Portal de gestión

24.03

Guía del administrador de la empresa

REVISIÓN: 11/04/2024

Contenido

Acerca de este documento

Este documento está dirigido a los administradores de clientes que quieren utilizar el portal de administración de la nube para crear y gestionar cuentas de usuario, unidades y cuotas; para configurar y controlar el acceso estas, y para supervisar el uso y las operaciones de su organización en la nube.

Acerca del portal de gestión

El portal de gestión es una interfaz web para la plataforma de la nube que proporciona servicios de protección de datos.

Cada servicio tiene su propia interfaz web, denominada la consola de servicio, el portal de gestión permite a los administradores controlar el uso de los servicios, crear cuentas de usuario y unidades, generar informes y mucho más.

Cuentas y unidades

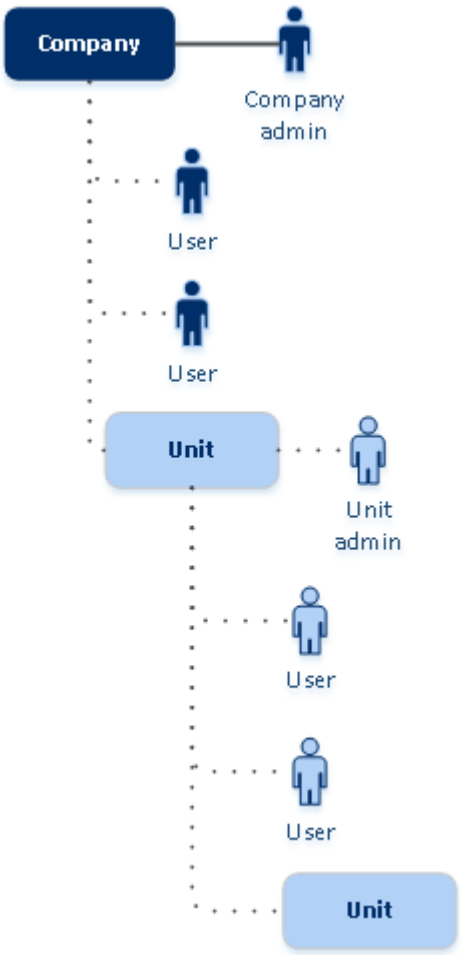
Hay dos tipos de cuentas de usuario: las cuentas de administrador y las cuentas de usuario.

- Los **Administradores** tienen acceso al portal de gestión. Tienen la función de administrador en todos los servicios.
- Los **Usuarios** no tienen acceso al portal de gestión. Su acceso a los servicios y sus funciones en los servicios están definidas por un administrador.

Los administradores pueden crear unidades, que normalmente se corresponden con unidades o departamentos de la organización. Cada cuenta existe en el nivel de la compañía o en una unidad.

Un administrador puede gestionar unidades, cuentas de administrador y cuentas de usuario en su mismo nivel jerárquico o en cualquier nivel inferior.

El diagrama que se muestra a continuación ilustra tres niveles de jerarquía: la compañía y dos unidades. Las cuentas y las unidades opcionales se indican mediante una línea de puntos.



En la siguiente tabla se resumen las operaciones que pueden realizar los administradores y usuarios.

Operación	Usuarios	Administradores
Crear unidades	No	Sí
Crear cuentas	No	Sí
Descargar e instalar el software.	Sí	Sí
Usar servicios	Sí	Sí
Crear informes acerca del uso del servicio	No	Sí

Gestión de cuotas

Las **cuotas** limitan la capacidad que tienen los inquilinos para utilizar el servicio.

En el portal de gestión, puede ver las cuotas de servicio que su proveedor de servicios asignó a su organización, pero no puede gestionarlas.

Puede gestionar las cuotas de servicio de sus usuarios.

Visualización de cuotas para su organización

En el portal de gestión, vaya a **Información general** > **Uso**. Verá un panel de control que muestra las cuotas asignadas a su organización. Las cuotas para cada servicio se muestran en otra pestaña.

Cuotas de Backup

Puede especificar la cuota de almacenamiento en la nube, la de copia de seguridad local y el número máximo de equipos, dispositivos o sitios web que un usuario puede proteger. Están disponibles las siguientes cuotas.

Cuota de dispositivos

- **Estaciones de trabajo**
- **Servidores**
- **Equipos virtuales**
- **Dispositivos móviles**
- **Servidores de alojamiento web** (servidores físicos y virtuales basados en Linux que ejecuten paneles de control Plesk, cPanel, DirectAdmin, VirtualMin o ISPManager)
- **Sitios web**

Se considera que un equipo, un dispositivo o un sitio web están protegidos si se les aplica, como mínimo, un plan de protección. Un dispositivo móvil se considera protegido después de la primera copia de seguridad.

Cuando se supera el límite de exceso de dispositivos, el usuario no puede aplicar un plan de protección a más dispositivos.

Cuotas de orígenes de datos en la nube

- **Licencias de Microsoft 365**

  Esta cuota la aplica el proveedor de servicios a toda la empresa. Los administradores de la empresa pueden ver la cuota y el uso en el portal de gestión.

  La concesión de licencias de usuarios de Microsoft 365 depende del modo de facturación seleccionado para Cyber Protection.

Importante
El agente local y el agente de la nube consumen cuotas independientes. Si lleva a cabo la copia de seguridad de las mismas cargas de trabajo con ambos agentes, se le cobrará dos veces. Por ejemplo:

- Si lleva a cabo la copia de seguridad de los buzones de correo de 120 usuarios con el agente local y la copia de seguridad de los archivos de OneDrive de los mismos usuarios con el agente de la nube, se le cobrarán 240 licencias de Microsoft 365.
- Si lleva a cabo la copia de seguridad de los buzones de correo de 120 usuarios con el agente local y la copia de seguridad de los mismos buzones de correo con el agente de la nube, se le cobrarán 240 licencias de Microsoft 365.

En el modo de facturación **por carga de trabajo**, la cuota de **licencias de Microsoft 365** se cuenta por usuarios únicos. Un usuario único es un usuario que tiene, al menos, uno de los siguientes:

- Buzón de correo protegido
- OneDrive protegido
- Acceso a, como mínimo, un recurso de nivel de empresa protegido: Un sitio de Microsoft 365 SharePoint Online o Microsoft 365 Teams.
  Para comprobar el número de miembros de un sitio de Microsoft 365 SharePoint o Teams, consulte este artículo de la base de conocimientos.

Nota
No se cobra a los usuarios bloqueados de Microsoft 365 que no tienen un buzón de correo personal protegido o OneDrive, y solo pueden acceder a recursos compartidos (buzones de correo compartidos, sitios de SharePoint y Microsoft Teams).

Los usuarios bloqueados son aquellos que no tienen un inicio de sesión válido y no pueden acceder a los servicios de Microsoft 365. Para obtener información sobre cómo bloquear a todos los usuarios sin licencia en una organización de Microsoft 365, consulte "Impedir que los usuarios de Microsoft 365 sin licencia inicien sesión" (p. 11).

No se le cobrará por los siguientes usuarios de Microsoft 365 y no requieren una licencia por usuario:

- Buzones de correo compartidos
- Salas y equipos
- Usuarios externos con acceso a sitios de SharePoint o Microsoft Teams con copia de seguridad

Para obtener más información sobre las opciones de licencia con el modo de facturación por gigabyte, consulte Cyber Protect Cloud: Licencias de Microsoft 365 por GB.

Para obtener más información sobre las opciones de licencia con el modo de facturación por carga de trabajo, consulte Cyber Protect Cloud: Licencias de Microsoft 365 y cambios de precios.

- **Microsoft 365 Teams**

Esta cuota la aplica el proveedor de servicios a toda la empresa. Esta cuota habilita o deshabilita la capacidad de proteger Microsoft 365 Teams y establece el número máximo de equipos que es posible proteger. Para proteger un equipo, independientemente de su número de miembros o canales, se necesita una cuota. Los administradores de la empresa pueden ver la cuota y el uso en el portal de gestión.

- **Microsoft 365 SharePoint Online**

  Esta cuota la aplica el proveedor de servicios a toda la empresa. Esta cuota habilita o deshabilita la capacidad de proteger SharePoint Online y establece el número máximo de recopilaciones de sitios y grupos de sitios que es posible proteger.

  Los administradores de la empresa pueden ver la cuota y el uso en el portal de administración. También pueden ver la cuota junto con la cantidad de almacenamiento que ocupan las copias de seguridad de SharePoint Online en los informes de uso.
- **Licencias de Google Workspace**

  Esta cuota la aplica el proveedor de servicios a toda la empresa. Se puede permitir que la empresa proteja buzones de correo de **Gmail** (incluido Calendar y Contactos), archivos de **Google Drive** o ambos. Los administradores de la empresa pueden ver la cuota y el uso en el portal de gestión.
- **Unidad compartida de Google Workspace**

  Esta cuota la aplica el proveedor de servicios a toda la empresa. Esta cuota habilita o deshabilita la capacidad de proteger unidades compartidas de Google Workspace. Si la cuota está habilitada, se pueden proteger todas las unidades compartidas que se desee. Los administradores de la empresa no pueden ver la cuota en el portal de gestión, pero sí la cantidad de almacenamiento ocupado por copias de seguridad de unidades compartidas en los informes de uso.

  La realización de copias de seguridad de unidades compartidas de Google Workspace solo está disponible para clientes que también tengan una cuota de puestos de Google Workspace como mínimo. Esta cuota solo se verificará, así que el proceso no tardará.

Se considera que una licencia de Microsoft 365 está protegida si se ha aplicado, como mínimo, un plan de protección al buzón de correo o al OneDrive del usuario. Se considera que una licencia de Google Workspace está protegida si se ha aplicado, como mínimo, un plan de protección al buzón de correo o al Google Drive del usuario.

Si se supera el límite de exceso de licencias, el administrador de una empresa no puede aplicar un plan de protección a más licencias.

Cuotas de almacenamiento

- **Copia de seguridad local**

  La cuota de las **Copia de seguridad local** limita el tamaño total de las copias de seguridad locales que se crean mediante el uso de la infraestructura en la cloud. Para esta cuota no se puede establecer un uso por encima del límite.
- **Recursos en la nube**

  La cuota de **Recursos en la nube** combina la cuota del almacenamiento de copias de seguridad y las de recuperación ante desastres. La cuota de almacenamiento de copias de seguridad limita

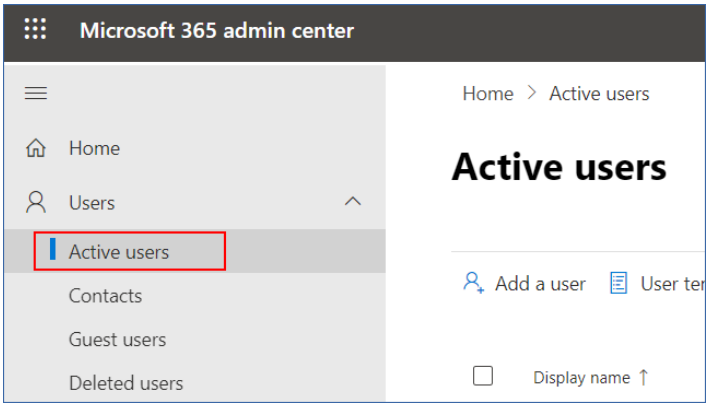
el tamaño total de las copias de seguridad que se encuentran en el almacenamiento en la nube. Si se supera este uso por encima del límite de la cuota de almacenamiento de copias de seguridad, no se realizan copias de seguridad.

Impedir que los usuarios de Microsoft 365 sin licencia inicien sesión

Para impedir que todos los usuarios sin licencia en la organización de Microsoft 365 inicien sesión, puede modificar su estado de inicio de sesión.

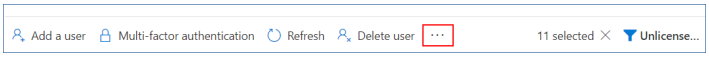
Para impedir que los usuarios sin licencia inicien sesión

1. Inicie sesión en el Centro de administración de Microsoft 365 (https://admin.microsoft.com) como administrador global.
2. En el menú de navegación, vaya a **Usuarios** > **Usuarios activos**.



3. Haga clic en **Filtro** y seleccione **Usuarios sin licencia**.

4. Seleccione las casillas de verificación que se encuentran junto a los nombres de usuario y después haga clic en el icono de puntos suspensivos (...).



5. En el menú, seleccione **Editar estado de inicio de sesión**.
6. Seleccione la casilla de verificación **Impedir que los usuarios inicien sesión** y haga clic en **Guardar**.

Cuotas de Recuperación ante desastres

Nota
Los artículos de oferta de recuperación ante desastres solo están disponibles con el complemento de recuperación ante desastres.

Estas cuotas las aplica el proveedor de servicios a toda la empresa. Los administradores de la empresa pueden ver las cuotas y el uso en el portal de gestión, pero no pueden establecer cuotas para un usuario.

- **Almacenamiento de recuperación ante desastres**

  El almacenamiento de la recuperación ante desastres muestra el tamaño del almacenamiento de copia de seguridad de los servidores protegidos por la recuperación ante desastres. El uso del almacenamiento de recuperación ante desastres es igual al uso del almacenamiento de copia de seguridad de las cargas de trabajo protegidas con servidores de recuperación ante desastres. Este almacenamiento se calcula a partir de la hora en la que se crea el servidor de recuperación, independientemente de si el servidor se está ejecutando actualmente. Si se alcanza el uso por encima del límite para esta cuota, no se podrán crear servidores principales ni de recuperación ni agregar o extender discos de los servidores principales existentes. Si se supera el uso por encima del límite para esta cuota, no se podrá iniciar una conmutación por error ni iniciar un servidor detenido. Los servidores en ejecución siguen funcionando.
- **Puntos de cálculo**

  Esta cuota limita los recursos de la CPU y la RAM que consumen los servidores principales y los de recuperación durante un periodo de facturación. Si se alcanza el uso por encima del límite para esta cuota, todos los servidores principales y de recuperación se apagarán. Estos servidores no se pueden usar hasta que comience el siguiente periodo de facturación. El periodo de facturación predeterminado es un mes completo.

  Cuando la cuota se deshabilita, los servidores no se pueden usar, independientemente del periodo de facturación.
- **Direcciones IP públicas**

  Esta cuota limita el número de direcciones IP públicas que se pueden asignar a los servidores principales y de recuperación. Si se alcanza el uso por encima del límite para esta cuota, no se podrán habilitar direcciones IP públicas para más servidores. Desmarque la casilla de verificación **Dirección IP pública** de la configuración del servidor para hacer que no pueda usar ninguna IP pública. Después, puede permitir que otro servidor use una dirección IP pública, que normalmente no será la misma.

  Cuando la cuota se deshabilita, todos los servidores dejan de usar direcciones IP públicas y, por tanto, no se puede acceder a ellos desde Internet.
- **Servidores en la nube**

  Esta cuota limita el número total de servidores primarios y de recuperación. Si se alcanza el uso por encima del límite para esta cuota, no se podrán crear servidores principales ni de recuperación.

  Cuando se deshabilita la cuota, los servidores se pueden ver en la consola de Cyber Protect, pero la única operación disponible es **Eliminar**.
- **Acceso a Internet**

  Esta cuota habilita o deshabilita el acceso a Internet desde servidores principales y de recuperación.

  Cuando la cuota está deshabilitada, los servidores principales y de recuperación no pueden establecer conexión a Internet.

Cuotas de File Sync & Share

Estas cuotas las aplica el proveedor de servicios a toda la empresa. Los administradores de la empresa pueden ver las cuotas y el uso en el portal de gestión.

- **Usuarios**
  La cuota define el número de usuarios que pueden acceder a este servicio.
  Las cuentas de administrador no se incluyen como parte de esta cuota.
- **Almacenamiento en la nube**
  Se trata de un almacenamiento en la nube que permite guardar los archivos de los usuarios. La cuota define el espacio asignado a un inquilino en el almacenamiento en la nube.

Cuotas de envío de datos físicos

Las cuotas del servicio de envío de datos físicos se consumen por unidad. Puede guardar copias de seguridad iniciales de múltiples equipos en una unidad de disco rígido.

Estas cuotas las aplica el proveedor de servicios a toda la empresa. Los administradores de la empresa pueden ver las cuotas y el uso en el portal de gestión, pero no pueden establecer cuotas para un usuario.

- **En la nube**
  Permite enviar una copia de seguridad inicial al centro de datos en el cloud con una unidad de disco rígido. Esta cuota define el número máximo de unidades que se pueden transferir al centro de datos en la nube.

Cuotas de certificación

Estas cuotas las aplica el proveedor de servicios a toda la empresa. Los administradores de la empresa pueden ver las cuotas y el uso en el portal de gestión.

- **Almacenamiento de Notary**
  Define el espacio máximo de almacenamiento en la nube para los archivos certificados ante notario, los firmados y aquellos cuya certificación o firma está en progreso.
  Para reducir el uso de esta cuota, puede eliminar los archivos ya certificados ante notario o firmados del almacenamiento de Notary.
- **Notarizaciones**
  Define el número máximo de archivos que se pueden certificar ante notario con el servicio de certificación.
  Un archivo se considera certificado ante notario en el momento en el que se carga al almacenamiento de Notary y su estado de certificación cambia a **En progreso**.
  Si el mismo archivo se certifica varias veces, cada certificación cuenta como una nueva.
- **Firmas electrónicas**
  Define el número máximo de firmas electrónicas digitales.

Definición de cuotas para sus usuarios

Las **cuotas** le permiten limitar la capacidad de los usuarios de utilizar el servicio. Para establecer las cuotas para un usuario, selecciónelo en la pestaña **Usuarios** de **Gestión empresarial** y haga clic en el icono del lápiz en la sección **Cuotas**.

Cuando se supera una cuota, se envía una notificación a la dirección de correo electrónico del usuario. Si no establece un uso por encima del límite de cuota, la cuota se considera "**flexible**". Esto significa que no se aplican restricciones para usar el servicio de Cyber Protection.

Al especificar el uso por encima del límite de cuota, esta se considera "**rígida**". Un **uso por encima del límite** permite al usuario sobrepasar la cuota en un valor especificado. Si el uso por encima del límite se sobrepasa, se aplican las restricciones sobre el uso del servicio.

Ejemplo

Cuota flexible: Ha establecido el valor 20 para la cuota de estaciones de trabajo. Cuando el usuario llegue a 20 estaciones de trabajo protegidas, se le enviará una notificación por correo electrónico, pero el servicio Cyber Protection seguirá estando disponible.

Cuota rígida: Si ha establecido la cuota de estaciones de trabajo en 20 y el exceso admitido es de 5, el usuario recibirá la notificación por correo electrónico cuando llegue a 20 estaciones de trabajo protegidas, y el servicio Cyber Protection se deshabilitará cuando alcance las 25.

Cuotas de Backup

Puede especificar la cuota de almacenamiento de copia de seguridad y el número de equipos, dispositivos o sitios web que un usuario puede proteger. Están disponibles las siguientes cuotas.

Cuota de dispositivos

- **Estaciones de trabajo**
- **Servidores**
- **Equipos virtuales**
- **Dispositivos móviles**
- **Servidores de alojamiento web** (servidores físicos y virtuales basados en Linux que ejecuten paneles de control Plesk, cPanel, DirectAdmin, VirtualMin o ISPManager)
- **Sitios web**

Se considera que un equipo, un dispositivo o un sitio web están protegidos si se les aplica, como mínimo, un plan de protección. Un dispositivo móvil se considera protegido después de la primera copia de seguridad.

Cuando se supera el límite de exceso de dispositivos, el usuario no puede aplicar un plan de protección a más dispositivos.

Cuota de almacenamiento

- **Almacenamiento de copias de seguridad**

La cuota de almacenamiento de copias de seguridad limita el tamaño total de las copias de seguridad que se encuentran en el almacenamiento en el cloud. Si se supera la cuota de almacenamiento de copias de seguridad, estas no se realizan.

Importante
El agente local y el agente de la nube consumen cuotas independientes. Si lleva a cabo la copia de seguridad de las mismas cargas de trabajo con ambos agentes, se le cobrará dos veces. Por ejemplo:

- Si lleva a cabo la copia de seguridad de los buzones de correo de 120 usuarios con el agente local y la copia de seguridad de los archivos de OneDrive de los mismos usuarios con el agente de la nube, se le cobrarán 240 licencias de Microsoft 365.
- Si lleva a cabo la copia de seguridad de los buzones de correo de 120 usuarios con el agente local y la copia de seguridad de los mismos buzones de correo con el agente de la nube, se le cobrarán 240 licencias de Microsoft 365.

Cuotas de File Sync & Share

Puede definir las siguientes cuotas de File Sync & Share para un usuario:

- **Espacio de almacenamiento personal**
  Define el espacio de almacenamiento en la nube asignado a los archivos de un usuario.

Cuotas de certificación

Puede definir las siguientes cuotas de certificación para un usuario:

- **Almacenamiento de Notary**
  Define el espacio máximo de almacenamiento en la nube para los archivos certificados ante notario, los firmados y aquellos cuya certificación o firma está en progreso.
  Para reducir el uso de esta cuota, puede eliminar los archivos ya certificados ante notario o firmados del almacenamiento de Notary.
- **Notarizaciones**
  Define el número máximo de archivos que se pueden certificar ante notario con el servicio de certificación.
  Un archivo se considera certificado ante notario en el momento en el que se carga al almacenamiento de Notary y su estado de certificación cambia a **En progreso**.
  Si el mismo archivo se certifica varias veces, cada certificación cuenta como una nueva.
- **Firmas electrónicas**
  Define el número máximo de firmas electrónicas digitales.

Navegadores web compatibles

La interfaz web es compatible con los siguientes navegadores web:

- Google Chrome 29 o posterior
- Mozilla Firefox 23 o posterior
- Opera 16 o posterior
- Microsoft Edge 25 o posterior
- Safari 8 o una versión posterior que se ejecute en los sistemas operativos macOS y iOS

En otros navegadores web (incluido Safari para otros sistemas operativos), es posible que la interfaz de usuario no se muestre correctamente o que algunas funciones no estén disponibles.

Instrucciones paso a paso

Los siguientes pasos lo guiarán a través del uso básico del portal de gestión. Describen cómo:

- Activar su cuenta de administrador
- Acceso al portal de gestión y a los servicios
- Crear una unidad
- Crear una cuenta de usuario

Activar una cuenta de administrador

Una vez que se asocie con un servicio, recibirá un mensaje por correo electrónico con la siguiente información:

- **Sus credenciales de inicio de sesión.** Este es el nombre de usuario que utiliza para iniciar sesión. Sus credenciales de inicio de sesión aparecen también en la página de activación de la cuenta.
- Botón **Activar cuenta**. Haga clic en el botón y establezca la contraseña de su cuenta. Asegúrese de que la contraseña tenga al menos nueve caracteres. Para obtener más información sobre la contraseña, consulte "Requisitos de contraseña" (p. 17).

Requisitos de contraseña

La contraseña de las cuentas de usuario debe tener una longitud de al menos 9 caracteres. También se comprueba la complejidad de las contraseñas, que entran dentro de una de las siguientes categorías:

- Débil
- Medio
- Fuerte

No puede guardar una contraseña débil, incluso aunque contenga 9 caracteres o más. Las contraseñas que repiten el nombre de usuario, el inicio de sesión, el correo electrónico del usuario o el nombre del inquilino al que pertenece la cuenta de usuario siempre se consideran débiles. Las contraseñas más comunes también se consideran débiles.

Para reforzar una contraseña, añada más caracteres. No es obligatorio utilizar diferentes tipos de caracteres, como números, mayúsculas y minúsculas y caracteres especiales, pero se obtienen contraseñas más fuertes y más cortas.

Acceso al portal de gestión y a los servicios

1. Vaya a la página de inicio de la consola de servicio.
2. Escriba el usuario y haga clic en **Siguiente**.

3. Escriba la contraseña y haga clic en **Siguiente**.
4. Realice uno de los siguientes procedimientos:
   - Para iniciar sesión en el portal de gestión, haga clic en el **Portal de gestión**.
   - Para iniciar sesión en un servicio, haga clic en el nombre del servicio.

El tiempo de espera para el portal de administración es de 24 horas en las sesiones activas y de 1 hora en las inactivas.

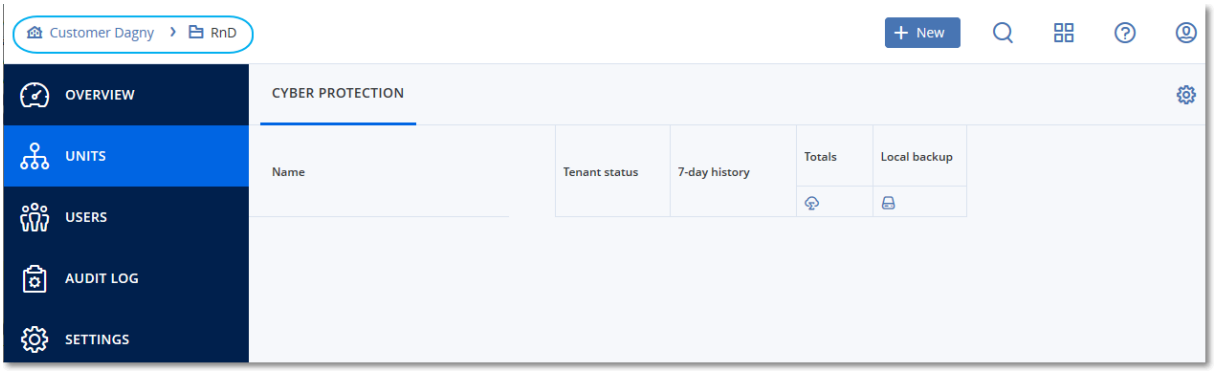
Cambiar del portal de administración a las consolas de servicio y viceversa

Para cambiar del portal de administración a las consolas de servicio, y viceversa, haga clic en el icono que se encuentra en la esquina superior derecha y seleccione **Portal de gestión** o el servicio al que quiera acceder.

Navegación en el portal de gestión

Cuando se utiliza el portal de gestión, en un momento dado está operando en una compañía o en una unidad. Esto se indica en la esquina superior izquierda.

De forma predeterminada, aparece seleccionado el máximo nivel de jerarquía disponible para usted. Haga clic en el nombre de la unidad para profundizar en la jerarquía. Para volver a un nivel superior, haga clic en su nombre en la esquina superior izquierda.



Todas las partes de la interfaz de usuario solo muestran y afectan a la compañía o a una unidad en la que está operando actualmente. Por ejemplo:

- Usando el botón **Nuevo** puede crear una unidad o una cuenta de usuario únicamente en esta compañía o unidad.
- La pestaña **Unidades** solo muestra las unidades que son secundarias directas de esta compañía o unidad.
- La pestaña **Usuarios** solo muestra las cuentas de usuario que existen en esta compañía o unidad.

Creación de una unidad

Omita este paso si no desea organizar cuentas de usuario en unidades.

Si está pensando en crear unidades más adelante, no olvide que las cuentas existentes no se pueden mover entre unidades o entre la compañía y unidades. Primero, necesita crear una unidad y luego introducir cuentas.

Para crear una unidad

1. Inicie sesión en el portal de gestión.
2. Vaya hasta la unidad en la que desee crear una unidad nueva.
3. En la esquina superior derecha, haga clic en **Nuevo** > **Unidad**.
4. En **Nombre**, especifique un nombre para la nueva unidad.
5. [Opcional] En **Idioma**, cambie el idioma predeterminado de las notificaciones, los informes y el software que se usarán para esta unidad.
6. Realice uno de los siguientes procedimientos:
   - Para crear un administrador de unidades, haga clic en **Siguiente** y, a continuación, siga los pasos descritos en "Creación de una cuenta de usuario". Empiece desde el paso 4.
   - Para crear una unidad sin un administrador, haga clic en **Guardar y cerrar**. Puede añadir administradores y usuarios a la unidad más tarde.

La unidad creada recientemente aparece en la pestaña **Unidades**.

Si desea modificar la configuración de la unidad o especificar la información de contacto, seleccione la unidad en la pestaña **Unidades** y luego haga clic en el icono de lápiz en la sección que desea modificar.

Creación de una cuenta de usuario

Omita este paso si no desea crear cuentas de usuario adicionales.

Es posible que desee crear cuentas adicionales en los siguientes casos:

- Cuentas de administrador de empresa: para compartir las funciones de gestión con otras personas.
- Cuentas de administrador de unidad: para delegar la gestión en otras personas cuyos permisos de acceso estarán limitados a las unidades correspondientes.
- Cuentas de usuario: para permitir que los usuarios solo puedan acceder a un subconjunto de servicios.

Para crear una cuenta de usuario

1. Inicie sesión en el portal de gestión.
2. Vaya hasta la unidad en la que desee crear una cuenta de usuario nueva.

3. En la esquina superior derecha, haga clic en **Nuevo** > **Usuario**.
4. Especifique la siguiente información para la cuenta:
   - **Usuario**

     Importante
     Debe haber únicamente un usuario en cada cuenta.

   - **Correo electrónico**

     Importante
     Si el usuario está registrado en el servicio de File Sync & Share, facilite el correo electrónico que se utilizó para el registro de File Sync & Share.
     Tenga en cuenta que cada cuenta de usuario de cliente debe tener una dirección de correo electrónico única.

   - [Opcional] **Nombre**
   - [Opcional] **Apellido**
   - En **Idioma**, cambie el idioma predeterminado de las notificaciones, los informes y el software de esta cuenta.
5. Seleccione los servicios a los que tendrá acceso el usuario y las funciones en cada servicio.
   - Si selecciona la opción **Administrador de la compañía**, el usuario tendrá acceso al portal de gestión y a la función de administrador en todos los servicios.
   - Si marca la casilla de verificación **Administrador de unidad**, el usuario tendrá acceso al portal de gestión, pero que tenga la función de administrador del servicio dependerá del servicio.
   - De lo contrario, el usuario tendrá las funciones seleccionadas en los servicios que seleccione.
6. Haga clic en **Crear**.

La cuenta de usuario creada recientemente aparece en la pestaña **Usuarios**.

Si desea modificar la configuración del usuario o especificar parámetros de notificación o cuotas para el usuario, seleccione al usuario en la pestaña **Usuarios** y luego haga clic en el icono de lápiz de la sección que desea modificar.

Pasos para restablecer la contraseña de un usuario

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. Seleccione el usuario cuya contraseña desee restablecer y, a continuación, haga clic en el icono > **Restablecer contraseña**.
3. Haga clic en **Restablecer** para confirmar la acción.

En este momento el usuario puede completar el proceso de restablecimiento si sigue las instrucciones incluidas en el correo electrónico que ha recibido.

En el caso de los servicios que no son compatibles con la autenticación de doble factor (por ejemplo, el registro en Cyber Infrastructure) es posible que deba convertir una cuenta de usuario en una *Cuenta de servicio*, la cual no requiere la autenticación de doble factor.

Pasos para convertir una cuenta de usuario al tipo de cuenta de servicio

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. Seleccione el usuario cuya cuenta desee convertir al tipo de cuenta de servicio y, a continuación, haga clic en el icono de los tres puntos > **Marcar como cuenta de servicio**.
3. En la ventana de confirmación, introduzca el código de autenticación de doble factor y confirme su acción.

Ahora la cuenta puede utilizarse para servicios que no son compatibles con la autenticación de doble factor.

Funciones de usuario disponibles para cada servicio

Un usuario puede tener varias funciones, pero solo una por servicio.

Para cada servicio, puede definir qué función se asignará a un usuario.

Servicio	Rol	Descripción
n/d	Administrador de la compañía	Este rol concede todos los derechos de administrador de todos los servicios. Este rol concede acceso a la lista blanca corporativa. Si la característica Recuperación ante desastres del servicio Protección está activada para la empresa, este rol también permite acceder a la funcionalidad de recuperación ante desastres.
Portal de gestión	Administrador	Este rol concede acceso al portal de gestión, donde el administrador puede gestionar a los usuarios dentro de toda la organización. Por ejemplo, este rol otorga permisos completos para los análisis de Endpoint Detection and Response, incluidos los widgets.
	Administrador de solo lectura Nivel de partner	Este rol proporciona acceso de solo lectura a todos los objetos en el portal de administración del partner y los portales de administración de todos los clientes de este partner. Dichos usuarios pueden acceder a los datos de otros usuarios de la organización en modo de solo lectura. Son capaces de editar planes de protección, pero no pueden guardar ningún cambio en los planes de scripting, planes de supervisión o planes de agente.

	Administrador de solo lectura Nivel de cliente	Esta función proporciona acceso de solo lectura a todos los objetos del portal de administración de toda la empresa. Estos usuarios pueden acceder a los datos de otros usuarios de la organización en modo de solo lectura.
	Administrador de solo lectura Nivel de unidad	Esta función proporciona acceso de solo lectura a todos los objetos del portal de administración de la unidad y subunidades de la empresa. Estos usuarios pueden acceder a los datos de otros usuarios de la organización en modo de solo lectura.
Protección	Administrador de cibernética	Además de los derechos del rol de administrador, este rol permite configurar y gestionar el servicio de Cyber Protection, así como aprobar acciones en Programación cibernética. El rol de administrador de cibernética solo está disponible para los inquilinos con el paquete de Advanced Management habilitado.
	Administrador	Este rol permite configurar y gestionar Protección para sus clientes. Por ejemplo, el rol es necesario para configurar y gestionar la funcionalidad de Recuperación ante desastres, Endpoint Detection and Response y la lista de permitidos corporativa.
	Administrador de solo lectura	La función proporciona acceso de solo lectura a todos los objetos del servicio Protección. Estos usuarios pueden acceder a los datos de otros usuarios de la organización en modo de solo lectura. El administrador de solo lectura no puede configurar ni gestionar la funcionalidad de Recuperación ante desastres, Endpoint Detection and Response ni la lista de permitidos corporativa.
	Restaurar operador	El rol proporciona acceso a las copias de seguridad de las organizaciones de Microsoft 365 y Google Workspace y permite su recuperación, al mismo tiempo que restringe el acceso a contenido confidencial.
	Usuario	Esta función permite el uso del servicio Protección, pero sin privilegios administrativos. Se otorga acceso a las funcionalidades como Endpoint Detection and Response, pero los usuarios asignados a este rol no pueden acceder a los datos de otros usuarios de la organización.
File Sync & Share	Administrador	Este rol permite configurar y gestionar File Sync & Share para sus usuarios. Las cuentas con este rol no se

		consideran parte de la cuota de **Usuarios** porque no otorgan acceso a la funcionalidad de File Sync & Share.
	Usuario	Esta función permite el uso del servicio de File Sync & Share. Los usuarios solo pueden acceder a sus datos y a los que se comparten con ellos.
	Invitado	Se crea una cuenta con este rol cuando un usuario de File Sync & Share comparte contenido con un usuario de Cyber Protect Cloud que no puede utilizar el servicio de File Sync & Share o con una persona que no es un usuario de Cyber Protect Cloud. Los roles de invitado no tienen ninguna carpeta de sincronización, no consumen almacenamiento de la nube y no se consideran parte de la cuota de **Usuarios** porque no otorgan acceso a la funcionalidad de File Sync & Share. Se puede promocionar a un invitado a la función de Usuario o administrador.
Notary	Administrador	Esta función permite configurar y gestionar Notary para sus usuarios.
	Usuario	Esta función permite el uso del servicio Notary, pero sin privilegios administrativos. Estos usuarios no pueden acceder a los datos de otros usuarios de la organización.

Función de administrador de solo lectura

Una cuenta con este rol tiene acceso de solo lectura a la consola de Cyber Protect y puede hacer lo siguiente:

- Recopilar datos de diagnóstico, como informes del sistema.
- Ver todos los puntos de recuperación de una copia de seguridad, pero no profundizar en los contenidos de esta ni ver archivos, carpetas ni correos electrónicos.

Un administrador de solo lectura no puede hacer lo siguiente:

- Iniciar o detener ninguna tarea.

  Por ejemplo, un administrador de solo lectura no puede iniciar una recuperación o detener una copia de seguridad que esté en curso.
- Acceder al sistema de archivos en equipos de origen o de destino.

  Por ejemplo, un administrador de solo lectura no puede ver archivos, carpetas ni correos electrónicos en un equipo del que se ha realizado una copia de seguridad.
- Cambiar ninguna configuración.

  Por ejemplo, un administrador de solo lectura no puede crear un plan de protección ni cambiar ninguna de sus configuraciones.

- Crear, actualizar o eliminar ningún tipo de datos.
  Por ejemplo, un administrador de solo lectura no puede borrar copias de seguridad.

  Todos los objetos de la interfaz de usuario que no son accesibles para un administrador de solo lectura están ocultos, excepto en el caso de la configuración predeterminada del plan de protección. Esta configuración sí se muestra, pero el botón **Guardar** no está activo.

  Todos los cambios relacionados con las cuentas y los roles se muestran en la pestaña **Actividades** con la siguiente información:

  - Qué es lo que ha cambiado
  - Quién realizó cada cambio
  - La fecha y hora de los cambios

Rol de operador de restauración

Este rol solo está disponible en el servicio Cyber Protection y está limitado a copias de seguridad de Microsoft 365 y Google Workspace.

Un operador de restauración puede:

- Ver alertas y actividades.
- Examinar y actualizar la lista de copias de seguridad.
- Examinar copias de seguridad sin acceder al contenido. El operador de restauración puede ver los nombres de los archivos de la copia de seguridad y el asunto y los emisores de los correos electrónicos con copia de seguridad.
- Buscar copias de seguridad (la búsqueda de texto completo no es compatible).
- Recuperar copias de seguridad de la nube a la nube a la ubicación original dentro de la organización original de Microsoft 365 o Google Workspace.

Un operador de restauración no puede:

- Eliminar alertas.
- Añadir o eliminar organizaciones de Microsoft 365 o Google Workspace.
- Añadir, eliminar o cambiar el nombre de las ubicaciones de las copias seguridad.
- Eliminar o cambiar el nombre de las copias de seguridad.
- Crear, eliminar o cambiar el nombre de carpetas al recuperar una copia de seguridad a una ubicación personalizada.
- Aplicar un plan de copias de seguridad o ejecutar una copia de seguridad.
- Acceder a los archivos de la copia de seguridad o al contenido de los correos electrónicos con copia de seguridad.
- Descargar archivos de la copia de seguridad o adjuntos de correos electrónicos.
- Enviar recursos en la nube con copia de seguridad, como correos electrónicos o elementos del calendario, mediante correo electrónico.

- Ver o recuperar conversaciones de Microsoft 365 Teams.
- Recuperar copias de seguridad de la nube a la nube a ubicaciones que no sean originales, como un buzón de correo diferente, OneDrive, Google Drive, o Microsoft 365 Team.

Cambiar los ajustes de notificaciones para un usuario

Para cambiar los ajustes de notificaciones para un usuario, vaya a **Gestión empresarial** > **Usuarios**. Seleccione el usuario para el que desee configurar las notificaciones y haga clic en el icono del lápiz en la sección **Configuración**. Están disponibles los siguientes ajustes de notificaciones si el servicio Cyber Protection está habilitado para el inquilino en el que se creó el usuario:

- **Notificaciones de uso excesivo de las cuotas** (habilitado de forma predeterminada)
  Notificaciones sobre cuotas superadas.
- **Informes de uso planificados** (habilitado de forma predeterminada)
  Informes de uso que se envían el primer día de cada mes.
- **Notificaciones de adaptación de marca de URL** (opción deshabilitada de manera predeterminada)
  Notificaciones acerca del próximo vencimiento del certificado utilizado para la URL personalizada de los servicios de Cyber Protect Cloud. Se envían notificaciones a todos los administradores del inquilino seleccionado: 30 días, 15 días, 7 días, 3 días y 1 día antes de que venza el certificado.
- **Notificaciones de error**, **Notificaciones de advertencia** y **Notificaciones de acciones realizadas correctamente** (deshabilitado de forma predeterminada)
  Notificaciones relacionadas con los resultados de la ejecución de planes de protección y con los resultados de las operaciones de recuperación ante desastres de cada dispositivo.
- **Resumen diario de alertas activas** (habilitado de forma predeterminada)
  El resumen diario se genera a partir de la lista de alertas activas presentes en la consola de Cyber Protect en el momento de la generación. El resumen se genera y envía una vez al día, entre las 10:00 y las 23:59 UTC. La hora a la que se genera y envía el informe depende de la carga de trabajo del centro de datos. Si no hay alertas activas en ese momento, no se envía el resumen. El resumen no incluye información sobre alertas pasadas que ya no estén activas. Por ejemplo, si un usuario encuentra una copia de seguridad fallida y anula la alerta, o si la copia de seguridad se vuelve a intentar y se completa correctamente antes de generarse el resumen, la alerta ya no estará presente y el resumen no la incluirá.
- **Notificaciones de control de dispositivos** (deshabilitadas de manera predeterminada)
  Notificaciones de los intentos de utilizar dispositivos periféricos y puertos limitados por planes de protección con el módulo de control de dispositivos habilitado.
- **Notificaciones de recuperación** (opción deshabilitada de manera predeterminada)
  Notificaciones sobre las acciones de recuperación en los siguientes recursos: mensajes de correo electrónico del usuario y buzón de correo completo, carpetas públicas; OneDrive/Google Drive: archivos o carpetas completos de OneDrive, archivos de SharePoint; Teams: Canales, todo Teams, mensajes de correo electrónico y sitio de Teams.

En el contexto de estas notificaciones, se consideran acciones de recuperación las siguientes: enviar un correo electrónico, descargar o iniciar una operación de recuperación.

- **Notificaciones de prevención de pérdida de datos** (opción deshabilitada de manera predeterminada)
  Notificaciones sobre las alertas de prevención de la pérdida de datos relacionadas con la actividad de este usuario en la red.
- **Notificaciones de incidentes de seguridad** (opción deshabilitada de manera predeterminada)
  Notificaciones de malware detectado durante exploraciones en acceso, en ejecución y bajo demanda y de detecciones desde los motores de comportamiento y de filtrado de URL.
  Hay dos opciones disponibles: **Mitigado** y **No mitigado**. Estas opciones son relevantes para las alertas de incidentes de Endpoint Detection and Response (EDR), las alertas EDR de fuente de amenazas y las alertas individuales (para las cargas de trabajo que no tienen activada la EDR).
  Cuando se crea una alerta EDR, se envía un correo electrónico al usuario correspondiente. Si el estado de la amenaza del incidente cambia, se envía un nuevo correo electrónico. Los correos electrónicos incluyen botones de acción que permiten al usuario ver detalles del incidente (si se ha mitigado) o investigar y solucionar el incidente (si no se ha mitigado).
- **Notificaciones de infraestructura** (deshabilitadas de forma predeterminada)
  Notificaciones sobre problemas con la infraestructura de la recuperación ante desastres: cuando la infraestructura de la recuperación ante desastres o los túneles VPN no están disponibles.

Todas las notificaciones se envían a la dirección de correo electrónico del usuario.

Notificaciones recibidas por cada función de usuario

Las notificaciones que Cyber Protection envía dependen de la función de usuario.

Tipo de notificación/función de usuario	Usuario	Administrador de clientes
Notificaciones de los dispositivos propios	Sí	Sí
Notificaciones de todos los dispositivos de la organización	n/d	Sí (excepto **Notificaciones de incidentes de seguridad**)
Notificaciones de Microsoft 365, Google Workspace y otras copias de seguridad basadas en la nube	n/d	Sí

Deshabilitación y habilitación de una cuenta de usuario

Es posible que tenga que deshabilitar una cuenta de usuario para restringir temporalmente su acceso a la plataforma en la nube.

Pasos para deshabilitar una cuenta de usuario

1. En el portal de administración, vaya a **Usuarios**.
2. Seleccione la cuenta de usuario que desee deshabilitar y, a continuación, haga clic en el icono

 > **Deshabilitar**.

3. Haga clic en **Deshabilitar** para confirmar la acción.

Como resultado, este usuario no podrá usar la plataforma en la nube ni recibir ninguna notificación.

Para habilitar una cuenta de usuario deshabilitada, selecciónela de la lista de usuarios y, a continuación, haga clic en el icono > **Habilitar**.

Eliminación de una cuenta de usuario

Es posible que tenga que eliminar una cuenta de usuario permanentemente para liberar los recursos que usa, como espacio de almacenamiento o licencia. Las estadísticas de uso se actualizarán en el plazo de un día después de la eliminación. En cuentas con muchos datos, es posible que tarde más.

Antes de eliminar una cuenta de usuario, tiene que deshabilitarla. Para obtener más información sobre cómo hacerlo, consulte: Deshabilitación y habilitación de una cuenta de usuario.

Pasos para eliminar una cuenta de usuario

1. En el portal de administración, vaya a **Usuarios**.
2. Seleccione la cuenta de usuario deshabilitada y, a continuación, haga clic en el icono de puntos suspensivos  > **Eliminar**.
3. Para confirmar su acción, introduzca su información de inicio de sesión y luego haga clic en **Eliminar**.

Como resultado:

- Se deshabilitarán todas las notificaciones configuradas para esta cuenta.
- Se eliminarán todos los datos que pertenecen a esta cuenta de usuario.
- El administrador no podrá acceder al portal de administración.
- Se eliminarán todas las copias de seguridad de las cargas de trabajo asociadas a este usuario.
- Se eliminará el registro de todos los equipos asociados a esta cuenta de usuario.
- Se revocarán todos los planes de protección de todas las cargas de trabajo asociadas a este usuario.
- Se eliminarán todos los datos de File Sync & Share que pertenezcan a este usuario (por ejemplo, archivos y carpetas).
- Se eliminarán todos los datos de Notary que pertenezcan a este usuario (por ejemplo, los archivos certificados y los firmados electrónicamente).
- El **Estado** del usuario será **Eliminado**. Cuando pase el ratón sobre el estado **Eliminado**, verá la fecha en la que se eliminó el usuario. Tenga en cuenta que aún puede recuperar todos los datos relevantes y la configuración en un plazo de 30 días desde la fecha de eliminación.

Transferencia de la propiedad de una cuenta de usuario

Es posible que tenga que transferir la propiedad de una cuenta de usuario si quiere conservar el acceso a los datos de un usuario restringido.

Importante
No se puede reasignar el contenido de una cuenta eliminada.

Pasos para transferir la propiedad de una cuenta de usuario:

1. En el portal de administración, vaya a **Usuarios**.
2. Seleccione la cuenta de usuario cuya propiedad quiera transferir y, a continuación, haga clic en el icono del lápiz de la sección **información general**.
3. Sustituya el correo electrónico existente por el del futuro propietario de la cuenta y luego haga clic en **Listo**.
4. Haga clic en **Sí** para confirmar la acción.
5. Deje que el futuro propietario de la cuenta compruebe su dirección de correo electrónico siguiendo las instrucciones que se le han enviado por esa vía.
6. Seleccione la cuenta de usuario cuya propiedad está transfiriendo y luego haga clic en el icono > **Restablecer contraseña**.
7. Haga clic en **Restablecer** para confirmar la acción.
8. Deje que el futuro propietario de la cuenta restablezca la contraseña siguiendo las instrucciones que se le han enviado a su dirección de correo electrónico.

Ahora el nuevo usuario puede acceder a esta cuenta.

Establecimiento de la autenticación de doble factor

La **Autenticación de doble factor** es un tipo de autenticación de varios factores que comprueba la identidad de un usuario mediante la combinación de dos factores distintos:

- Algo que un usuario conoce (PIN o contraseña).
- Algo que un usuario posee (token).
- Algo que un usuario es (biometría).

La autenticación de doble factor proporciona protección adicional contra el acceso no autorizado a su cuenta.

La plataforma es compatible con la autenticación por **Contraseña de un solo uso y duración definida (TOTP)**. Si se activa la autenticación TOTP en el sistema, los usuarios deben introducir su contraseña habitual y el código TOTP de un solo uso para acceder al sistema. Dicho de otro modo, el usuario introduce la contraseña (el primer factor) y el código TOTP (el segundo factor). El código

TOTP se genera en la aplicación de autenticación del dispositivo de segundo factor del usuario, basándose en la hora actual y el código secreto (QR o alfanumérico) que proporciona la plataforma.

Cómo funciona

1. Puede habilitar la autenticación de doble factor a nivel de su organización.
2. Todos los usuarios de su organización deben instalar una aplicación de autenticación en sus dispositivos de segundo factor (teléfonos móviles, equipos portátiles, de sobremesa o tabletas). Dicha aplicación se utilizará para generar códigos TOTP de un solo uso. Aplicaciones de autenticación recomendadas:
   - Google Authenticator

     Versión de la aplicación de iOS (https://apps.apple.com/app/google-authenticator/id388497605)

     Versión de Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator

     Versión de la aplicación de iOS (https://apps.apple.com/app/microsoft-authenticator/id983156458)

     Versión de Android (https://play.google.com/store/apps/details?id=com.azure.authenticator)

   Importante
   Los usuarios deben establecer correctamente la hora en el dispositivo en el que instalen la aplicación de autenticación, de forma que refleje la hora actual.
3. Los usuarios de su organización deben volver a iniciar sesión en el sistema.
4. Tras introducir la información de inicio de sesión y la contraseña, se les solicitará que establezcan la autenticación de doble factor para su cuenta de usuario.
5. Deben escanear el código QR con su aplicación de autenticación. Si no pueden escanear el código QR, pueden usar el código de 32 dígitos que aparece bajo el código QR y agregarlo manualmente en la aplicación de autenticación.

   Importante
   Se recomienda guardarlo (imprimir el código QR, escribir la contraseña temporal de un solo uso (TOTP) o usar una aplicación compatible con la creación de copias de seguridad de códigos de la nube). Necesitará la contraseña temporal de un solo uso (TOTP) para restablecer la autenticación de doble factor en caso de perder el dispositivo de segundo factor.
6. El código de contraseña temporal de un solo uso (TOTP) se generará en la aplicación de autenticación. Se regenera automáticamente cada 30 segundos.
7. Los usuarios deben introducir el código TOTP en la ventana **Establecer autenticación de doble factor** después de introducir la contraseña.
8. Como resultado, se establecerá la autenticación de doble factor para los usuarios.

Cuando los usuarios inicien sesión en el sistema, se les solicitará la información de inicio de sesión, la contraseña y el código TOTP de un solo uso generado en la aplicación de autenticación. Al iniciar sesión en el sistema, los usuarios pueden establecer que su navegador es de confianza y no se les volverá a solicitar el código TOTP las próximas veces que inicien sesión en dicho navegador.

Pasos para restaurar la autenticación de doble factor en un nuevo dispositivo

Si tiene acceso a la app de autenticación para entorno móvil instalada previamente:

1. Instale un app de autenticación en su nuevo dispositivo.
2. Utilice el archivo PDF que ha guardado al instalar la autenticación de doble factor (2FA) en el dispositivo. El archivo contiene el código de 32 dígitos que debe introducir en la app de autenticación para enlazar de nuevo la app de autenticación con su cuenta de Acronis.

   Importante
   Si el código es correcto, pero no funciona, asegúrese de sincronizar la hora en la app de autenticación para entorno móvil.

3. Si ha olvidado guardar el archivo PDF durante la instalación:

a. *Haga clic en **Restablecer autenticación de doble factor (2FA)** e introduzca la contraseña de un solo uso mostrada en la app de autenticación para entorno móvil instalada previamente.*
b. Siga las instrucciones que aparecen en pantalla.

Si no tiene acceso a la app de autenticación para entorno móvil instalada previamente:

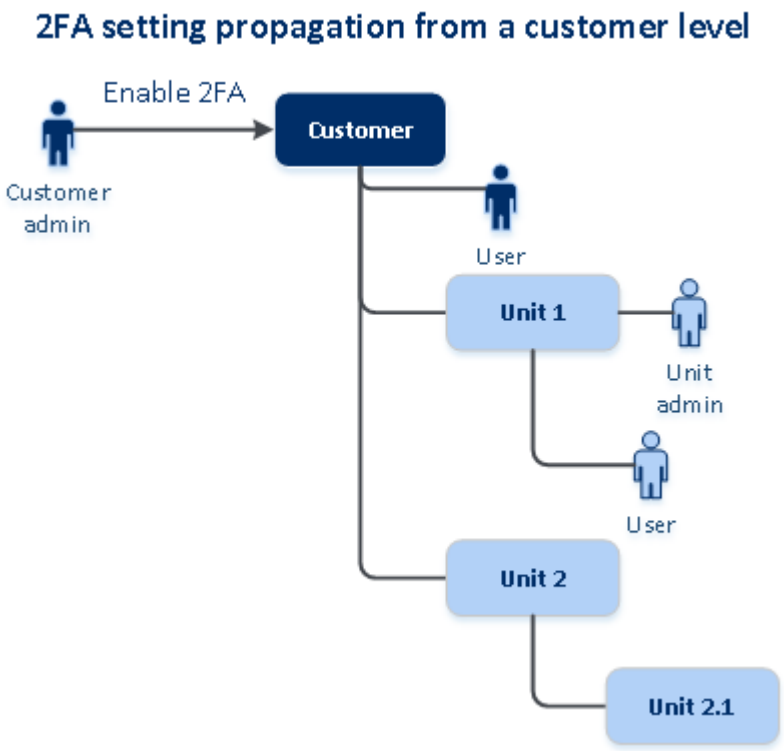
1. Utilice un nuevo dispositivo móvil.
2. Utilice el archivo PDF almacenado para enlazar un nuevo dispositivo (el nombre predeterminado del archivo es `cyberprotect-2fa-backupcode.pdf`).
3. Restaure el acceso a su cuenta desde la copia de seguridad. Asegúrese de que las copias de seguridad son compatibles con su app para entorno móvil.
4. Abra la app en la misma cuenta desde otro dispositivo móvil si es compatible con la app.

Propagación de la configuración de doble factor en niveles de inquilino

La autenticación de doble factor se establece en el nivel de **organización**. Puede establecer la autenticación de doble factor solo para su propia organización.

La configuración de la autenticación de doble factor se propaga a los niveles de inquilino de la siguiente manera:

- Las unidades heredan automáticamente la configuración de autenticación de doble factor de la organización de sus clientes.



Nota

1. No es posible establecer la autenticación de doble factor en el nivel de unidad.
2. Puede gestionar la autenticación de doble factor de los usuarios de las organizaciones secundarias (unidades).

Establecimiento de la autenticación de doble factor para el inquilino

Como administrador, puede habilitar la autenticación de doble factor para la organización.

Para habilitar la autenticación de doble factor para el inquilino:

1. En el portal de gestión, vaya a **Configuración** > **Seguridad**.
2. Active el control deslizante **Autenticación de doble factor** y haga clic en **Habilitar**.

Ahora todos los usuarios de la organización deben establecer la autenticación de doble factor en sus cuentas. Se les solicitará que lo hagan la próxima vez que intenten iniciar sesión o cuando sus sesiones actuales caduquen.

La barra de progreso bajo el control deslizante muestra cuántos usuarios han establecido la autenticación de doble factor para sus cuentas. Para comprobar que los usuarios hayan configurado sus cuentas, acceda a la pestaña **Gestión empresarial** > **Usuarios** y consulte la columna **Estado de la autenticación de doble factor**. El estado de 2FA de los usuarios que no hayan configurado la autenticación de doble factor en la cuenta será **Configuración requerida**.

Tras configurar correctamente la autenticación de doble factor, los usuarios deberán introducir su nombre de usuario, contraseña y un código TOTP cada vez que inicien sesión en la consola de servicio.

Para deshabilitar la autenticación de doble factor para el inquilino:

1. En el portal de gestión, vaya a **Configuración** > **Seguridad**.
2. Para deshabilitar la autenticación de doble factor, desactive el control deslizante y haga clic en **Deshabilitar**.
3. [Si al menos un usuario ha configurado la autenticación de doble factor dentro de la organización] Introduzca el código TOTP generado en su aplicación de autenticación del dispositivo móvil.

Como resultado, se deshabilita la autenticación de doble factor en su organización, se eliminan todos los secretos y se borran todos los navegadores de confianza. Todos los usuarios iniciarán sesión en el sistema usando únicamente su información de inicio de sesión y contraseña. En la pestaña **Gestión empresarial** > **Usuarios**, se ocultará la columna **Estado de la autenticación de doble factor**.

Gestión de la autenticación de doble factor para usuarios

Puede controlar la configuración de la autenticación de doble factor para todos sus usuarios y restablecerla en el portal de administración, en la pestaña **Gestión empresarial** > **Usuarios**.

Supervisión

En el portal de administración, en **Gestión empresarial** > **Usuarios**, puede ver una lista de los usuarios de su organización. El **estado de la autenticación de doble factor** indica si se ha establecido la configuración de doble factor para un usuario.

Pasos para restablecer la autenticación de doble factor para un usuario

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. En la pestaña **Usuarios** , busque el usuario cuya configuración desee cambiar y haga clic en el icono de elipsis.
3. Haga clic en **Restablecer autenticación de doble factor**.
4. Introduzca el código TOTP generado en la aplicación de autenticación del dispositivo de segundo factor y haga clic en **Restablecer**.

Como resultado, el usuario podrá volver a establecer la autenticación de doble factor.

Para restablecer los navegadores de doble confianza para un usuario:

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. En la pestaña **Usuarios** , busque el usuario cuya configuración desee cambiar y haga clic en el icono de elipsis.
3. Haga clic en **Restablecer todos los navegadores de confianza**.
4. Introduzca el código TOTP generado en la aplicación de autenticación del dispositivo de segundo factor y haga clic en **Restablecer**.

El usuario para el que ha restablecido todos los navegadores de confianza tendrá que proporcionar el código TOTP la próxima vez que inicie sesión.

Los usuarios pueden restablecer tanto los navegadores de confianza como la configuración de autenticación de doble factor por sí mismos. Para ello, deben iniciar sesión en el sistema haciendo clic en el enlace correspondiente e introduciendo el código TOTP para confirmar la operación.

Para deshabilitar la autenticación de doble factor para un usuario:

No recomendamos que deshabilite la autenticación de doble factor porque genera la posibilidad de que aparezcan amenazas de la seguridad del inquilino.

Como excepción, puede deshabilitar la autenticación de doble factor para un usuario y mantenerla para el resto de usuarios del inquilino. Es una solución para los casos en los que la autenticación de doble factor está habilitada en un inquilino en el que hay una integración de la nube configurada y esta integración da autorización a la plataforma mediante la cuenta del usuario (nombre de usuario y contraseña). Para seguir usando la integración, como solución temporal, se puede convertir el usuario en una cuenta de servicio que no admita autenticación de doble factor.

Importante
No se recomienda cambiar usuarios comunes a usuarios del servicio para deshabilitar la autenticación de doble factor porque implica riesgos para la seguridad del inquilino.

Para usar integraciones de la nube sin deshabilitar la autenticación de doble factor de los inquilinos, la solución segura que se recomienda es crear clientes API y configurar sus integraciones de cloud para que funcionen con ellas.

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. En la pestaña **Usuarios** , busque el usuario cuya configuración desee cambiar y haga clic en el icono de elipsis.
3. Haga clic en **Marcar como cuenta de servicio**. Como resultado, un usuario obtendrá un estado de autenticación de doble factor especial llamado **Cuenta de servicio.**
4. [Si al menos un usuario dentro de un inquilino ha configurado la autenticación de doble factor] Introduzca el código TOTP generado en la aplicación de autenticación del dispositivo de segundo factor para confirmar la desactivación.

Para habilitar la autenticación de doble factor para un usuario:

Puede tener que habilitar la autenticación de doble factor para un usuario específico para el que la había deshabitado anteriormente.

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. En la pestaña **Usuarios** , busque el usuario cuya configuración desee cambiar y haga clic en el icono de elipsis.
3. Haga clic en **Marcar como cuenta habitual**. Como resultado, el usuario tendrá que establecer la autenticación de doble factor o introducir el código TOTP al entrar en el sistema.

Restablecimiento de la autenticación de doble factor en caso de pérdida de dispositivo de segundo factor

Para restablecer el acceso a su cuenta en caso de haber perdido el dispositivo de segundo factor, siga una de estas sugerencias:

- Restaure su código secreto TOTP (código QR o alfanumérico) a partir de una copia de seguridad. Use otro dispositivo de segundo factor y agregue el código secreto TOTP guardado en la aplicación de autenticación instalada en dicho dispositivo.
- Pida a su administrador que restablezca la configuración de autenticación de doble factor para usted.

Protección de fuerza bruta

Un ataque de fuerza bruta es aquel en el que un intruso intenta acceder al sistema mediante el uso de numerosas contraseñas con la esperanza de que una de ellas sea la correcta.

La plataforma cuenta con un sistema de protección contra la fuerza bruta que se basa en cookies del dispositivo.

La configuración predeterminada de la plataforma para la protección contra la fuerza bruta es la siguiente:

Parámetro	Ingresar la mot de passe	Introducción del código TOTP
Límite de intentos	10	5
Período límite de intentos (el límite se restablece después del tiempo de espera)	15 min (900 s)	15 min (900 s)
Momento del bloqueo	Límite de intentos + 1 (11.º intento)	Límite de intentos
Período de bloqueo	5 min (300 s)	5 min (300 s)

Si habilita la autenticación de doble factor, se emite una cookie del dispositivo a un cliente (navegador) una vez que la autenticación se ha efectuado correctamente mediante ambos factores (contraseña y código TOTP).

En el caso de los navegadores de confianza, la cookie del dispositivo se emite tras una autenticación correcta mediante un solo factor (contraseña).

Los intentos de introducción del código TOTP se registran por usuario, no por dispositivo. Esto significa que, aunque un usuario intente introducir el código TOTP en varios dispositivos, estos se bloquearán igualmente.

Actualización de agentes automáticamente

Importante
Actualmente, solo tiene acceso a la funcionalidad de gestión de actualizaciones de agentes si tiene Protección habilitado.

Cyber Protect tiene tres tipos de agentes que se pueden instalar en los equipos protegidos: Agente para Windows, Agente para Linux y Agente para Mac.

Cyber Files Cloud cuenta con una versión para Windows y otra para MacOS del agente de escritorio para File Sync & Share, que permite la sincronización de archivos y carpetas entre un equipo y el área de almacenamiento en la nube de File Sync & Share de un usuario para promover el trabajo offline, así como las prácticas de trabajo WFH (Trabaje desde casa) y BYOD (Traiga su propio dispositivo).

Para facilitar la gestión de varias cargas de trabajo, puede configurar (y deshabilitar) las actualizaciones automáticas y sin supervisión de todos los agentes en todos los equipos.

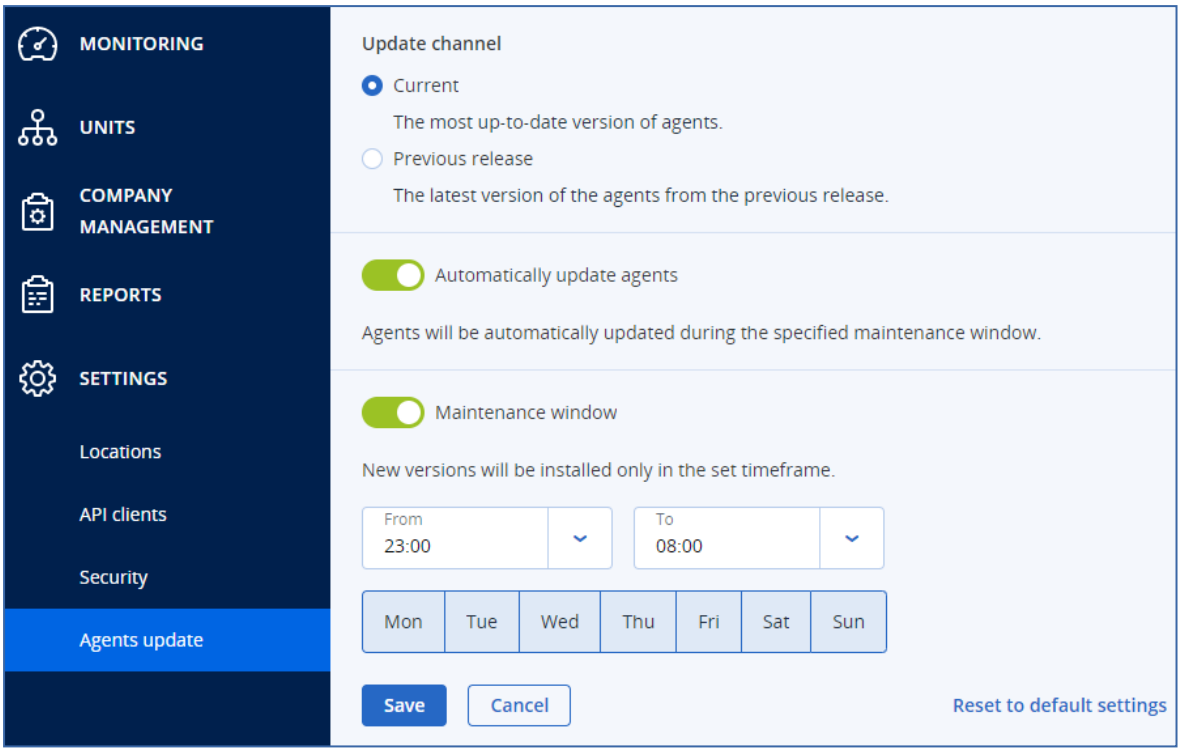
Nota
Para gestionar los agentes en equipos individuales y personalizar la configuración de las actualizaciones automáticas, consulte la actualización de agentes en la sección Manual del usuario de Cyber Protect.

Pasos para actualizar agentes automáticamente

Nota
La configuración de la actualización automática del agente para File Sync & Share se hereda de su proveedor de servicios si no tiene habilitada la protección.

Pasos para establecer una actualización automática de los agentes desde la página inicial del portal de administración

1. Seleccione **Configuración > Actualización de agentes**.



2. Seleccione la versión que desea detectar para las actualizaciones automáticas: **Actual** o **Versión anterior**.
   (El valor predeterminado es **Actual**).
3. Active la **actualización automática de agentes**.
   (El valor predeterminado es **Activado**).
4. Establezca el margen de tiempo de mantenimiento.
   (El margen predeterminado es de 23:00 a 08:00).

Nota
Aunque los procesos de actualización de los agentes están diseñados para ser rápidos y fluidos, recomendamos elegir un margen de tiempo que provoque la mínima interrupción a los usuarios, ya que estos no pueden impedir o posponer las actualizaciones automáticas.

5. [Opcional] Seleccione días específicos para que se produzcan actualizaciones automáticas.
6. Seleccione **Guardar.**

Nota
Las actualizaciones automáticas solo están disponibles para:

- Agentes de Cyber Protect de la versión 15.0.26986 (publicada en mayo de 2021) o posterior.
- Agente de escritorio para File Sync & Share, versión 15.0.30370 o posterior.

Los agentes más antiguos se deben actualizar de forma manual a la versión más reciente antes de que se produzcan las actualizaciones automáticas.

Pasos para supervisar las actualizaciones de los agentes

Importante
Las actualizaciones de los agentes solo se pueden supervisar si tiene habilitado el módulo de protección.

Para supervisar las actualizaciones de los agentes, consulte las secciones Alertas y Actividades del manual del usuario de Cyber Protect.

Configuración del almacenamiento inmutable

Con el almacenamiento inmutable, puede acceder a copias de seguridad eliminadas durante un periodo de retención especificado. Puede recuperar el contenido de esas copias de seguridad, pero no puede cambiarlo, moverlo o eliminarlo. Cuando finaliza el período de retención, las copias de seguridad eliminadas se eliminan de forma permanente.

El almacenamiento inmutable contiene las siguientes copias de seguridad:

- Copias de seguridad eliminadas manualmente.
- Las copias de seguridad eliminadas automáticamente, según la configuración de la sección **Cuánto tiempo se conservarán** de un plan de protección o la sección **Normas de retención** de un plan de limpieza.

Las copias de seguridad eliminadas en el almacenamiento inmutable siguen usando espacio de almacenamiento y se cobran en consonancia.

A los inquilinos eliminados no se les cobra por ningún almacenamiento, incluido el almacenamiento inmutable.

Para los inquilinos cliente, el almacenamiento inmutable está disponible en los siguientes modos:

- **Modo de gobierno**
  Puede deshabilitar y volver a habilitar el almacenamiento inmutable. Puede cambiar el período de retención o cambiar al modo de cumplimiento.
- **Modo de cumplimiento normativo**

  Advertencia.
  Seleccionar el modo de cumplimiento es irreversible.

  No puede desactivar el almacenamiento inmutable. No puede cambiar el período de retención y tampoco puede volver al modo de administración.

Para configurar los parámetros del almacenamiento inmutable es necesario que esté habilitada la autenticación de doble factor para el inquilino al que pertenece la cuenta de administrador.

Nota
Para permitir el acceso a las copias de seguridad eliminadas, el puerto 40440 en el almacenamiento de copia de seguridad debe estar habilitado para conexiones entrantes.

Pasos para habilitar el almacenamiento inmutable

1. Inicie sesión en el portal de administración como administrador y vaya a **Configuración** > **Seguridad**.
2. Habilite el control deslizante **Almacenamiento inmutable**.
3. Especifique un período de retención de entre 14 y 3650 días.
   El período de retención predeterminado es de 14 días. Si establece un período de retención mayor, aumentará el uso del almacenamiento.
4. Seleccione el modo de almacenamiento inmutable y, a continuación, confirme su elección si se le solicita.
5. Haga clic en **Guardar**.

   Advertencia.
   La selección del **Modo de cumplimiento normativo** es irreversible. Después de seleccionar este modo, no podrá deshabilitar el almacenamiento inmutable ni cambiar su modo o período de retención.

6. Para establecer un soporte de archivo comprimido como el almacenamiento inmutable, cree una nueva copia de seguridad en ese archivo comprimido.
   Para crear una nueva copia de seguridad, ejecute el plan de protección de forma manual o planificada.

   Advertencia.
   Si elimina una copia de seguridad antes de establecer el soporte de archivo comprimido como el almacenamiento inmutable, la copia de seguridad se eliminará de forma permanente.

Pasos para deshabilitar el almacenamiento inmutable

1. Inicie sesión en el portal de administración como administrador y vaya a **Configuración** > **Seguridad**.
2. Deshabilite el control deslizante **Almacenamiento inmutable**.

   Nota
   Solo puede deshabilitar el almacenamiento inmutable en el Modo de gobierno.

Advertencia.
La deshabilitación del almacenamiento inmutable no tiene efecto inmediato. Durante un período de gracia de 14 días, el almacenamiento inmutable seguirá activo y podrá acceder a las copias de seguridad eliminadas en función de su periodo de retención original. Cuando finaliza el período de gracia, todas las copias de seguridad en el almacenamiento inmutable se eliminan de forma permanente.

3. Haga clic en **Deshabilitar** para confirmar su elección.

Almacenamientos y agentes admitidos

- El almacenamiento inmutable solo es compatible con el almacenamiento en la nube.
  El almacenamiento inmutable está disponible para los almacenamientos en la nube alojados por Acronis y para los partners que utilicen la versión 4.7.1 o posterior de Cyber Infrastructure.
  Todos los almacenamientos que se pueden utilizar con Cyber Infrastructure Backup Gateway son compatibles. Por ejemplo, el almacenamiento Cyber Infrastructure, los almacenamientos Amazon S3 y EC2, y el almacenamiento Microsoft Azure.
  El almacenamiento inmutable requiere que el puerto TCP 40440 esté abierto para el servicio Backup Gateway en Cyber Infrastructure. En la versión 4.7.1 y posteriores, el puerto TCP 40440 se abre automáticamente con el tipo de tráfico **Copia de seguridad (ABGW) pública**. Para obtener más información sobre los tipos de tráfico, consulte la documentación de Acronis Cyber Infrastructure.
- Para el almacenamiento inmutable es necesario un agente de protección versión 21.12 (compilación 15.0.28532) o posteriores.
- Solo se admiten copias de seguridad TIBX (versión 12).

Gestión de tareas

Si su cuenta incluye el acceso al servicio Advanced Automation, haga clic en **Gestión de tareas** para ver y gestionar sus tickets del centro de asistencia.

Nota
Los usuarios que tienen asignado el rol Administrador de clientes en Advanced Automation pueden ver y gestionar todos los tickets del centro de asistencia de la organización; los usuarios que tienen asignado el rol Cliente solo pueden ver y actualizar sus propios tickets.

Visualización de tickets del centro de asistencia

Para ver los tickets del centro de asistencia creados, vaya a **Gestión de tareas > Centro de asistencia** en el portal de administración. Se muestra información sobre cada ticket, que incluye:

- Un enlace al ticket.
- El estado actual del ticket.
- El tiempo total invertido en el ticket.
- El solicitante del ticket.
- El cliente.
- La prioridad del ticket.
- El agente de soporte asignado.
- El acuerdo de nivel de servicio (SLA) asignado, cuándo se infringirá el SLA y cuándo se espera la siguiente actualización de un ingeniero de tickets.
- La fecha de la última actualización del ticket.

Para exportar los datos del ticket, haga clic en **Exportar**. Se descargará un archivo XSL con el nombre **Tickets** en su carga de trabajo.

También puede filtrar y ordenar la lista que se muestra para buscar un ticket específico. Si necesita un filtrado más avanzado, use la herramienta **Filtro** para definir qué tickets deben mostrarse.

Creación de un ticket del centro de asistencia

Pasos para crear un nuevo ticket

1. Vaya a **Gestión de tareas > Centro de asistencia**. Se muestra una lista con los tickets abiertos.

   Nota
   Los usuarios que tienen asignado el rol Administrador de clientes en Advanced Automation verán todos los tickets del centro de asistencia de la organización; los usuarios que tienen asignado el rol Cliente solo verán sus propios tickets.

2. Haga clic en **+ Nuevo**. Se muestra el diálogo Crear nuevo ticket.
3. Defina lo siguiente:
   - En el campo **Título del ticket**, añada el título del ticket.
   - En el campo **Solicitante** (solo habilitado para los usuarios con el rol Administrador de clientes), seleccione el usuario correspondiente en la lista de usuarios y contactos activos del cliente. Tenga en cuenta que el campo **Nombre de cliente** está deshabilitado tanto para los usuarios con el rol Administrador de clientes como los del rol Cliente.
   - (Opcional) En el campo **Número de teléfono**, añada un número de teléfono. Tenga en cuenta que, si actualiza el número de teléfono que se muestra por defecto, se almacenará el nuevo número de teléfono como el predeterminado de ese usuario.
   - En el campo **Superior**, seleccione el usuario correspondiente en la lista de usuarios de cliente activos (por ejemplo, los usuarios que tienen asignado el rol Administrador de clientes).
   - En la sección **Elemento o servicio de configuración**, seleccione **Servicio gestionado** o **Servicio de TI**:
     - **Servicio gestionado**: Esta opción se selecciona y se rellena automáticamente con los detalles correspondientes si el tipo de producto Servicio gestionado está disponible en el contrato correspondiente. Tenga en cuenta que se deshabilitará esta opción si no hay ningún tipo de producto Servicio gestionado en el contrato.
     - **Servicio de TI**: Esta opción se selecciona y se rellena automáticamente con los detalles correspondientes si el tipo de producto Servicio de TI está disponible en el contrato correspondiente. Tenga en cuenta que se deshabilitará esta opción si no hay ningún tipo de producto Servicio de TI en el contrato.
     - El campo **Elemento de configuración** muestra los dispositivos enlazados con el servicio de TI o gestionado seleccionado (se muestra **CI desconocida** si el dispositivo es desconocido); es opcional seleccionar un dispositivo después de seleccionar un servicio (cuando selecciona un dispositivo en este caso, se mantiene el SLA que pertenece al servicio).

       Nota
       Entre los dispositivos que se muestran, se incluyen los que proporciona Cyber Protect. Si Cyber Protection proporciona una opción de control remoto para un dispositivo especificado, puede conectarse de forma remota desde el ticket a través del protocolo RDP o del cliente HTML5.

- También puede seleccionar una categoría en el campo **Categoría** y definir una prioridad en el campo **Prioridad**. El campo **SLA** indica el acuerdo de SLA con el proveedor de servicios gestionados.

- En la sección **Actualización del ticket**, puede añadir comentarios y descripciones de texto enriquecido (con imágenes y otros archivos multimedia hasta un máximo de 25 MB; los formatos y tipos compatibles se enumeran en la sección **Adjuntos**) en el cuadro de texto que se muestra. Tenga en cuenta que el estado del ticket se establece por defecto en **Nuevo** y no se puede cambiar.
- Haga clic para habilitar el conmutador **Enviar correo electrónico al solicitante** para asegurarse de que las actualizaciones del ticket se envían por correo electrónico al solicitante.
- En la sección **Adjuntos**, haga clic (o arrastre y suelte) para añadir los adjuntos correspondientes.

  Los adjuntos pueden ser de los siguientes formatos y tipos (hasta un máximo de 25 MB):
  - Multimedia: .avi, .mp4, .mp3
  - Correo electrónico: .eml, .msg
  - Imágenes: .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg
  - Documentos y archivos de registro: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
  - Archivos comprimidos: .zip, .rar

4. Haga clic en **Listo**. Cuando se genere el ticket, se añadirá a la lista de tickets abiertos.

Actualización de tickets del centro de asistencia

Pasos para actualizar un ticket

1. Vaya a **Gestión de tareas > Centro de asistencia**. Se muestra una lista con los tickets abiertos actualmente.

   Nota
   Los usuarios que tienen asignado el rol Administrador de clientes en Advanced Automation verán todos los tickets del centro de asistencia de la organización; los usuarios que tienen asignado el rol Cliente solo verán sus propios tickets.

2. (Opcional) Si tiene muchos tickets, utilice el filtro para localizar los que busca.

   Haga clic en **Filtro** (o **Filtros guardados** si ya había definido un filtro) y seleccione los valores correspondientes en los campos que se muestran. Tenga en cuenta que puede hacer clic en el conmutador **Añadir a los filtros guardados** para guardar el filtro definido para usarlo más adelante.

   Otra opción es utilizar la barra de **búsqueda** para localizar los tickets correspondientes.
3. Haga clic en el enlace de la fila del ticket correspondiente en las pestañas que se muestran:
   - **Actividades**: Muestra la actividad reciente del ticket, incluido el estado actual y los comentarios introducidos en el ticket.

Nota
Si cambia el estado de un ticket que se había creado debido a una alerta en la consola de Cyber Protect a **Cerrado**, también se cerrará la alerta en la consola de Cyber Protect.

- **Información general**: Muestra la configuración general del ticket que se puede modificar si es necesario; para obtener más información, consulte "Creación de un ticket del centro de asistencia" (p. 40).

  Tenga en cuenta que en esta pestaña puede cambiar el estado del ticket; por ejemplo, cámbielo a **En progreso** cuando empiece a trabajar en él o páselo a **Cerrado** cuando pueda cerrarse. También puede cambiar los dispositivos enlazados con un ticket. Por ejemplo, si se ha creado un ticket que no incluye el dispositivo correcto, puede hacer clic en la lista desplegable **Elemento de configuración** para seleccionar el dispositivo correspondiente.

Para obtener más información sobre los distintos campos disponibles al editar un ticket, consulte "Creación de un ticket del centro de asistencia" (p. 40).

4. Haga clic en **Guardar cambios**.

   Tenga en cuenta que, si se habilita el conmutador **Enviar correo electrónico al solicitante**, se enviará un correo electrónico al usuario correspondiente.

Supervisión

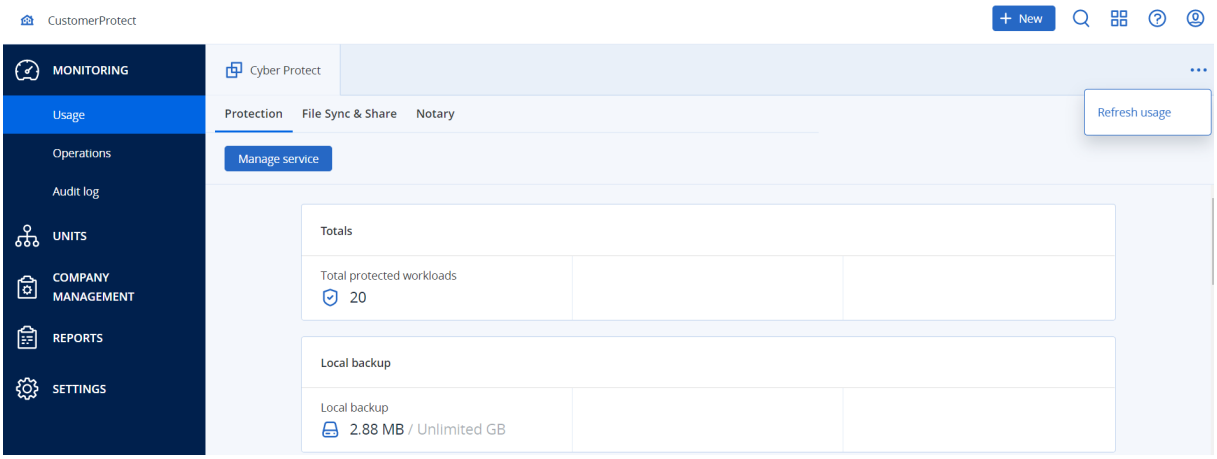
Para acceder a la información sobre las operaciones y el uso de los servicios, haga clic en **Supervisión**.

Uso

En la pestaña **Uso** se ofrece un resumen del uso de los servicios, incluidas las cuotas, si hay alguna, y a través de ella puede acceder a las consolas del servicio.

Para actualizar los datos de uso que se muestran en la tabla, haga clic en la esquina superior derecha de la pantalla y seleccione **Actualizar uso**.

Nota
Puede llevar hasta 10 minutos recuperar los datos. Recargue la página para ver los datos actualizados.



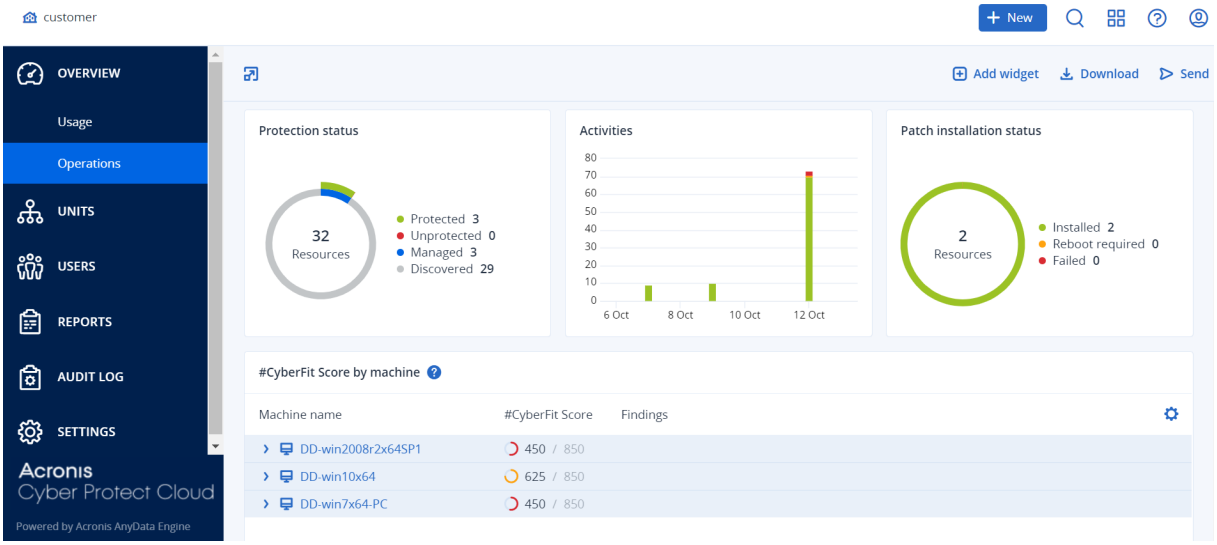
Panel de control de operaciones

El panel de información **Operaciones** está disponible solo para los administradores de la empresa cuando trabajan como empresa.

El panel de control **Operaciones** proporciona una serie de widgets personalizables que dan una imagen general de las operaciones relacionadas con el servicio de Cyber Protection.

Los widgets se actualizan cada dos minutos. Los widgets tienen elementos interactivos que le permiten investigar y solucionar problemas. Puede descargar el estado actual del panel de información o bien enviarlo por correo electrónico en formato .pdf y/o .xls.

Puede elegir entre una gran variedad de widgets, presentados como tablas, gráficos circulares, diagramas de barras, listas y estructuras de árbol. Puede agregar varios widgets del mismo tipo con diferentes filtros.



Pasos para reorganizar los widgets en el panel de información

Haga clic en los nombres de los widgets para arrastrarlos y soltarlos.

Pasos para editar un widget

Haga clic en el icono de lápiz situado al lado del nombre del widget. Al editar un widget, puede cambiarle el nombre, modificar el intervalo de tiempo y establecer filtros.

Pasos para agregar un widget

Haga clic en **Añadir widget** y, luego, realice uno de los siguientes procedimientos:

- Haga clic en el widget que quiera añadir. El widget se añadirá con la configuración predeterminada.
- Para editar el widget antes de añadirlo, haga clic en el icono de lápiz cuando el widget esté seleccionado. Después de editar el widget, haga clic en **Listo**.

Pasos para eliminar un widget

Haga clic en el signo de X situado al lado del nombre del widget.

Estado de la protección

Estado de la protección

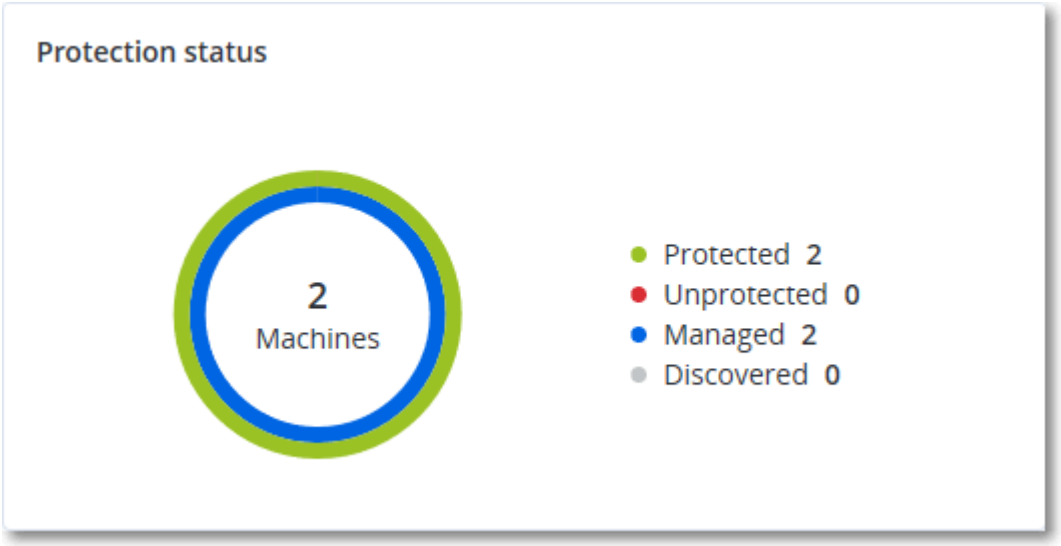
Este widget muestra el estado de protección actual de todos los equipos.

Un equipo puede encontrarse en uno de los siguientes estados:

- **Protegido**: equipos con un plan de protección aplicado.
- **Sin protección**: equipos sin un plan de protección aplicado. Incluyen tanto a los equipos detectados como a los gestionados en los que no hay ningún plan de protección aplicado.

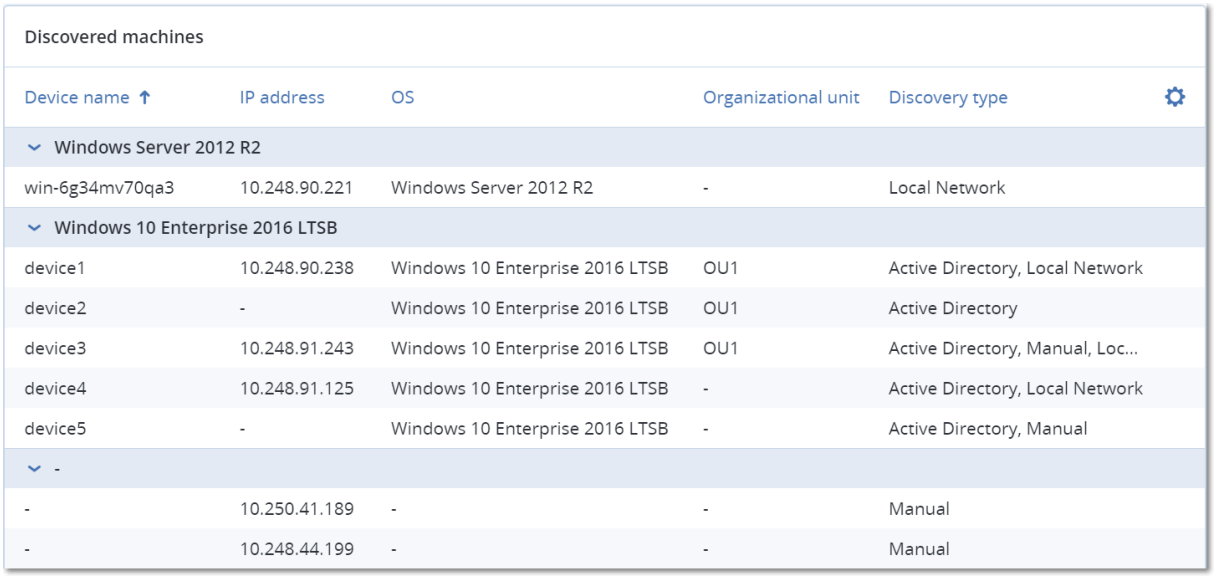
- **Gestionado**: equipos en los que está instalado un agente de protección.
- **Detectado**: equipos en los que no está instalado un agente de protección.

Si hace clic en el estado del equipo, se le redirigirá a la lista de equipos con este estado para que obtenga más información.



Equipos detectados

Este widget muestra la lista de equipos detectados en el intervalo de tiempo especificado.



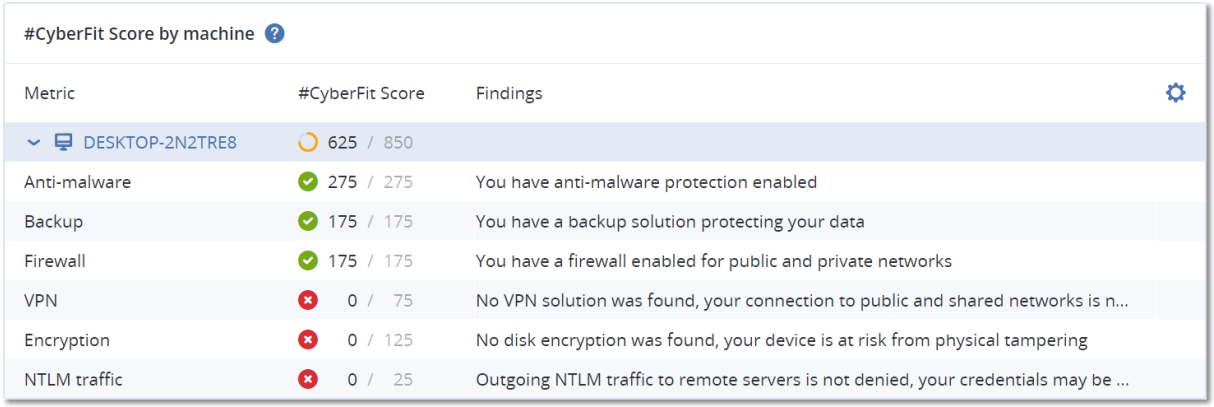
#CyberFit Score por equipo

Este widget muestra para cada equipo el #CyberFit Score total, las puntuaciones que lo componen e información sobre cada uno de los parámetros evaluados:

- Antimalware
- Copia de seguridad
- Cortafuegos
- VPN
- Cifrado
- Tráfico NTLM

Para mejorar la puntuación de cada parámetro, puede consultar las recomendaciones disponibles en el informe.

Para obtener más información sobre #CyberFit Score, consulte "#CyberFit Score para equipos".



Widgets de Endpoint Detection and Response (EDR)

Importante
Es una versión de Acceso Temprano de la documentación de EDR. Algunas de las funciones y descripciones pueden estar incompletas.

Endpoint Detection and Response (EDR) incluye un número de widgets a los que se puede acceder desde el panel de control **Operaciones**.

Los widgets disponibles son los siguientes:

- Distribución de los principales incidentes por carga de trabajo
- Tiempo medio de reparación de incidentes
- Gráfico de quemado de incidentes de seguridad
- Estado de la red de las cargas de trabajo

Distribución de los principales incidentes por carga de trabajo

Este widget muestra las cinco cargas de trabajo con más incidentes (haga clic en **Mostrar todo** para volver a la lista de incidentes, que se filtra según los ajustes del widget).

Mantenga el ratón encima de la fila de una carga de trabajo para ver un desglose del estado actual de la investigación de los incidentes; los estados de la investigación son **Sin iniciar**, **Investigando**, **Cerrada** y **Falso positivo**. A continuación, haga clic en la carga de trabajo que desea analizar en profundidad y seleccione el cliente correspondiente en la notificación mostrada. La lista de incidentes se actualiza según los ajustes del widget.

Tiempo medio de reparación de incidentes

Este widget muestra el tiempo medio de reparación de incidentes de seguridad. Indica la rapidez con la que se investigan y reparan los incidentes.

Haga clic en una columna para ver un desglose de incidentes según la gravedad (**Crítica**, **Alta** y **Media**) y una indicación sobre cuánto tardan en repararse los distintos niveles de gravedad. El valor % mostrado entre paréntesis indica el aumento o descenso en comparación con el periodo de tiempo anterior.

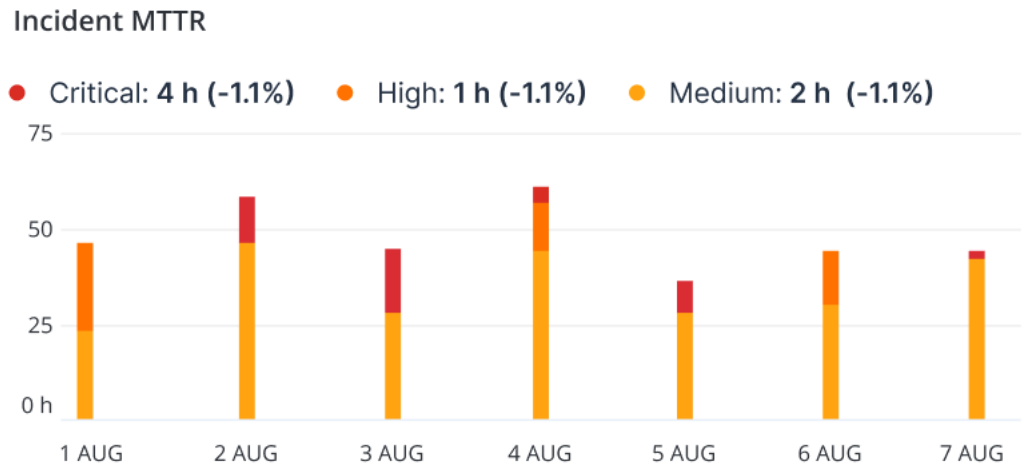
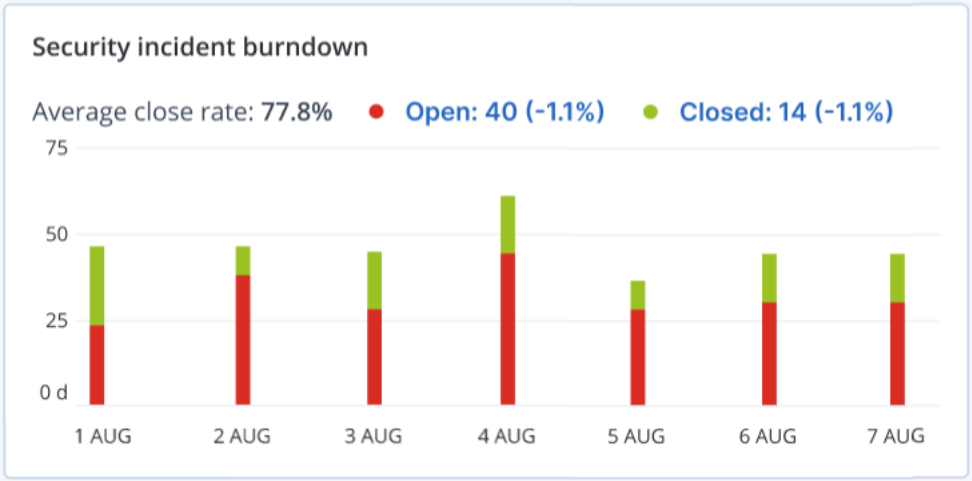


Gráfico de quemado de incidentes de seguridad

Este widget muestra la tasa de eficiencia de incidentes cerrados; el número de incidentes abiertos se mide comparado con el número de incidentes cerrados en un periodo de tiempo.

Mantenga el ratón encima de una columna para ver un desglose de los incidentes cerrados y abiertos del día seleccionado. Si hace clic en el valor Abierto, se muestra una ventana emergente para seleccionar el inquilino correspondiente. Aparece la lista de incidentes filtrados del inquilino seleccionado para mostrar los incidentes abiertos actualmente (en los estados **Investigando** o **Sin iniciar**). Si hace clic en el valor Cerrado, se muestra la lista de incidentes para el inquilino seleccionado filtrada para mostrar los incidentes que ya no están abiertos (en los estados **Cerrada** o **Falso positivo**).

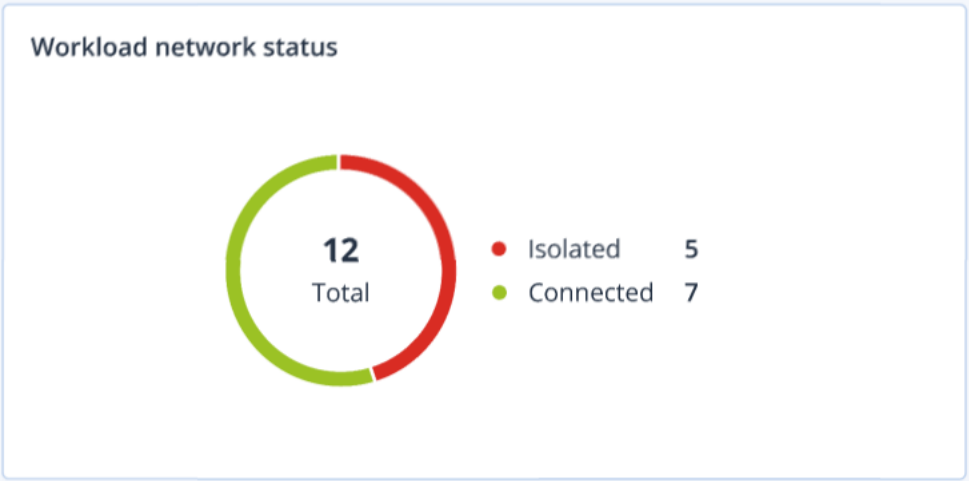
El valor % mostrado entre paréntesis indica el aumento o descenso en comparación con el periodo de tiempo anterior.



Estado de la red de las cargas de trabajo

Este widget muestra el estado de red actual de sus cargas de trabajo e indica cuántas están aisladas y cuántas conectadas.

Si hace clic en el valor Aislada, se muestra una ventana emergente para seleccionar el inquilino correspondiente. La vista de la carga de trabajo mostrada se filtra para que aparezcan las cargas de trabajo aisladas. Haga clic en el valor Conectada para ver la Carga de trabajo con la lista de agentes filtrada para mostrar las cargas de trabajo conectadas (para el inquilino seleccionado).



Supervisión del estado del disco

La supervisión del estado del disco proporciona información sobre el estado actual del disco y una previsión para que pueda evitar una pérdida de datos que pueda estar relacionada con un fallo del disco. Son compatibles tanto los discos duros como los SSD.

Limitaciones

- La previsión del estado del disco solo se puede realizar en equipos Windows.
- Únicamente se supervisan los discos de equipos físicos. Los discos de máquinas virtuales no se pueden supervisar ni aparecen en los widgets sobre el estado del disco.
- No se admiten configuraciones RAID. Los widgets de estado del disco no incluyen ninguna información sobre los equipos con implementación RAID.
- Las unidades SSD NVMe no son compatibles.

El estado del disco puede ser uno de los siguientes:

- **OK**:
  El estado del disco se encuentra entre el 70 y el 100 %.
- **Advertencia**:
  El estado del disco se encuentra entre el 30 y el 70 %.
- **Crítico**:
  El estado del disco se encuentra entre el 0 y el 30 %.
- **Calculando datos del disco**:
  Se están calculando tanto el estado del disco actual como su previsión.

Cómo funciona

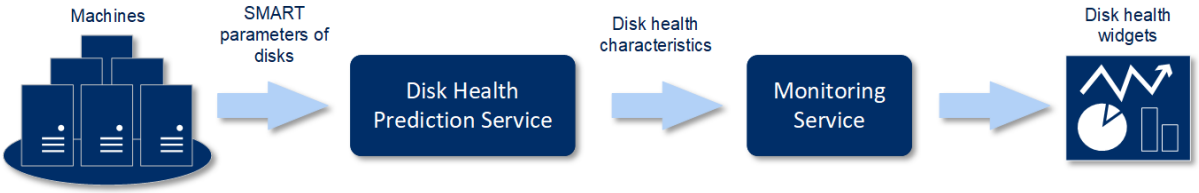
El servicio de predicción de estado del disco utiliza un modelo de predicción basado en la inteligencia artificial.

1. El agente de protección recopila los parámetros SMART de los discos y envía estos datos al servicio de predicción de estado del disco:
   - SMART 5: Número de sectores reasignados.
   - SMART 9: Horas durante las que está encendido.
   - SMART 187: Errores incorregibles de los que se ha informado.
   - SMART 188: Comando de tiempo de espera.
   - SMART 197: Número de sectores pendientes actuales.
   - SMART 198: Número de sectores incorregibles fuera de línea.
   - SMART 200: Tasa de error de escritura.
2. El servicio de previsión de estado de disco procesa los parámetros SMART recibidos, realiza predicciones y proporciona las siguientes características del estado del disco:

- Estado actual del disco: OK, Advertencia, Crítico.
- Previsión del estado del disco: negativa, estable, positiva.
- Probabilidad de la previsión del estado del disco en porcentaje.

El periodo de predicción es de un mes.

3. El servicio de supervisión recibe estas características y muestra la información relevante en los widgets del estado del disco en la consola de Cyber Protect.



Widgets sobre el estado del disco

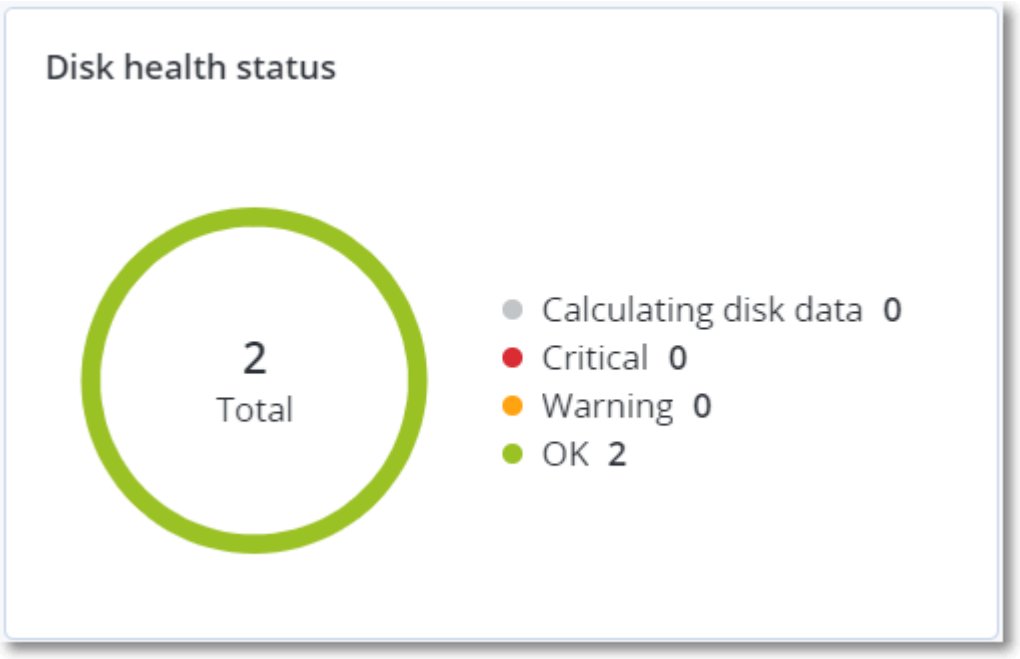
Los resultados de la supervisión del estado del disco se muestran en los siguientes widgets que están disponibles en la consola de Cyber Protect.

- **Resumen del estado del disco**: Es un widget en estructura de árbol con dos niveles de datos que se pueden cambiar al desplazarse.
  - Nivel de equipo:
    Muestra información resumida sobre el estado del disco de los equipos de los clientes seleccionados. Solo se muestra el estado del disco más crítico. El resto de los estados aparecen en la información sobre herramientas cuando se pasa el ratón por encima de un bloque concreto. El tamaño del bloque del equipo depende del tamaño total de todos los discos del equipo. El color del bloque del equipo depende del estado del disco más crítico encontrado.

- Nivel de disco:
  Muestra el estado actual de todos los discos para el equipo seleccionado. Cada bloque de discos muestra el porcentaje de una de las siguientes previsiones del estado del disco y su probabilidad:
  - Se degradará
  - Permanecerá estable

- Mejorará

- **Estado del disco**: Es un widget con gráfico circular en el que se muestra el número de discos de cada estado.



Alertas sobre el estado del disco

La comprobación del estado del disco se ejecuta cada 30 minutos, pero la alerta correspondiente se genera una vez al día. Cuando el estado del disco cambia de **Advertencia** a **Crítico**, se genera siempre una alerta.

Nombre de la alerta	Gravedad	Estado del disco	Descripción
Es posible que falle el disco	Advertencia	(30 – 70)	Es probable que el disco <disk name> en este equipo falle en el futuro. Ejecute lo antes posible una copia de seguridad de imágenes completa de este disco, reemplácelo y, a continuación, recupere la imagen en el nuevo disco.
El fallo del disco es inminente	Crítico	(0 – 30)	El disco <disk name> en este equipo está en estado crítico y es muy probable que falle pronto. En este punto, no le recomendamos realizar una copia de seguridad de imágenes de este disco, ya que la carga añadida podría hacer que el disco falle. Realice inmediatamente una copia de seguridad de los archivos más importantes de este disco y reemplácelo.

Mapa de protección de datos

Gracias a la función del mapa de protección de datos, puede descubrir todos los datos que sean importantes para usted y obtener información detallada sobre el número, el tamaño, la ubicación y el estado de protección de todos los archivos importantes en una vista escalable representada con una estructura de árbol.

El tamaño de cada bloque depende del tamaño o el número total de archivos importantes que pertenecen a un cliente o un equipo.

Los archivos pueden tener uno de los siguientes estados de protección:

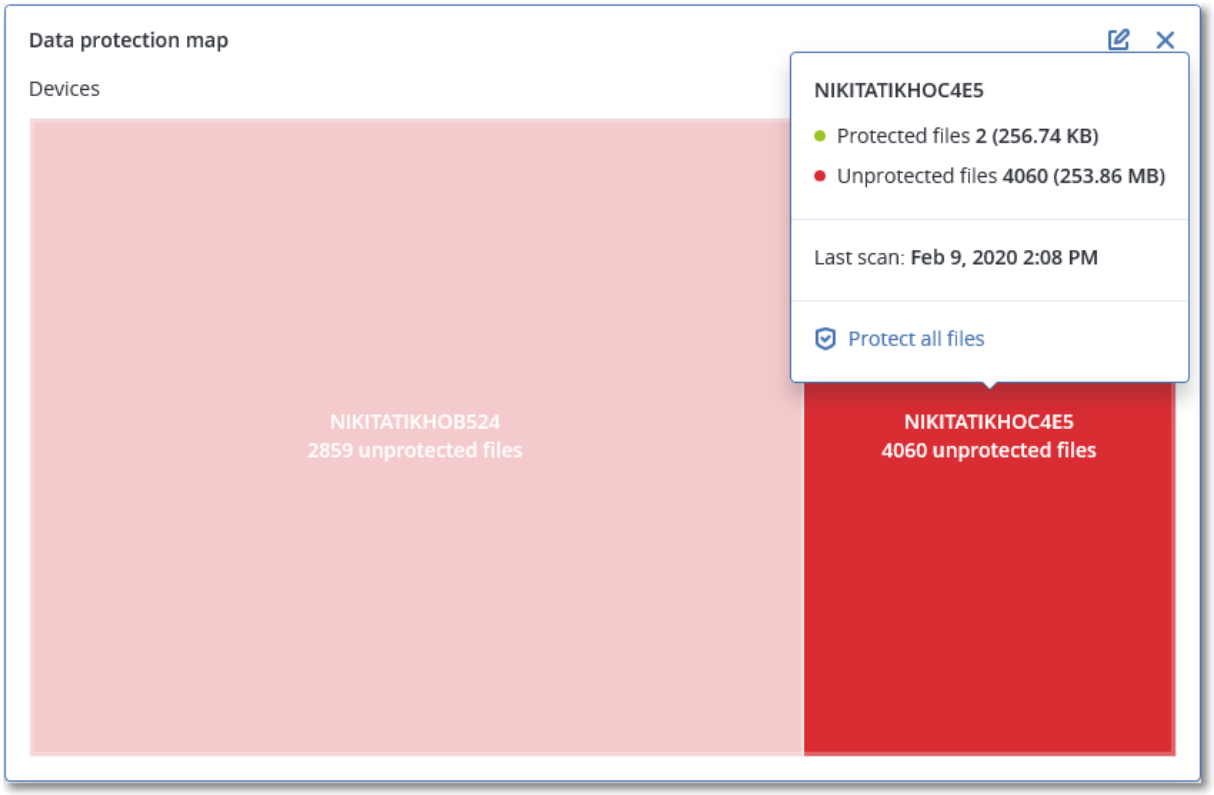
- **Crítico**: hay entre un 51 y un 100 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ni se va a realizar ninguna copia de seguridad con la configuración de copias de seguridad existentes para la ubicación, el inquilino cliente o el equipo seleccionado.
- **Bajo**: hay entre un 21 y un 50 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ni se va a realizar ninguna copia de seguridad con la configuración de copias de seguridad existentes para la ubicación, el inquilino cliente o el equipo seleccionado.
- **Medio**: hay entre un 1 y un 20 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ni se va a realizar ninguna copia de seguridad con la

configuración de copias de seguridad existentes para la ubicación, el inquilino cliente o el equipo seleccionado.

- **Alto**: todos los archivos con las extensiones que ha especificado están protegidos (se ha realizado una copia de seguridad de ellos) para la ubicación o el equipo seleccionado.

Los resultados de la evaluación de la protección de datos se encuentran en el panel de control en el widget del mapa de protección de datos, un widget en estructura de árbol en el que se muestra información sobre el nivel de un equipo:

- Nivel de equipo: muestra información sobre el estado de protección de archivos importantes según los equipos del cliente seleccionado.



Para proteger los archivos que no estén protegidos, pase el ratón por encima del bloque y haga clic en **Proteger todos los archivos**. En la ventana de diálogo encontrará información sobre el número de archivos que no están protegidos y su ubicación. Para protegerlos, haga clic en **Proteger todos los archivos**.

También puede descargar un informe detallado en formato CSV.

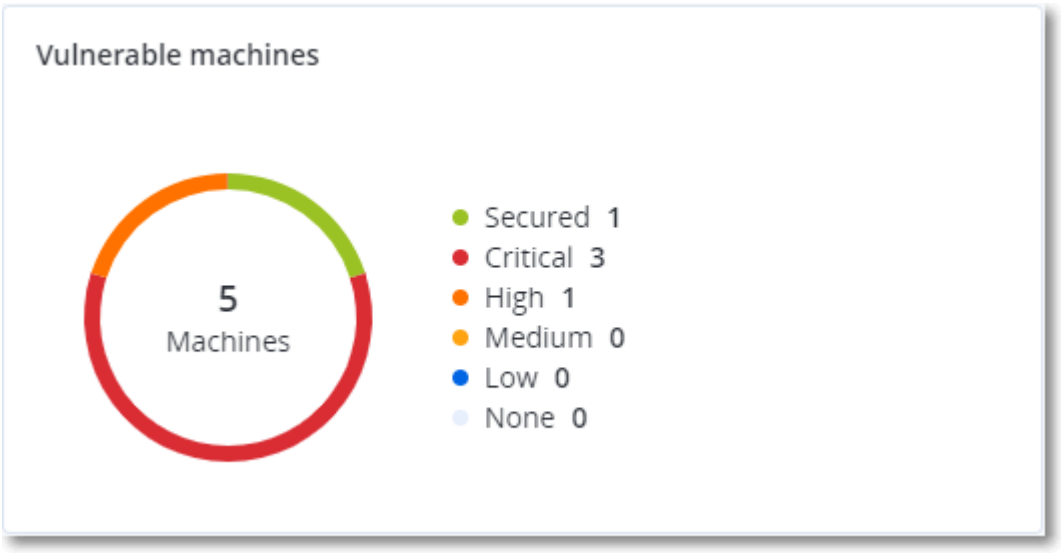
Widgets de evaluación de vulnerabilidades

Equipos vulnerables

Este widget muestra los equipos vulnerables por gravedad de la vulnerabilidad.

La vulnerabilidad encontrada tendrá uno de los siguientes niveles de gravedad de acuerdo con el sistema Common Vulnerability Scoring System (CVSS) v3.0:

- Protegido: no se ha encontrado ninguna vulnerabilidad
- Crítico: 9,0-10,0 CVSS
- Alto: 7,0-8,9 CVSS
- Medio: 4,0-6,9 CVSS
- Bajo: 0,1-3,9 CVSS
- Ninguno: 0,0 CVSS



Vulnerabilidades existentes

Este widget muestra las vulnerabilidades que existen actualmente en los equipos. En el widget **Vulnerabilidades existentes**, hay dos columnas en las que se muestran determinadas marcas de hora y fecha:

- **Primera detección**: fecha y hora en que se detectó por primera vez una vulnerabilidad en el equipo.
- **Última detección**: fecha y hora en que se detectó por última vez una vulnerabilidad en el equipo.

Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

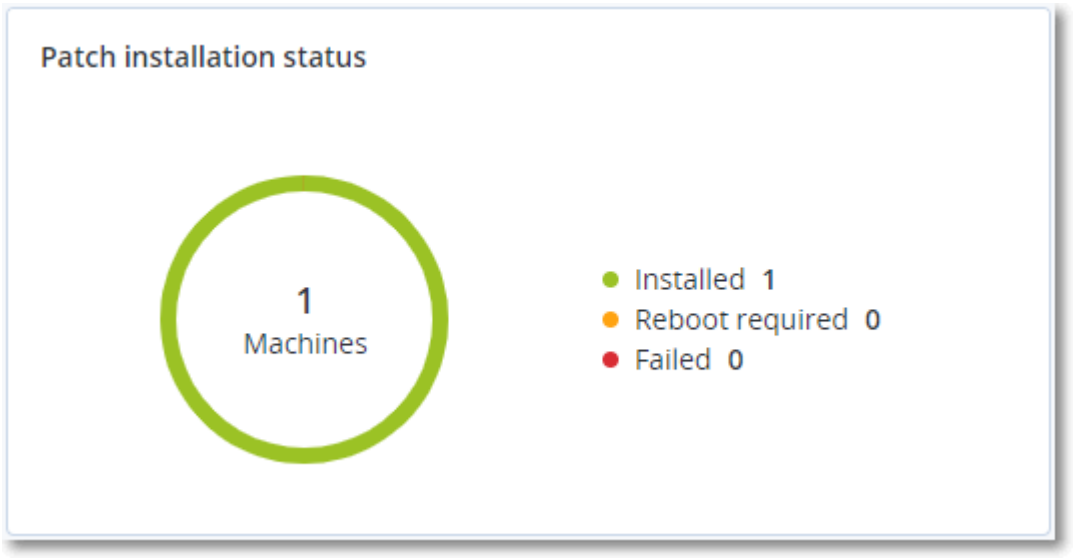
Widgets de instalación de parches

Hay cuatro widgets relacionados con la funcionalidad de gestión de parches.

Estado de instalación del parche

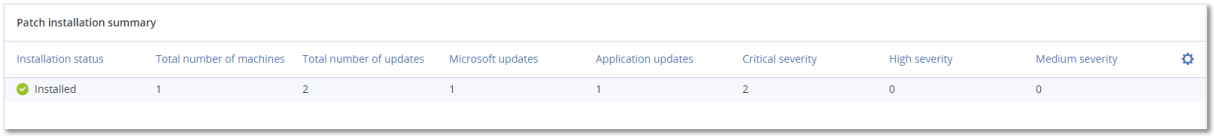
Este widget muestra el número de equipos agrupados por estado de instalación de parches.

- **Instalado**: todos los parches disponibles están instalados en el equipo.
- **Reinicio necesario**: después de la instalación de un parche, es necesario reiniciar el equipo.
- **Fallida**: la instalación del parche ha fallado en el equipo.



Resumen de la instalación del parche

Este widget muestra el resumen de parches que hay en los equipos por estado de instalación de parches.



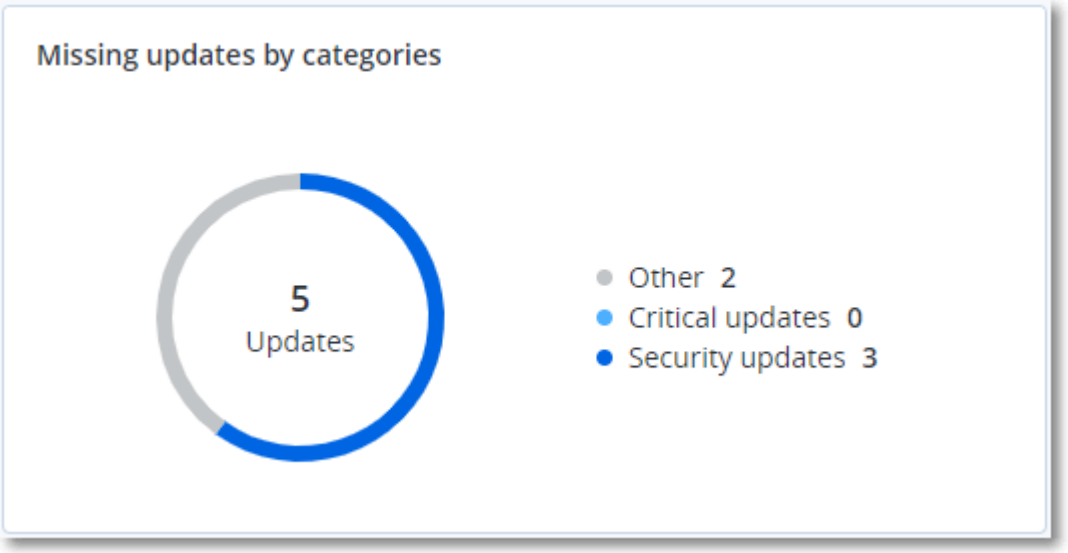
Historial de instalación de parches

Este widget muestra información detallada sobre los parches que hay en los equipos.

Actualizaciones que faltan por categoría

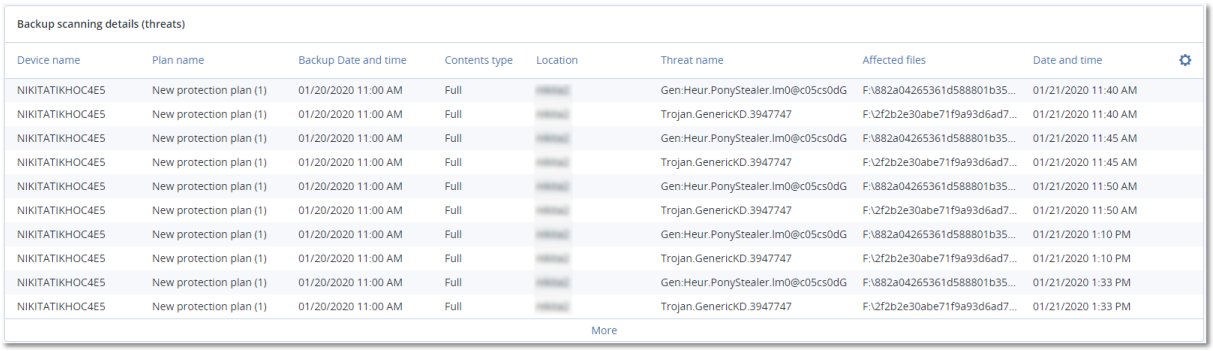
Este widget muestra el número de actualizaciones que faltan por categoría. Se muestran las siguientes categorías:

- Actualizaciones de seguridad
- Actualizaciones críticas
- Otros



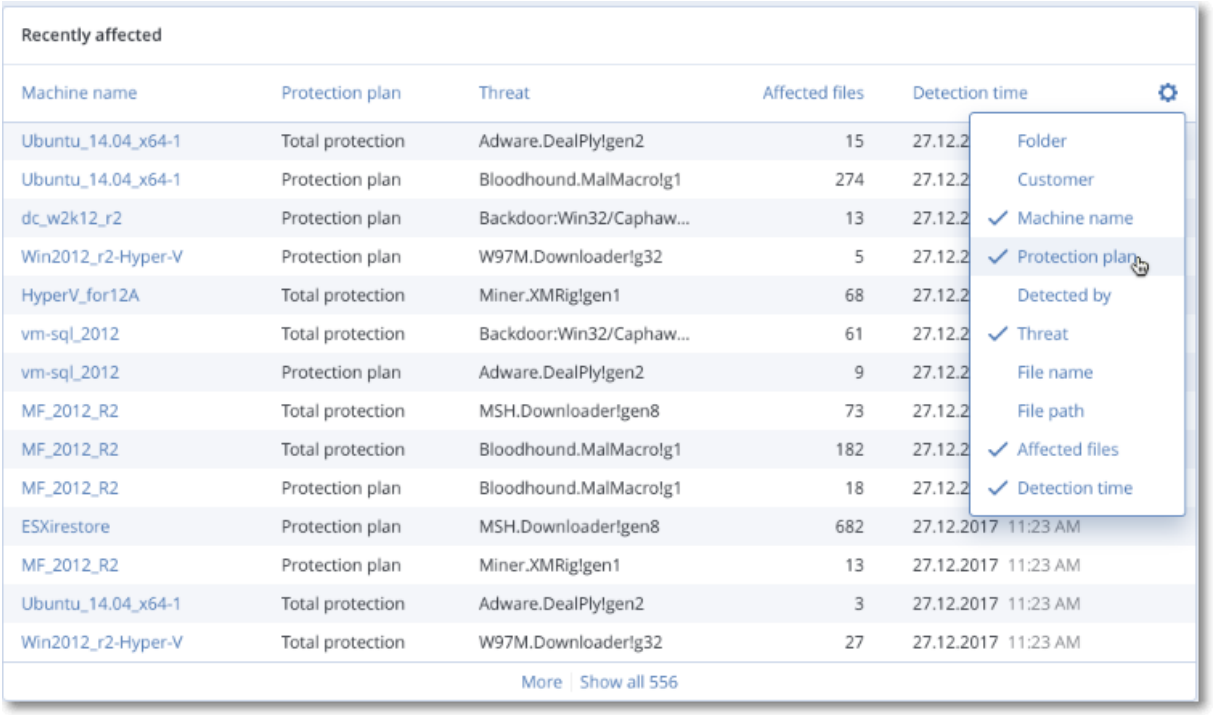
Detalles del análisis de copias de seguridad

Este widget muestra información detallada sobre las amenazas detectadas en las copias de seguridad.



Elementos afectados recientemente

Este widget muestra información detallada sobre las cargas de trabajo que se han visto afectadas por amenazas como virus, malware y ransomware. Puede encontrar información sobre las amenazas detectadas, la hora a la que se detectaron y el número de archivos que se vieron afectados.



Descargar datos de cargas de trabajo afectadas recientemente

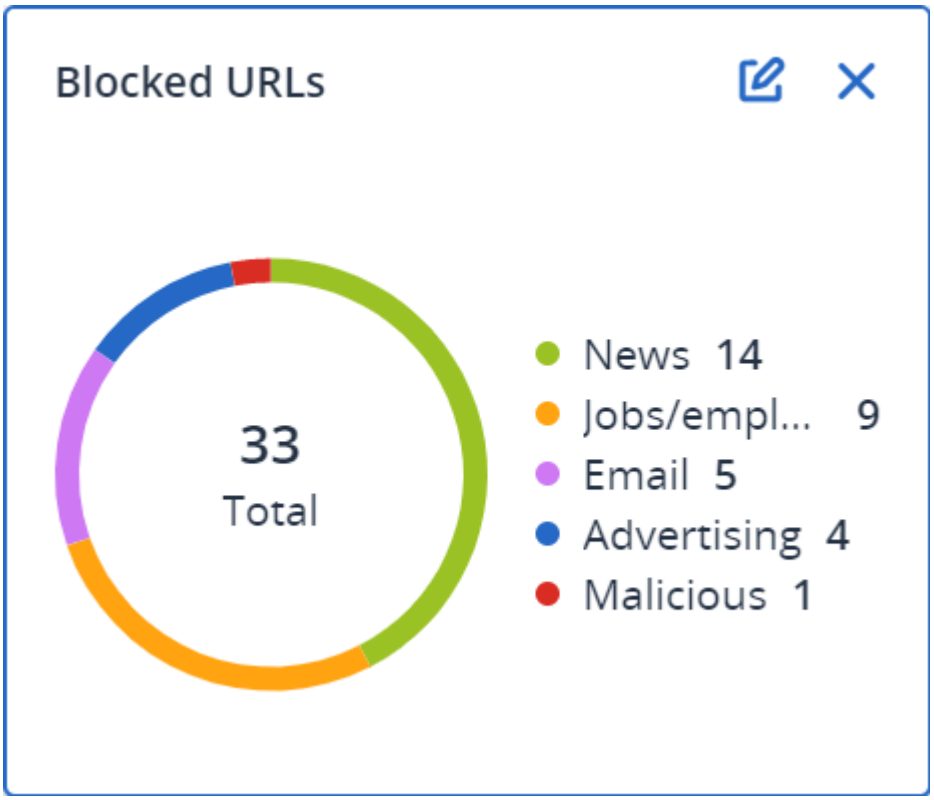
Puede descargar los datos de las cargas de trabajo que se han visto afectadas, generar un archivo CSV y enviarlo a los destinatarios que especifique.

Para descargar los datos de las cargas de trabajo que se han visto afectadas, siga los siguientes pasos:

1. En el widget **Elementos afectados recientemente**, haga clic en **Descargar datos**.
2. En el campo **Período**, introduzca el número de días de los cuales desee descargar datos. Solo puede indicar 200 días como máximo.
3. En el campo **Destinatarios**, introduzca las direcciones de correo electrónico de todas las personas que recibirán un mensaje con un enlace para descargar el archivo CSV.
4. Haga clic en **Descargar**.
   El sistema empezará a generar el archivo CSV con los datos de las cargas de trabajo que se han visto afectadas en el período de tiempo que ha especificado. Cuando el archivo CSV se haya creado, el sistema enviará un correo electrónico a los destinatarios. Entonces, cada destinatario podrá descargar el archivo CSV.

URL bloqueadas

El widget muestra las estadísticas de las URL bloqueadas por categoría. Para obtener más información acerca del filtrado y la categorización de las URL, consulte el manual del usuario de ciberprotección.



Widgets de inventario de software

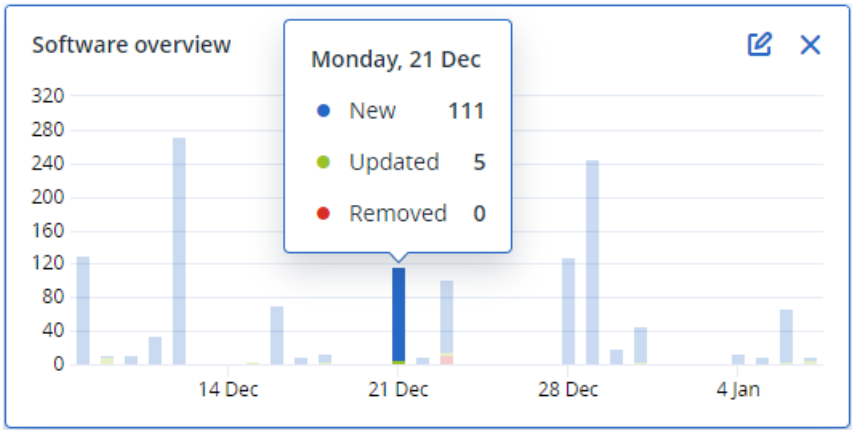
El widget de tabla de **Inventario de software** muestra información detallada sobre todo el software que se ha instalado en dispositivos de Windows y macOS en su organización.

Software inventory

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
O0003079									
O0003079	Microsoft Policy Platform	68.1.1010.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Silverlight	5.1.50918.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	c:\Program Files\Microsof...	System
O0003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft VC++ redistribu...	12.0.0.0	Intel Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 200...	8.0.61000	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 200...	9.0.30729	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 2010	10.0.40219	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 201...	11.0.61030.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System

More Less Show 248

El widget de **información general del software** muestra el número de aplicaciones nuevas, actualizadas y eliminadas en dispositivos de Windows y macOS en su organización durante un período específico de tiempo (7 días, 30 días o el mes en curso).



Cuando pase el ratón sobre determinada barra del gráfico, aparecerá la siguiente información sobre la herramienta:

Nuevas: el número de aplicaciones instaladas recientemente.

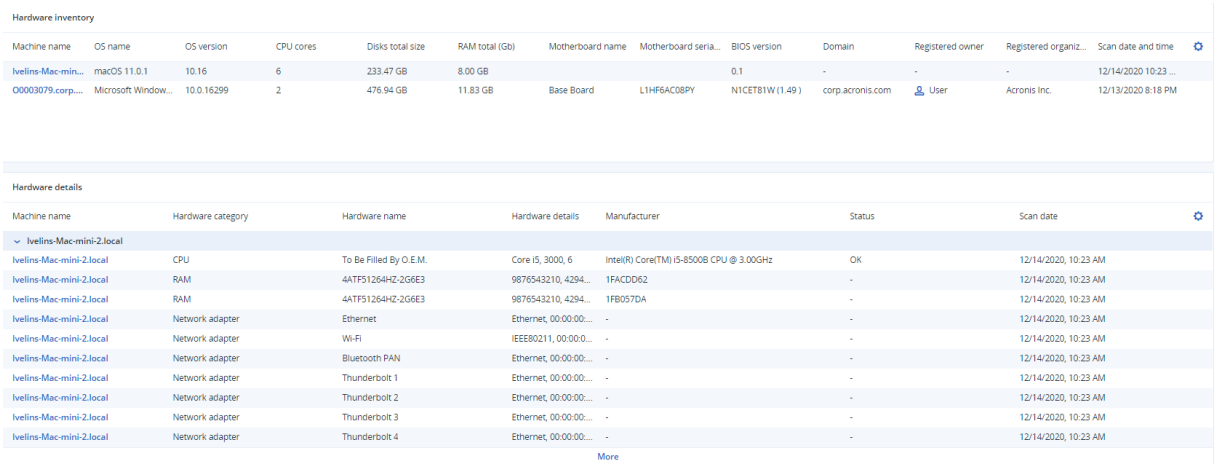
Actualizadas: el número de aplicaciones actualizadas.

Eliminadas: el número de aplicaciones eliminadas.

Cuando haga clic en la parte de la barra correspondiente a determinado estado, se le redirigirá a la página **Gestión del software** -> **Inventario del software**. La información que aparece en esa página está filtrada de acuerdo con la fecha y el estado correspondientes.

Widgets de inventario de hardware

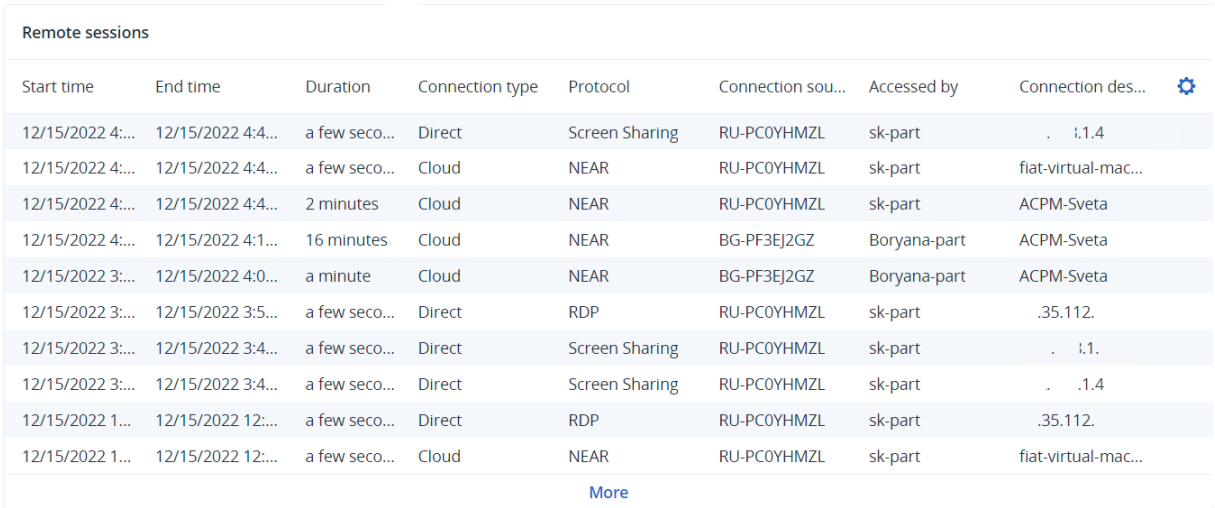
Los widgets de tablas de **inventario de hardware** y de **detalles de hardware** muestran información sobre todo el hardware instalado en dispositivos físicos y virtuales de Windows y macOS en su organización.



El widget de tabla de **cambios de hardware** muestra información sobre el hardware que se ha añadido, eliminado y cambiado en dispositivos físicos y virtuales de Windows y macOS en su organización durante un período específico de tiempo (7 días, 30 días o el mes en curso).

Historial de sesión

El widget muestra la información detallada sobre las sesiones de escritorio remoto y de transferencia de archivos realizadas en su organización durante un período de tiempo determinado.



Registro de auditoría

Para ver el registro de auditoría, Vaya a **Supervisión** > **Registro de auditoría**.

El registro de auditoría proporciona un registro cronológico de los eventos siguientes:

- Operaciones realizadas por los usuarios en el portal de gestión
- Operaciones con recursos de la nube a la nube ejecutadas por los usuarios en la consola de Cyber Protect
- Las operaciones de secuencia de comandos cibernética realizadas por los usuarios en la consola de Cyber Protect
- Sistema de mensajes sobre el cumplimiento de cuotas y el uso de estas

El registro muestra eventos de la organización o la unidad en la que esté operando, así como de sus unidades secundarias. Puede hacer clic en un evento para ver más información sobre este.

Los registros de auditoría se almacenan en el centro de datos y su disponibilidad no puede verse afectada por problemas relacionados con los equipos de usuarios finales.

El registro se borra a diario. Los eventos se eliminan tras 180 días.

Campos del registro de auditoría

El registro muestra la siguiente información para cada evento:

- **Evento**
  Descripción breve del evento. Por ejemplo, **Se ha creado un inquilino**, **Se ha eliminado un inquilino**, **Se ha creado un usuario**, **Se ha eliminado un usuario**, **Se ha alcanzado la cuota**, **Se ha examinado el contenido de la copia de seguridad** o **Se ha cambiado la secuencia de comandos**.
- **Gravedad**
  Puede ser una de las opciones siguientes:
  - **Error**
    Indica un error.
  - **Advertencia**
    Indica una acción potencialmente negativa. Por ejemplo, **Se ha eliminado un inquilino**, **Se ha eliminado un usuario** o **Se ha alcanzado la cuota**.
  - **Aviso**
    Indica que es posible que un evento requiera atención. Por ejemplo, **Se ha actualizado un inquilino** o **Se ha actualizado un usuario**.
  - **Informativo**
    Indica una acción o un cambio informativo neutral. Por ejemplo, **Se ha creado un inquilino**, **Se ha creado un usuario**, **Se ha actualizado la cuota** o **Se ha eliminado el plan de programación**.

- **Fecha**

  La fecha y la hora en las que ocurrió el evento.
- **Nombre del objeto**

  El objeto con el que se realizó la operación. Por ejemplo, el objeto del evento **Se ha actualizado un usuario** es el usuario cuyas propiedades se modificaron. En el caso de los eventos relacionados con una cuota, dicha cuota sería el objeto.
- **Inquilino**

  El nombre de la unidad a la que pertenece el objeto. Por ejemplo, el inquilino del evento **Se ha actualizado un usuario** es la unidad a la que pertenece el usuario. El inquilino del evento **Se ha alcanzado la cuota** es el usuario que ha alcanzado la cuota.
- **Iniciador**

  El inicio de sesión del usuario que inició el evento. En el caso de mensajes del sistema y eventos iniciados por los administradores de nivel superior, el iniciador se muestra como **Sistema**.
- **Inquilino del iniciador**

  El nombre de la unidad a la que pertenece el iniciador. En el caso de mensajes del sistema y eventos iniciados por los administradores de nivel superior, el campo está vacío.
- **Método**

  Muestra si el evento se inició a través de la interfaz web o la API.
- **IP**

  Dirección IP del equipo desde el que se inició el evento.

Filtrado y búsqueda

Puede filtrar los eventos por tipo, gravedad o fecha. También puede buscarlos por nombre, objeto, inquilino, iniciador o inquilino del iniciador.

Generación de informes

Para acceder a los informes sobre las operaciones y el uso de los servicios, haga clic en **Informes**.

Nota
Esta función no está disponible en las ediciones Estándar del servicio Cyber Protection.

Informes de uso

Los informes de uso proporcionan datos históricos sobre la utilización de los servicios. Los informes de uso están disponibles en formato CSV y HTML.

Tipo de informe

Puede seleccionar uno de los siguientes tipos de informe:

- **Uso actual**
  En el informe se incluyen los parámetros de uso del servicio actuales.
- **Resumen del período**
  En el informe se incluyen los parámetros de uso del servicio para el final del periodo especificado y la diferencia entre los parámetros del comienzo y el final del periodo especificado.
- **Día a día del período**
  En el informe se incluyen los parámetros de uso del servicio y sus cambios para cada día del periodo especificado.

Ámbito del informe

Puede seleccionar el ámbito del informe entre los valores siguientes:

- **Clientes y socios directos**
  El informe solo incluye las métricas de uso del servicio para las unidades secundarias inmediatas de la compañía o unidad en la que está operando.
- **Todos los socios y clientes**
  El informe incluye las métricas de uso del servicio para todas las unidades secundarias de la compañía o unidad en la que está operando.
- **Todos los clientes y partners (incluyendo los detalles de usuario)**
  El informe incluye las métricas de uso del servicio para todas las unidades secundarias de la compañía o unidad en la que está operando, y para todos los usuarios de la unidades.

Parámetros con uso cero

Puede reducir el número de filas en el informe si muestra la información sobre los parámetros cuyo uso sea distinto a cero y oculta la información de aquellos cuyo uso sea cero.

Configuración de los informes de uso planificados

Un informe programado recoge los parámetros de uso del servicio durante el último mes natural completo. Los informes se generan a las 23:59:59 (hora UTC) del primer día del mes y se envían el segundo día. Los informes se envían a todos los administradores de su compañía o unidad que tengan marcada la casilla de verificación **Informes de uso planificados** seleccionada en la configuración del usuario.

Para habilitar o deshabilitar un informe programado

1. Inicie sesión en el portal de gestión.
2. Asegúrese de que opera en la máxima compañía o unidad disponible para usted.
3. Haga clic en **Informes** > **Uso**.
4. Haga clic en **Programado**.
5. Seleccione o deseleccione la casilla de verificación de informes **Enviar un resumen mensual**
6. En **Nivel de detalle**, seleccione el ámbito del informe.
7. [Opcional] Seleccione **Ocultar parámetros con uso cero** si no desea incluir parámetros con uso cero en el informe.

Configuración de los informes de uso personalizados

Un informe personalizado no puede planificarse, se genera a petición. El informe se enviará a su dirección de correo electrónico.

Para generar un informe personalizado

1. Inicie sesión en el portal de gestión.
2. Vaya hasta la unidad en la que desee crear un informe.
3. Haga clic en **Informes** > **Uso**.
4. Haga clic en **Personalizar**.
5. En **Tipo**, seleccione el tipo de informe.
6. [No disponible para el tipo de informe **Uso actual**] En **Período**, seleccione el período del informe:
   - **Mes actual**
   - **Mes anterior**
   - **Personalizado**
7. [No disponible para el tipo de informe **Uso actual**] Si quiere especificar un período de informe personalizado, seleccione las fechas de inicio y fin. De lo contrario, omita este paso.
8. En **Nivel de detalle**, seleccione el ámbito del informe.
9. [Opcional] Seleccione **Ocultar parámetros con uso cero** si no desea incluir parámetros con uso

cero en el informe.

10. Para generar el informe, haga clic en **Generar y enviar**.

Datos de los informes de uso

El informe sobre el uso del servicio de Cyber Protection incluye los datos siguientes sobre una empresa o unidad:

- Tamaño de las copias de seguridad por unidad, usuario o tipo de dispositivo.
- Número de dispositivos protegidos por unidad, usuario o tipo de dispositivo.
- Precio por unidad, usuario o tipo de dispositivo.
- El tamaño total de las copias de seguridad.
- La cantidad total de dispositivos protegidos.
- Precio total.

Nota
Si el servicio Cyber Protection no puede detectar un tipo de dispositivo, dicho dispositivo aparecerá como **sin tipo** en el informe.

Informes de operaciones

Los informes de las **operaciones** están disponibles solo para los administradores de la empresa cuando trabajan como empresa.

Un informe sobre operaciones puede incluir cualquier conjunto de los widgets del panel de información **Operaciones**. Todos los widgets muestran la información de resumen de toda la empresa.
Según el tipo de widget, el informe incluye datos para un intervalo de tiempo o para el momento de la navegación o generación de informes. Consulte "Datos informados según el tipo de widget" (p. 84).

Todos los widgets históricos muestran la información del mismo intervalo de tiempo. Puede cambiar este intervalo en la configuración de los informes.

Puede utilizar informes predeterminados o crear uno personalizado.

Puede descargar un informe o enviarlo por correo electrónico en formato XLSX (Excel) o PDF.

Los informes predeterminados se indican a continuación:

Nombre del informe	Descripción
#CyberFit Score por equipo	Muestra el #CyberFit Score, basado en la evaluación de parámetros de seguridad y en la configuración de cada equipo, así como las recomendaciones para mejoras.

Alertas	Muestra las alertas que se producen durante un periodo especificado.
Detalles del análisis de copias de seguridad	Muestra información detallada sobre las amenazas detectadas en las copias de seguridad.
Actividades diarias	Muestra información resumida sobre las actividades realizadas durante un periodo especificado.
Mapa de protección de datos	Muestra información detallada sobre el número, el tamaño, la ubicación y el estado de protección de todos los archivos importantes de los equipos.
Amenazas detectadas	Muestra información sobre los equipos afectados por número de amenazas bloqueadas, así como la de los equipos en buen estado y los vulnerables.
Equipos detectados	Enumera todos los equipos hallados en la red de la organización.
Predicción del estado del disco	Muestra predicciones de cuándo se deteriorará el disco duro/SSD y del estado actual del disco.
Vulnerabilidades existentes	Muestra las vulnerabilidades existentes en el sistema operativo de su organización. El informe también muestra información de los equipos afectados en su red respecto a cada producto enumerado.
Resumen de gestión de parches	Muestra el número de parches que faltan, los instalados y los aplicables. Puede desglosar los informes para obtener información sobre los parches que faltan y los instalados, así como detalles de todos los sistemas.
Resumen	Muestra la información resumida sobre los dispositivos protegidos durante un periodo especificado.
Actividades semanales	Muestra información resumida sobre las actividades realizadas durante un periodo especificado.
Inventario de software	Muestra información detallada sobre todo el software instalado en equipos de Windows y macOS en su organización.
Inventario de hardware	Muestra información detallada sobre todo el hardware disponible en equipos físicos y virtuales de Windows y macOS en su organización.
Sesiones remotas	Muestra información detallada sobre las sesiones de escritorio remoto y de transferencia de archivos realizadas en su organización durante un período de tiempo determinado.

Acciones con informes

Para ver un informe, haga clic en su nombre.

Pasos para añadir un nuevo informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes disponibles, haga clic en **Añadir informe**.
3. [Para añadir un informe predefinido] Haga clic en el nombre del informe predefinido.
4. [Para añadir un informe personalizado] Haga clic en **Personalizar** y añada widgets al informe.
5. [Opcional] Arrastre y suelte los widgets para reorganizarlos.

Pasos para editar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe que desea editar.
   Puede hacer lo siguiente:
   - Cambie el nombre al informe.
   - Cambie el intervalo de tiempo de todos los widgets del informe.
   - Especifique los destinatarios del informe y cuándo se les enviará. Los formatos disponibles son PDF y XLSX.

Pasos para eliminar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe que desea eliminar.
3. Haga clic en el icono de puntos suspensivos (...) y en **Eliminar**.
4. Haga clic en **Eliminar** para confirmar su elección.

Para programar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe que desea programar y haga clic en **Configuración**.
3. Habilite el conmutador **Planificado**.
   - Especifique las direcciones de correo electrónico de los destinatarios.
   - Seleccione el formato del informe.

     Nota
     Puede exportar hasta 1000 elementos en un archivo PDF y hasta 10 000 elementos en un archivo XLSX. La fecha y hora de los archivos PDF y XLSX utilizan la hora local de su equipo.

   - Seleccione el idioma del informe.
   - Configure la planificación.
4. Haga clic en **Guardar**.

Pasos para descargar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe y haga clic en **Descargar**.

3. Seleccione el formato del informe.

Pasos para enviar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe y haga clic en **Enviar**.
3. Especifique las direcciones de correo electrónico de los destinatarios.
4. Seleccione el formato del informe.
5. Haga clic en **Enviar**.

Pasos para exportar la estructura del informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe.
3. Haga clic en el icono de puntos suspensivos (...) y en **Exportar**.

Como resultado, la estructura del informe se guarda en su equipo como un archivo JSON.

Para volcar los datos del informe

Al utilizar esta opción, puede exportar todos los datos para un periodo personalizado, sin filtrarlos, a un archivo CSV y enviarlo a un destinatario de correo electrónico.

Nota
Puede exportar hasta 150 000 elementos en un archivo CSV. La fecha y hora del archivo CSV utilizan la Hora universal coordinada (UTC).

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe cuyos datos desea volcar.
3. Haga clic en el icono de puntos suspensivos (...) y en **Volcar datos**.
4. Especifique las direcciones de correo electrónico de los destinatarios.
5. En **Intervalo de tiempo**, especifique el periodo personalizado para el que desea volcar datos.

   Nota
   La preparación de archivos CSV para periodos más largos lleva más tiempo.

6. Haga clic en **Enviar**.

Resumen ejecutivo

El informe resumido ejecutivo presenta la información general del estado de la protección del entorno de su organización y los dispositivos protegidos para un intervalo de tiempo específico.

El informe resumido ejecutivo incluye secciones personalizables con widgets dinámicos que muestran parámetros de rendimiento claves relacionados con el uso de los siguientes servicios en

la nube: Copia de seguridad, protección contra malware, evaluación de vulnerabilidades, gestión de parches, certificación, recuperación ante desastres y File Sync & Share.

Puede personalizar el informe de diversas formas:

- Añadir o quitar secciones.
- Cambiar el orden de las secciones.
- Cambiar el nombre de secciones.
- Mover widgets de una sección a otra.
- Cambiar el orden de los widgets de cada sección.
- Añadir o quitar widgets.
- Personalizar widgets.

Puede generar informes resumidos ejecutivos en formato PDF y Excel y enviarlos a las partes interesadas o los dueños de su organización para que puedan ver fácilmente el valor técnico y comercial de los servicios prestados.

Widgets de resúmenes ejecutivos

Puede añadir o eliminar las secciones y widgets del informe resumido ejecutivo y controlar qué información incluir en él.

Widgets de resumen de cargas de trabajo

La siguiente tabla proporciona más información sobre los widgets de la sección **Resumen de cargas de trabajo**.

Widget	Descripción
Estado de la protección de las cargas de trabajo de la nube	Este widget muestra el número de cargas de trabajo de la nube protegidas y no protegidas por tipo en el momento en que se generó el informe. Las cargas de trabajo de la nube protegidas son aquellas a las que se les aplica, como mínimo, un plan de copias de seguridad. Las cargas de trabajo de la nube sin protección son aquellas a las que no se les aplica ningún plan de copias de seguridad. El gráfico muestra los siguientes tipos de carga de trabajo de la nube (en orden alfabético de la A a la Z): • Google Workspace: Drive • Gmail de Google Workspace • Unidad compartida de Google Workspace • Buzones de correo de Hosted Exchange • Buzones de correo de Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams

Widget	Descripción
	• Sitios web Para algunos tipos de carga de trabajo, se utilizan los siguientes grupos de cargas de trabajo: • Microsoft 365: Usuarios, grupos, carpeta públicas, equipos y colecciones de sitios • Google Workspace: Usuarios y unidades compartidas • Hosted Exchange: Usuarios Si un grupo de cargas de trabajo tiene más de 10 000 cargas de trabajo, el widget no mostrará ningún dato de las correspondientes cargas de trabajo. Por ejemplo, si el cliente tiene una cuenta de Microsoft 365 con 10 000 buzones de correo y un servicio de OneDrive para 500 usuarios, todos pertenecen al grupo de cargas de trabajo Usuarios. La suma de estas cargas de trabajo es 10 500, lo que excede el límite de 10 000 de un grupo de cargas de trabajo. Por lo tanto, el widget ocultará los correspondientes tipos de carga de trabajo: Buzones de correo de Microsoft 365 y Microsoft 365 OneDrive.
Resumen de ciberprotección	El widget muestra los parámetros clave del rendimiento de la ciberprotección para el periodo de tiempo especificado. **Datos en la copia de seguridad**: el tamaño total de los archivos comprimidos que se crearon en el almacenamiento local y en la nube. **Amenazas mitigadas**: el número total de malware bloqueado en los dispositivos. **URL maliciosas bloqueadas**: el número total de URL bloqueadas en todos los dispositivos. **Vulnerabilidades solucionadas**: el número total de vulnerabilidades solucionadas mediante la instalación de parches de software en todos los dispositivos. **Parches instalados**: el número total de parches instalados en todos los dispositivos. **Servidores protegidos por la recuperación ante desastres**: el número total de servidores protegidos por la recuperación ante desastres. **Usuarios de File Sync & Share**: el número total de usuarios finales e invitados que utilizan Cyber Files. **Archivos certificados ante notario**: el número total de archivos certificados ante notario. **Documentos firmados electrónicamente**: el número total de documentos firmados electrónicamente.

Widget	Descripción
	Dispositivos periféricos bloqueados: el número total de dispositivos periféricos bloqueados.
Estado de la red de las cargas de trabajo	Este widget muestra cuántas cargas de trabajo están aisladas y cuántas conectadas (el estado normal de la carga de trabajo). Seleccione el cliente correspondiente. La vista de la carga de trabajo mostrada se filtra para que aparezcan las cargas de trabajo aisladas. Haga clic en el valor Conectada para ver la Carga de trabajo con la lista de agentes filtrada para mostrar las cargas de trabajo conectadas (para el cliente seleccionado).
Estado de la protección de las cargas de trabajo	El widget muestra las cargas de trabajo protegidas y sin protección por tipo en el momento en que se generó el informe. Las cargas de trabajo protegidas son aquellas a las que se les aplica, como mínimo, un plan de protección o de copias de seguridad. Las cargas de trabajo sin protección son aquellas a las que no se les aplica ningún plan de protección ni de copias de seguridad. Se tienen en cuenta las siguientes cargas de trabajo: **Servidores**: servidores físicos y servidores de controladores de dominio. **Estaciones de trabajo**: estaciones de trabajo físicas. **Equipos virtuales**: equipos virtuales con agente y sin agente. **Servidores de alojamiento web**: servidores virtuales o físicos con cPanel o Plesk instalado. **Dispositivos móviles**: dispositivos móviles físicos. Una carga de trabajo puede pertenecer a más de una categoría. Por ejemplo, un servidor de alojamiento web se incluye en dos categorías: **Servidores** y **Servidores de alojamiento web**.

Widgets de protección contra malware

La siguiente tabla proporciona más información sobre los widgets de la sección **Protección frente a amenazas**.

Widget	Descripción
Análisis antimalware de archivos	El widget muestra los resultados del análisis antimalware bajo demanda de los dispositivos para el intervalo de fechas especificado. **Archivos**: el número total de archivos escaneados **Limpios**: el número total de archivos limpios **Detectados, en cuarentena**: el número total de archivos infectados puestos en cuarentena **Detectados, sin cuarentena**: el número total de archivos infectados que no se han puesto en cuarentena

Widget	Descripción
	Dispositivos protegidos: el número total de dispositivos con una política de protección contra malware aplicada **Número total de dispositivos registrados**: el número total de dispositivos registrados en el momento en que se generó el informe
Análisis antimalware de copias de seguridad	El widget muestra los resultados del análisis antimalware de las copias de seguridad para el intervalo de fechas especificado mediante los siguientes parámetros: • Número total de puntos de recuperación analizados • Número de puntos de recuperación limpios • Número de puntos de recuperación limpios con particiones no admitidas • Número de puntos de recuperación infectados. Este parámetro incluye el número de puntos de recuperación infectados con particiones no admitidas.
URL bloqueadas	El widget muestra los resultados de URL bloqueadas agrupadas por categoría de sitio web para el intervalo de fechas especificado. El widget enumera las siete categorías de sitio web que tienen un mayor número de URL bloqueadas y combina el resto de categorías de sitio web en **Otros**. Para obtener más información acerca de las categorías de sitio web, consulte el tema de filtrado de URL en Cyber Protection.
Gráfico de quemado de incidentes de seguridad	Este widget muestra la tasa de eficiencia de incidentes cerrados de la empresa seleccionada; el número de incidentes abiertos se mide comparado con el número de incidentes cerrados en un periodo de tiempo. Mantenga el ratón encima de una columna para ver un desglose de los incidentes cerrados y abiertos del día seleccionado. El valor % mostrado entre paréntesis indica el aumento o descenso en comparación con el periodo de tiempo anterior.
Tiempo medio de reparación de incidentes	Este widget muestra el tiempo medio de reparación de incidentes de seguridad. Indica la rapidez con la que se investigan y reparan los incidentes. Haga clic en una columna para ver un desglose de incidentes según la gravedad (**Crítica**, **Alta** y **Media**) y una indicación sobre cuánto tardan en repararse los distintos niveles de gravedad. El valor % mostrado entre paréntesis indica el aumento o descenso en comparación con el periodo de tiempo anterior.
Estado de la amenaza	Este widget muestra el estado actual de la amenaza para las cargas de trabajo de una empresa (independientemente del número de cargas de trabajo) y destaca el número de incidentes que no se han mitigado y deben investigarse. El widget también indica el número de incidentes mitigados (de forma manual o automáticamente por el sistema).

Widget	Descripción
Amenazas detectadas por la tecnología de protección	El widget muestra el número de amenazas detectadas para el intervalo de fechas especificado, agrupadas por las siguientes tecnologías de protección: • Analizando antimalware • Motor de comportamiento • Protección ante criptominado • Prevención de vulnerabilidades • Protección activa contra ransomware • Protección en tiempo real • Filtrado de URL

Widgets de copias de seguridad

La siguiente tabla proporciona más información sobre los widgets de la sección **Copia de seguridad**.

Widget	Descripción
Cargas de trabajo en la copia de seguridad	El widget muestra el número total de cargas de trabajo registradas según el estado de la copia de seguridad. **Con copia de seguridad**: número de cargas de trabajo con copia de seguridad (al menos una copia de seguridad realizada con éxito) durante el intervalo de fechas del informe. **Sin copia de seguridad**: número de cargas de trabajo sin copia de seguridad (sin una copia de seguridad realizada con éxito) durante el intervalo de fechas del informe.
Estado del disco por dispositivo físico	El widget muestra el estado agregado de los dispositivos físicos según el estado de sus discos. **OK**: este estado del disco hace referencia a los valores [70-100]. El estado del dispositivo es **OK** cuando todos sus discos tienen el estado **OK**. **Advertencia**: este estado del disco hace referencia a los valores [30-70]. El estado de un dispositivo es **Advertencia** cuando el estado de al menos uno de sus discos es **Advertencia** y cuando no hay discos con el estado **Error**. **Error**: este estado del disco hace referencia a los valores [0-30]. El estado de un dispositivo es **Error** cuando el estado de al menos uno de sus discos es **Error**. **Calculando datos del disco**: el estado de un dispositivo es **Calculando datos del disco** cuando los estados de sus discos no se han calculado todavía.
Uso del	El widget muestra el número y el tamaño totales de las copias de

Widget	Descripción
almacenamiento de copia de seguridad	seguridad en la nube y en el almacenamiento local para el intervalo de tiempo especificado.

Widgets de evaluación de vulnerabilidades y gestión de parches

La siguiente tabla proporciona más información sobre los widgets de la sección **Evaluación de vulnerabilidades y gestión de parches**.

Widget	Descripción
Vulnerabilidades solucionadas	El widget muestra los resultados de rendimiento de la evaluación de vulnerabilidades para el intervalo de fechas especificado. **Total**: el número total de vulnerabilidades solucionadas. **Vulnerabilidades de software de Microsoft**: número total de vulnerabilidades de Microsoft solucionadas en todos los dispositivos Windows. **Vulnerabilidades de software de terceros para Windows**: el número total de vulnerabilidades de terceros para Windows solucionadas en todos los dispositivos Windows. **Cargas de trabajo analizadas**: el número total de dispositivos que se han analizado correctamente para buscar vulnerabilidades al menos una vez en el intervalo de fechas especificado.
Parches instalados	El widget muestra los resultados de rendimiento de la gestión de parches para el intervalo de fechas especificado. **Instalado**: el número total de parches que se han instalado correctamente en todos los dispositivos. **Parches de software de Microsoft**: el número total de parches de software de Microsoft que se han instalado en todos los dispositivos Windows. **Parches de software de terceros para Windows**: el número total de parches de software de terceros para Windows que se han instalado en todos los dispositivos Windows. **Cargas de trabajo solucionadas**: el número total de dispositivos que se han solucionado correctamente (con al menos un parche instalado correctamente durante el intervalo de fechas especificado).

Widgets de recuperación ante desastres

La siguiente tabla proporciona más información sobre los widgets de la sección **Recuperación ante desastres**.

Widget	Descripción
Estadísticas de recuperación ante desastres	El widget muestra los parámetros de rendimiento claves de la recuperación ante desastres para el intervalo de fechas especificado. **Conmutaciones por error de producción**: el número de operaciones de conmutación por error de producción para el intervalo de tiempo especificado. **Conmutaciones por error de prueba**: el número total de operaciones de conmutación por error de prueba ejecutadas durante el intervalo de tiempo especificado. **Servidores principales**: el número total de servidores principales en el momento en que se generó el informe. **Servidores de recuperación**: el número total de servidores de recuperación en el momento en que se generó el informe. **IP públicas**: el número total de direcciones IP públicas (en el momento en que se generó el informe). **Total de puntos de cálculo consumidos**: el número total de puntos de cálculo consumidos durante el intervalo de tiempo especificado.
Servidores de recuperación ante desastres probados	El widget muestra información sobre los servidores protegidos por la recuperación ante desastres y comprobados con la conmutación por error de prueba. El widget muestra los siguientes parámetros: **Servidor protegido**: el número de servidores protegidos por la recuperación ante desastres (servidores que tienen al menos un servidor de recuperación) en el momento en que se generó el informe. **Probado**: el número de servidores protegidos por la recuperación ante desastres que se comprobaron con la conmutación por error de prueba durante el intervalo de tiempo seleccionado de entre todos los servidores protegidos por la recuperación ante desastres. **No probado**: el número de servidores protegidos por la recuperación ante desastres que no se comprobaron con la conmutación por error de prueba durante el intervalo de tiempo seleccionado de entre todos los servidores protegidos por la recuperación ante desastres. El widget también muestra el tamaño del almacenamiento de la recuperación ante desastres (en GB) en el momento en que se generó el informe. Es la suma del tamaño de las copias de seguridad de los servidores en la nube.
Servidores protegidos con recuperación ante desastres	El widget muestra información sobre los servidores protegidos por la recuperación ante desastres y los servidores que no están protegidos. El widget muestra los siguientes parámetros:

Widget	Descripción
	El número total de servidores registrados en el inquilino de cliente en el momento en que se generó el informe. **Protegido**: el número de servidores protegidos por la recuperación ante desastres (tienen al menos un servidor de recuperación y una copia de seguridad del servidor completa) de entre todos los servidores registrados en el momento en que se generó el informe. **Sin protección**: el número total de servidores sin protección de entre todos los servidores registrados en el momento en que se generó el informe.

Widget para la prevención de pérdida de datos

El siguiente tema proporciona más información sobre los dispositivos periféricos bloqueados de la sección **Prevención de pérdida de datos**.

El widget muestra el número total de dispositivos bloqueados por tipo de dispositivo para el intervalo de fechas especificado.

- Almacenamiento extraíble
- Extraíble cifrada
- Impresoras
- Portapapeles: incluye los tipos de dispositivo de captura del Portapapeles y la Captura de pantalla.
- Dispositivos móviles
- Bluetooth
- Unidades ópticas
- Unidades de disquetes
- USB: incluye los tipos de dispositivo de puerto USB y puerto USB redirigido.
- FireWire
- Dispositivos asignados
- Portapapeles redirigido: incluye los tipos de dispositivo Entrada de portapapeles redirigida y Salida de portapapeles redirigida.

El widget muestra los primeros siete tipos de dispositivo con el mayor número de dispositivos bloqueados y combina el resto de tipos de dispositivos en el tipo **Otros**.

Widgets de File Sync & Share

La siguiente tabla proporciona más información sobre los widgets de la sección **File Sync & Share**.

Widget	Descripción
Estadísticas de File Sync & Share	El widget muestra los siguientes parámetros: **Almacenamiento total en la nube utilizado**: el uso del almacenamiento total de todos los usuarios. **Usuarios finales**: el número total de usuarios finales. **Almacenamiento medio utilizado por usuario final**: el almacenamiento medio utilizado por usuario final. **Usuarios invitados**: el número total de usuarios invitados.
Uso del almacenamiento de File Sync & Share por los usuarios finales	El widget muestra el número total de usuarios finales de File Sync & Share que usan el almacenamiento en los siguientes intervalos: • 0-1 GB • 1-5 GB • 5-10 GB • 10-50 GB • 50-100 GB • 100-500 GB • 500-1 TB • Más de 1 TB

Widgets de certificación

La siguiente tabla proporciona más información sobre los widgets de la sección **Certificación**.

Widget	Descripción
Estadísticas de Cyber Notary	El widget muestra los siguientes parámetros de certificación: **Almacenamiento en la nube utilizado para certificación**: el tamaño total del almacenamiento utilizado para servicios de certificación. **Archivos certificados ante notario**: el número total de archivos certificados ante notario. **Documentos firmados electrónicamente**: el número total de documentos y archivos firmados electrónicamente.
Archivos certificados en usuarios finales	Muestra el número total de archivos certificados ante notario para todos los usuarios finales. Los usuarios se agrupan según el número de archivos certificados que tengan. • Hasta 10 archivos • 11-100 archivos • 101-500 archivos • 501-1000 archivos

Widget	Descripción
	• Más de 1000 archivos
Documentos firmados electrónicamente por los usuarios finales	El widget muestra el número total de documentos y archivos firmados electrónicamente para todos los usuarios finales. Los usuarios se agrupan según el número de documentos y archivos firmados electrónicamente que tengan. • Hasta 10 archivos • 11-100 archivos • 101-500 archivos • 501-1000 archivos • Más de 1000 archivos

Configuración del informe resumido ejecutivo

Puede actualizar los ajustes del informe que se configuraron al crear el informe resumido ejecutivo.

Para actualizar la configuración del informe resumido ejecutivo

1. En la consola de gestión, vaya a **Informes** > **Resumen ejecutivo**.
2. Haga clic en el nombre del informe resumido ejecutivo que desee actualizar.
3. Haga clic en **Configuración**.
4. Cambie los valores de los campos según sea necesario.
5. Haga clic en **Guardar**.

Crear un informe resumido ejecutivo

Puede crear un informe resumido ejecutivo, obtener la vista previa de su contenido, configurar los destinatarios y programar su envío automático.

Para crear un informe resumido ejecutivo

1. En la consola de gestión, vaya a **Informes** > **Resumen ejecutivo**.
2. Haga clic en **Crear informe resumido ejecutivo**.
3. En **Nombre del informe**, escriba el nombre.
4. Seleccione los destinatarios del informe.
   - Si desea enviarlo a todos los contactos y usuarios, seleccione **Enviar a todos los contactos y usuarios**.
   - Si desea enviar el informe a contactos y usuarios específicos
     a. Deseleccione **Enviar a todos los contactos y usuarios**.
     b. Haga clic en **Seleccionar contactos**.

c. Seleccione los contactos y usuarios específicos. Puede utilizar la Búsqueda para encontrar un contacto determinado fácilmente.
d. Haga clic en **Seleccionar**.

5. Seleccione el intervalo: **30 días** o **Este mes**
6. Seleccione el formato del archivo: **PDF**, **Excel**, o **Excel y PDF**.
7. Configure la programación.
   - Si desea enviar el informe a los destinatarios en una fecha y hora específicas:
     a. Habilite la opción **Programado**.
     b. Haga clic en el campo **Día del mes**, borre el campo Último día y haga clic en la fecha que desee establecer.
     c. En el campo **Hora**, introduzca la hora a la que desee enviarlo.
     d. Haga clic en **Aplicar**.
   - Si desea crear el informe sin enviarlo a los destinatarios, deshabilite la opción **Programado**.
8. Haga clic en **Guardar**.

Personalizar un informe resumido ejecutivo

Puede determinar qué información incluir en el informe resumido ejecutivo. Puede añadir o quitar secciones o widgets, cambiar el nombre a secciones, personalizar widgets y arrastrar y soltar widgets y secciones para cambiar el orden en que la información aparece en el informe.

Para añadir una sección

1. Haga clic en **Agregar elemento** > **Agregar sección**.
2. En la ventana **Agregar sección**, escriba un nombre de sección o utilice el nombre de sección predeterminado.
3. Haga clic en **Añadir al informe**.

Para cambiar el nombre de una sección

1. En la sección a la que quiere cambiarle al nombre, haga clic en **Editar**.
2. En la ventana **Editar sección**, escribe el nuevo nombre.
3. Haga clic en **Guardar**.

Para eliminar una sección

1. En la sección que quiere eliminar, haga clic en **Eliminar sección**.
2. En la ventana de confirmación **Eliminar sección**, haga clic en **Eliminar**.

Para añadir un widget con configuración predeterminada a una sección

1. En la sección a la que quiere añadir el widget, haga clic en **Añadir widget**.
2. En la ventana **Añadir widget**, haga clic en el widget que quiera añadir.

Para añadir un widget personalizado a una sección

1. En la sección a la que quiere añadir el widget, haga clic en **Añadir widget**.
2. En la ventana **Añadir widget**, busque el widget que quiera añadir y haga clic en **Personalizar**.
3. Configure los campos según sea necesario.
4. Haga clic en **Añadir widget**.

Para añadir un widget con configuración predeterminada al informe

1. Haga clic en **Agregar elemento** > **Agregar widget**.
2. En la ventana **Añadir widget**, haga clic en el widget que quiera añadir.

Para añadir un widget personalizado al informe

1. Haga clic en **Añadir widget**.
2. En la ventana **Añadir widget**, busque el widget que quiera añadir y haga clic en **Personalizar**.
3. Configure los campos según sea necesario.
4. Haga clic en **Añadir widget**.

Para restablecer la configuración predeterminada de un widget

1. Haga clic en **Editar** en el widget que quiera personalizar.
2. Haga clic en **Restablecer valores predeterminados**.
3. Haga clic en **Listo**.

Pasos para personalizar un widget

1. Haga clic en **Editar** en el widget que quiera personalizar.
2. Edite los campos según sea necesario.
3. Haga clic en **Listo**.

Enviar informes resumidos ejecutivos

Puede enviar un informe resumido ejecutivo bajo demanda. En este caso, no se tiene en cuenta el ajuste **Programado** y el informe se envía inmediatamente. Cuando envía el informe, el sistema utiliza los valores de los destinatarios, el intervalo y el formato de archivo que están configurados en **Configuración**. Puede modificar esta configuración manualmente antes de enviar el informe. Para obtener más información, consulte "Configuración del informe resumido ejecutivo" (p. 80).

Pasos para enviar un informe resumido ejecutivo

1. En el portal de gestión, vaya a **Informes** > **Resumen ejecutivo**.
2. Haga clic en el nombre del informe resumido ejecutivo que desee enviar.
3. Haga clic en **Enviar ahora**.
   El sistema envía el informe resumido ejecutivo a los destinatarios seleccionados.

Zonas horarias de los informes

Las zonas horarias que se utilizan en los informes varían en función del tipo de informe. En la siguiente tabla encontrará información que le servirá como referencia.

Ubicación y tipo de informe	Zona horaria utilizado en el informe
Portal de administración > Información general > Operaciones (widgets)	La hora de la generación del informe es la de la zona horaria del equipo en el que se está ejecutando el navegador.
Portal de administración > Información general > Operaciones (exportado en PDF o xslx)	• La marca de fecha y hora del informe exportado es la de la zona horaria del equipo que se utilizó para exportar informe. • La zona horaria de las actividades que aparecen en el informe es UTC.
Portal de administración > Informes > Uso > Informes planificados	• El informe se genera a las 23:59:59 UTC el primer día del mes. • El informe se envía el segundo día del mes.
Portal de administración > Informes > Uso > Informes personalizados	La zona horaria y la fecha del informe es UTC.
Portal de administración > Informes > Operaciones (widgets)	• La hora de la generación del informe es la de la zona horaria del equipo en el que se está ejecutando el navegador. • La zona horaria de las actividades que aparecen en el informe es UTC.
Portal de administración > Informes > Operaciones (exportado en PDF o xslx)	• La marca de fecha y hora del informe exportado es la de la zona horaria del equipo que se utilizó para exportar informe. • La zona horaria de las actividades que aparecen en el informe es UTC.
Portal de administración > Informes > Operaciones (entrega planificada)	• La zona horaria de entrega del informe es UTC. • La zona horaria de las actividades que aparecen en el informe es UTC.
Portal de administración > Usuarios > Resumen diario de alertas activas	• Este informe se envía una vez al día entre las 10:00 y las 23:59 UTC. La hora a la que se envía el informe depende de la carga de trabajo del centro de datos. • La zona horaria de las actividades que aparecen en el informe es

	UTC.
Portal de administración > Usuarios > notificaciones de estado de ciberprotección	• Este informe se envía cuando finaliza una actividad. **Nota** En función de la carga de trabajo del centro de datos, es posible que algunos informes se entreguen con retraso. • La zona horaria de la actividad del informe es UTC.

Datos informados según el tipo de widget

Según el rango de datos que muestran, hay dos tipos de widgets en el panel de control:

- Widgets que muestran los datos reales en el momento de la navegación o la generación de informes.
- Widgets que muestran datos históricos.

Cuando configure un rango de fechas en los ajustes del informe para volcar datos para un periodo determinado, el rango de tiempo seleccionado se aplicará solo a los widgets que muestran datos históricos. El parámetro del rango de tiempo no se aplica a los widgets que muestran los datos reales en el momento de la navegación.

La siguiente tabla enumera los widgets disponibles y sus rangos de datos.

Nombre del widget	Datos mostrados en el widget e informes
#CyberFit Score por equipo	Reales
5 últimas alertas	Reales
Detalles de las alertas activas	Reales
Resumen de alertas activas	Reales
Actividades	Históricos
Lista de actividades	Históricos
Historial de alertas	Históricos
Análisis antimalware de copias de seguridad	Históricos
Análisis antimalware de archivos	Históricos
Detalles del análisis de copias de seguridad (amenazas)	Históricos
Estado de la copia de seguridad	Históricos: en columnas **Ejecuciones totales** y **Número de ejecuciones correctas** Reales: en el resto de columnas

Uso del almacenamiento de copia de seguridad	Históricos
Dispositivos periféricos bloqueados	Históricos
URL bloqueadas	Reales
Aplicaciones de Cloud	Reales
Estado de la protección de las cargas de trabajo de la nube	Reales
Cyber protection	Reales
Resumen de ciberprotección	Históricos
Mapa de protección de datos	Históricos
Dispositivos	Reales
Servidores de recuperación ante desastres probados	Históricos
Estadísticas de recuperación ante desastres	Históricos
Equipos detectados	Reales
Resumen del estado del disco	Reales
Estado del disco	Reales
Estado del disco por dispositivos físicos	Reales
Documentos firmados electrónicamente por los usuarios finales	Reales
Vulnerabilidades existentes	Históricos
Estadísticas de File Sync & Share	Reales
Uso del almacenamiento de File Sync & Share por los usuarios finales	Reales
Cambios del hardware	Históricos
Detalles del hardware	Reales
Inventario de hardware	Reales
Resumen del historial de alertas	Históricos
Resumen de ubicaciones	Reales
Actualizaciones que faltan por categoría	Reales
Sin protección	Reales

Archivos certificados en usuarios finales	Reales
Estadísticas de Notary	Reales
Historial de instalación de parches	Históricos
Estado de instalación del parche	Históricos
Resumen de la instalación del parche	Históricos
Vulnerabilidades solucionadas	Históricos
Parches instalados	Históricos
Estado de la protección	Reales
Elementos afectados recientemente	Históricos
Sesiones remotas	Históricos
Gráfico de quemado de incidentes de seguridad	Históricos
Tiempo medio de reparación de incidentes de seguridad	Históricos
Servidores protegidos con recuperación ante desastres	Reales
Inventario de software	Reales
Información general del software	Históricos
Estado de la amenaza	Reales
Amenazas detectadas por la tecnología de protección	Históricos
Distribución de los principales incidentes por carga de trabajo	Reales
Equipos vulnerables	Reales
Estado de la red de las cargas de trabajo	Reales
Cargas de trabajo en la copia de seguridad	Históricos
Estado de la protección de las cargas de trabajo	Reales

Integraciones

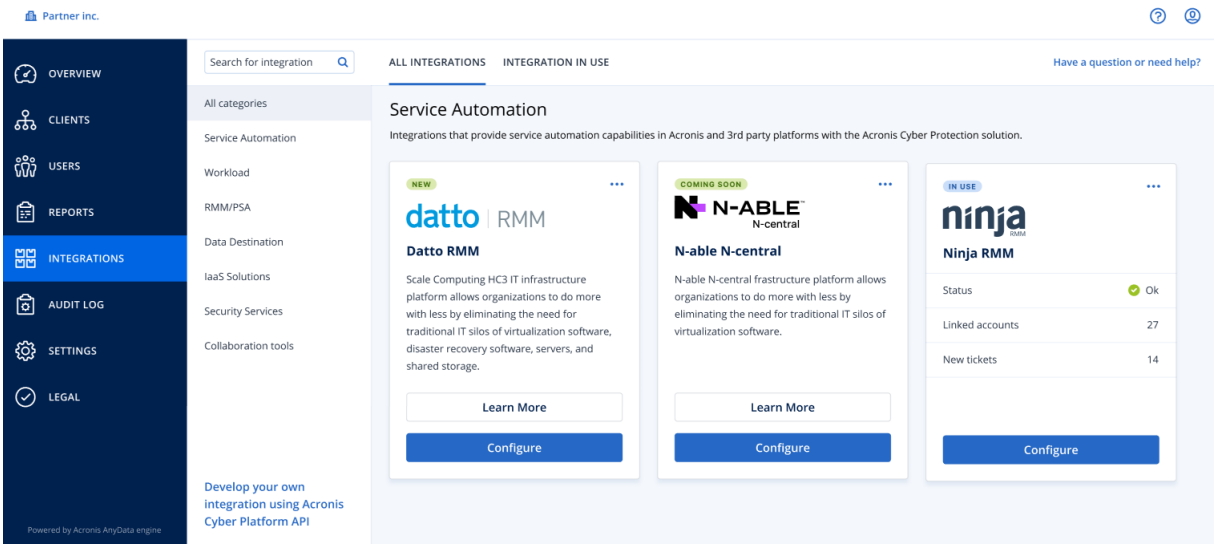
Catálogo de integraciones

Esta página sirve como lugar global donde se registran y actualizan todas las aplicaciones de integración.
Desde aquí es posible añadir nuevas integraciones o modificar las existentes.

Nota
Solo los usuarios con un rol de **Administrador de la empresa** tienen permiso para cambiar la configuración de la integración.

Todas las integraciones

La pestaña **Todas las integraciones** muestra una lista de todas las integraciones disponibles actualmente, ordenadas como mosaicos uno al lado del otro.



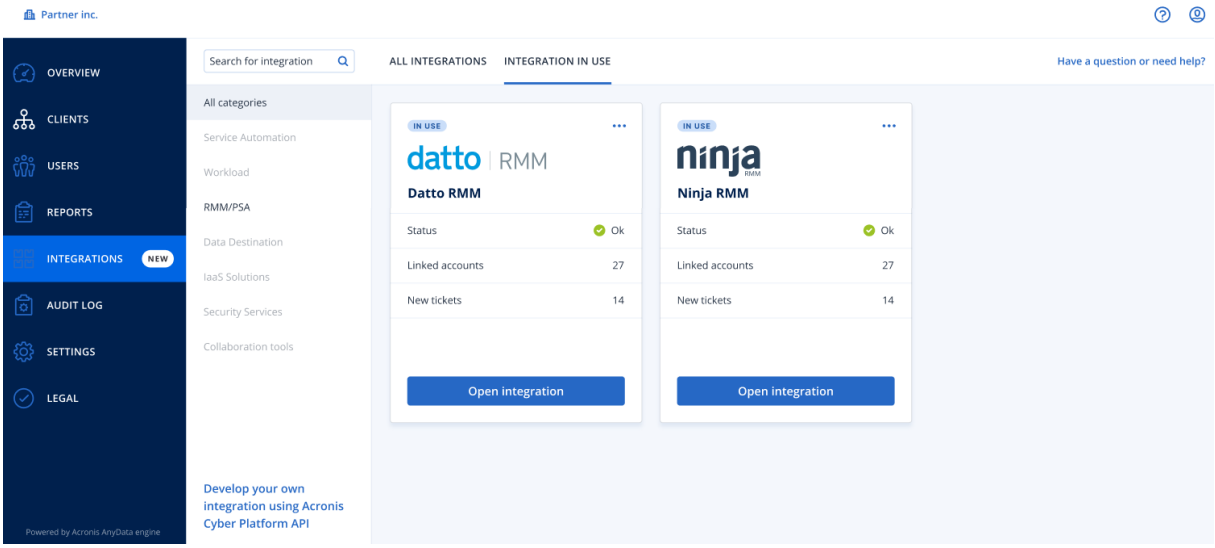
Cada mosaico muestra una breve descripción del producto y dos opciones adicionales:

- **Más información**: haga clic en este botón para obtener más detalles sobre la integración concreta:
  - **Características de integración**
  - **Enlaces de documentación**
  - **Contactos de soporte técnico**
- **Configurar**: utilice esta opción para editar algunos de los ajustes de integración.

Los mosaicos que representan integraciones inactivas aparecen en gris y deshabilitados, y pueden tener una etiqueta "**próximamente**".

Integraciones en uso

La pestaña **Integración en uso** muestra una lista de todas las integraciones que están actualmente activas, cada una de ellas acompañada de información general.



Haga clic en **Abrir integración** para acceder directamente a la aplicación correspondiente.

A la izquierda, hay una lista de categorías de integración, en la que todas las aplicaciones existentes se clasifican en determinados grupos, como automatización de servicios, carga de trabajo, RMM/PSA, etc. Al hacer clic en cada categoría, se mostrarán las integraciones que pertenecen a ese grupo en concreto. La categoría que esté viendo actualmente aparece resaltada.

Utilice la opción **Buscar** para realizar consultas y buscar las integraciones que desee.

Puede filtrar la lista de integraciones por categoría y etiqueta. Las etiquetas están ordenadas alfabéticamente. Si no se encuentran resultados, amplíe la búsqueda para incluir más categorías.

Para deshabilitar una aplicación, haga clic en el icono de puntos suspensivos (...) en la esquina superior derecha del mosaico y seleccione **Desactivar**.

También está disponible un enlace a la documentación de la API de Acronis si está interesado en desarrollar su propia integración.

Limitación del acceso a la interfaz web

Si quiere limitar el acceso a la interfaz web, especifique una lista de direcciones IP desde las que los usuarios pueden iniciar sesión.

La restricción también se aplica al acceso al portal de gestión a través de la API.

Esta restricción solo se aplica al nivel donde está configurado. Esta restricción *no* se aplica a los miembros de las unidades secundarias.

Para limitar el acceso a la interfaz web

1. Inicie sesión en el portal de gestión.
2. Vaya hasta la unidad en la que desee limitar el acceso.
3. Haga clic en **Configuración** > **Seguridad**.
4. Seleccione la casilla de verificación **Habilitar control de inicio de sesión**.
5. En **Direcciones IP permitidas**, indique las direcciones IP que quiere permitir.
   Puede escribir cualquiera de los parámetros siguientes separados por punto y coma.
   - Direcciones IP, por ejemplo: 192.0.2.0
   - Rangos de IP, por ejemplo: 192.0.2.0-192.0.2.255
   - Subredes, por ejemplo: 192.0.2.0/24
6. Haga clic en **Guardar**.

Limitación de acceso a su empresa

Los administradores de la compañía pueden limitar el acceso a la compañía para los administradores de nivel superior.

Si el acceso a la compañía está limitado, los administradores de nivel superior solo pueden modificar las propiedades de la compañía. No pueden ver ni las cuentas de usuario ni las unidades secundarias en ningún caso.

Para limitar el acceso a la compañía

1. Inicie sesión en el portal de gestión.
2. Haga clic en **Configuración** > **Seguridad**.
3. Deshabilite la opción **Acceso al soporte técnico**.
4. Haga clic en **Guardar**.

Gestión de clientes API

Se pueden integrar sistemas de terceros con Cyber Protect Cloud mediante interfaces de programación de aplicaciones (API). El acceso a estas API se habilita mediante clientes API, una parte integral del marco de autorización OAuth 2.0 de la plataforma.

¿Qué es un cliente API?

Un cliente API es una cuenta especial de una plataforma cuya función es representar a un sistema de terceros que se tiene que autenticar y autorizar para acceder a los datos de las API de la plataforma y sus servicios.

El acceso del cliente está limitado a un inquilino, en el que un administrador crea al cliente y a sus subinquilinos.

Al crearse, el cliente hereda los roles de servicio de la cuenta administrador, que no se pueden cambiar posteriormente. El hecho de que cambien los roles de la cuenta de administrador o que se deshabiliten no afecta al cliente.

Las credenciales del cliente están formadas por el identificador único (ID) y un valor secreto. Las credenciales no caducan y no se pueden utilizar para iniciar sesión en el portal de administración ni en ninguna consola de servicio. El valor secreto se puede restablecer.

No es posible habilitar la autenticación de doble factor para el cliente.

Proceso de integración habitual

1. Un administrador crea un cliente API en un inquilino que gestionará un sistema de terceros.
2. El administrador habilita el flujo de credenciales del cliente OAuth 2.0 en el sistema de terceros.
   Según este flujo, antes de acceder al inquilino y sus servicios a través de la API, el sistema debe usar la API de autorización para enviar las credenciales del cliente creado a la plataforma. La plataforma genera y devuelve un token de seguridad, la única cadena críptica asignada a este cliente concreto. A continuación, el sistema debe añadir este token a todas las solicitudes a la API.
   Un token de seguridad acaba con la necesidad de mandar las credenciales del cliente con las solicitudes a la API. Para obtener un nivel mayor de seguridad, el token expira en dos horas. Cuando pase este tiempo, todas las solicitudes a la API con el toque expirado fallarán y el sistema tendrá que solicitar uno nuevo a la plataforma.

Para obtener más información sobre cómo usar las API de plataforma y autorización, consulte la guía del desarrollador en https://developer.acronis.com/doc/account-management/v2/guide/index.

Creación de un cliente API

1. Inicie sesión en el portal de gestión.
2. Haga clic en **Configuración** > **Clientes API** > **Crear cliente API**.
3. Introduzca un nombre para el cliente API.
4. Haga clic en **Siguiente**.
   De forma predeterminada, el cliente API se crea con el estado **Habilitado**.
5. Copie y guarde el ID, el valor secreto del cliente y la URL del centro de datos. Los necesitará para habilitar el flujo de credenciales del cliente OAuth 2.0 en el sistema de terceros.

   Importante
   Por motivos de seguridad, la clave solo se muestra una vez. No hay ninguna forma de recuperar este valor si lo pierde, la única opción es restablecerlo.

6. Haga clic en **Listo**.

Restablecimiento del valor secreto de un cliente API

1. Inicie sesión en el portal de gestión.
2. Haga clic en **Configuración** > **Clientes API**.
3. En la lista, busque el cliente que necesite.
4. Haga clic en y luego en **Restablecer secreto**.
5. Para confirmar su decisión, haga clic en **Siguiente**.
   Se generará un nuevo valor secreto. El ID del cliente y la URL del centro de datos no cambiarán.
   Todos los tokens de seguridad asignados a este cliente expirarán inmediatamente y fallarán las solicitudes a la API con estos clientes.
6. Copie y guarde el nuevo valor secreto del cliente.

   Importante
   Por motivos de seguridad, la clave solo se muestra una vez. No hay ninguna forma de recuperar este valor si lo pierde, la única opción es restablecerlo.

7. Haga clic en **Listo**.

Deshabilitación de un cliente API

1. Inicie sesión en el portal de gestión.
2. Haga clic en **Configuración** > **Clientes API**.
3. En la lista, busque el cliente que necesite.
4. Haga clic en y en **Deshabilitar**.
5. Confirme su decisión.
   El estado del cliente cambiará a **Deshabilitado**.
   Las solicitudes a la API con tokens de seguridad que estén asignadas a este cliente fallarán, pero los tokens no caducarán inmediatamente. El hecho de deshabilitar el cliente no afecta a la fecha de caducidad de los tokens.
   El cliente se podrá volver a habilitar en cualquier momento.

Habilitación de un cliente API deshabilitado

1. Inicie sesión en el portal de gestión.
2. Haga clic en **Configuración** > **Clientes API**.
3. En la lista, busque el cliente que necesite.
4. Haga clic en y en **Habilitar**.
   El estado del cliente cambiará a **Activo**.

Las solicitudes a la API con tokens de seguridad que estén asignadas a este cliente se llevarán a cabo perfectamente si los tokens no han expirado todavía.

Eliminación de un cliente API

1. Inicie sesión en el portal de gestión.
2. Haga clic en **Configuración** > **Clientes API**.
3. En la lista, busque el cliente que necesite.
4. Haga clic en y en **Eliminar**.
5. Confirme su decisión.

   Todos los tokens de seguridad asignados a este cliente expirarán inmediatamente y fallarán las solicitudes a la API con estos clientes.

Importante
No hay manera de recuperar un cliente eliminado.

Índice

E

F

G

H

I

L

M

N

P

Z