguridad del sistema operativo, sólo se podrá garantizar una recuperación exitosa con una recuperación de prueba del medio de inicio a un disco duro libre.

## Validación del lado del agente

Es la validación (pág. 414) realizada por un agente (pág. 400) de acuerdo al plan de copia de seguridad (pág. 411) que produce el archivo (pág. 401). La validación del lado del agente la realiza las bóvedas sin gestionar (pág. 403).

## Validación del lado del nodo de almacenamiento

La validación (pág. 414) realizada por un nodo de almacenamient (pág. 410)o de acuerdo a los planes de copias de seguridad (pág. 411) que guarda los archivos (pág. 401) en una ubicación gestionada (pág. 402). Como es una alternativa a la validación del lado del agente (pág. 414), la validación del lado del nodo de almacenamiento evita la carga innecesaria de la CPU de los servidores de producción.

## Volumen dinámico

Es cualquier volumen ubicado en discos dinámicos (pág. 404), o más precisamente, en un grupo de discos (pág. 407). Los volúmenes dinámicos pueden abarcar múltiples discos. Los volúmenes dinámicos se configuran dependiendo del objetivo:

- Aumento del tamaño del volumen (volumen extendido).
- Reducción del tiempo de acceso (un volumen segmentado).
- Logra la tolerancia a fallos al incluir redundancia (volúmenes replicados y RAID-5).

# W

## WinPE (Entorno de preinstalación de Windows)

Es un sistema Windows reducido basado en alguno de los siguientes núcleos:

- Windows XP Professional con Service Pack 2 (PE 1.5)
- Windows Server 2003 con Service Pack 1 (PE 1.6)
- Windows Vista (PE 2.0)
- Windows Vista SP1 y Windows Server 2008 (PE 2.1).

Win PE suele utilizarse por fabricantes de equipos originales (OEM) y corporaciones para implementar, probar, diagnosticar y reparar sistemas. Se puede iniciar un equipo con WinPE mediante PXE, CD-ROM, unidad de memoria flash USB o disco duro. Complemento de Acronis para WinPE (pág. 403) permite la ejecución del agente Acronis Backup & Recovery 10 (pág. 400) entorno de preinstalación.