

Servicio de certificación

24.03

Contenido

Acerca del servicio de certificación	3
Cómo funciona la certificación	3
Roles de usuario	3
Limitaciones	4
Navegadores web compatibles	4
Utilización del servicio de certificación	5
Activación de la cuenta	5
Acceso a la interfaz web del servicio de certificación	5
Utilizar el servicio de certificación como usuario de certificación	5
Certificación de archivos	5
Verificación de la autenticidad de los archivos	8
Firmado de archivos	10
Plantillas de documento	13
Utilización del servicio de certificación como administrador de certificación	18
Administración del servicio de certificación	20
Gestión de claves de API	20
Administración de cuentas de usuario y cuotas	21
Cuotas	21
Notificaciones	22
Informes de uso	22
Índice	23

Acerca del servicio de certificación

El servicio de certificación es una solución basada en la tecnología de cadena de bloques que le permite hacer lo siguiente:

- Certificar archivos ante notario.
- Comprobar si un archivo certificado ante notario (o su copia) es auténtico y no se ha modificado desde su certificación.
- Enviar un archivo a varias personas para que lo firmen electrónicamente y, a continuación, validar el certificado de firma.

Este servicio está disponible a través de una interfaz web denominada "consola de certificación".

Cómo funciona la certificación

Para certificar un archivo ante notario, debe cargarlo en el almacenamiento en la nube. Después de cargar el archivo, el servicio de certificación calcula una huella digital (conocida como "código hash") de este. El código hash es único para cada archivo.

Nota

La interfaz de programación de aplicaciones (API) del servicio de certificación le permite certificar un archivo ante notario sin tener que cargarlo en el almacenamiento en el cloud. En su lugar, se puede utilizar el hash del archivo que se ha generado previamente. Para obtener más información acerca del uso de la API, consulte "[Gestión de claves de API](#)".

A continuación, el servicio de certificación envía el código hash a la base de datos basada en la tecnología de cadena de bloques de Ethereum. Dicha base de datos garantiza que el código hash permanezca inalterado.

Para comprobar la autenticidad de un archivo, el servicio calcula su código hash y lo compara con el código hash almacenado en la base de datos. Si los códigos coinciden, queda garantizado que se trata del mismo archivo y que no se ha modificado.

Roles de usuario

Existen dos roles de usuario en el servicio de certificación: el administrador de certificación y el usuario de certificación.

Tanto los administradores como los usuarios tienen acceso a todas las funciones del servicio de certificación en la consola de certificación.

Todos los usuarios tienen acceso solo a sus propias plantillas, archivos certificados ante notario y firmados electrónicamente.

Los administradores tienen derechos elevados para ver y trabajar con las plantillas y los archivos certificados ante notario y firmados electrónicamente que pertenecen al resto de usuarios o administradores del inquilino de cliente. Los administradores y usuarios pueden gestionar las claves

de API del servicio de certificación y utilizar la API de certificación. Los administradores y usuarios solo tienen acceso a sus propias claves de API.

Asimismo, se puede asignar a un administrador del servicio de certificación la función de administrador de empresa. Esta función da acceso al portal de gestión, donde el administrador puede gestionar cuentas de usuario, cuotas, notificaciones e informes.

Limitaciones

- Los archivos que ocupen más de 1 GB no se pueden certificar ante notario a través de la consola de certificación. Esto solo es posible a través de la API de servicios de certificación. Para ello, se envía un hash previamente calculado de un archivo al servicio de certificación.
- Los archivos que ocupen más de 1 GB no se pueden firmar a través de la consola de certificación. Esto solo es posible a través de la API del servicio de certificación. Para ello, se envía a dicho servicio un enlace al archivo.

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.

Utilización del servicio de certificación

Activación de la cuenta

Tras registrarse en el servicio, recibirá un correo electrónico con la siguiente información:

- **Un enlace de activación de cuenta.** Haga clic en el enlace y establezca la contraseña de la cuenta. Recuerde su usuario, el cual aparece en la página de activación de la cuenta.
- **Un enlace a la página de inicio de sesión a la consola de certificación.** Este enlace le permitirá acceder a la consola en el futuro. El usuario y la contraseña son los mismos que en el paso anterior.

Acceso a la interfaz web del servicio de certificación


Puede iniciar sesión en el servicio de certificación si ha activado su cuenta.

Cómo iniciar sesión en el servicio de certificación

1. Vaya a la página de inicio de sesión del servicio de certificación. La dirección de la página de inicio de sesión se incluye en el correo electrónico de activación.
2. Escriba el usuario y luego haga clic en **Continuar**.
3. Escriba la contraseña y luego haga clic en **Iniciar sesión**.
4. Si tiene la función de administrador de empresa, haga clic en **Certificación**.
Los usuarios que no tienen asignada la función de administrador de empresa inician sesión directamente en la consola de certificación.

Puede cambiar el idioma de la interfaz web si hace clic en el icono de la cuenta que hay en la esquina superior derecha.

Si **Notary** no es el único servicio al que está suscrito, puede cambiar de un servicio a otro con el

icono  de la esquina superior derecha. Los administradores de empresa también pueden usar este icono para pasar al portal de gestión.

Utilizar el servicio de certificación como usuario de certificación

Los usuarios de certificación tienen acceso solo a sus propias plantillas, archivos certificados ante notario y firmados electrónicamente.

Certificación de archivos

Cómo certificar archivos ante notario

1. Haga clic en **Archivos certificados ante notario**.
2. Si no hay archivos certificados ante notario, haga clic en **Examinar**. Haga clic en **Añadir archivos** y, a continuación, haga clic en **Examinar**.
3. Seleccione los archivos que desee certificar ante notario.
Cuando seleccione un archivo, el software empezará a cargarlo en el almacenamiento en la nube.
4. Cuando todos los archivos se hayan cargado, haga clic en **Certificar ante notario**.
El software calculará un código hash para cada archivo. El estado de los archivos cambiará a **En progreso**. El uso de la cuota de **Notarizaciones** se incrementará con el número de archivos.
5. Espere hasta que el estado de cada archivo pase de **En progreso** a **Certificado ante notario**.
El proceso de certificación puede durar hasta 70 minutos. Para reducir el coste de cada certificación, el servicio recopila los hash durante una hora, luego construye un árbol de hash basado en ellos y envía la raíz del árbol de hash al libro mayor de blockchain. A continuación, el servicio de certificación espera a que la transacción se confirme en el libro mayor de blockchain y, después, modifica el estado de los archivos a **Certificado ante notario**. Recibirá una notificación por correo electrónico cuando el estado del archivo pase a ser **Certificado ante notario**.

Nota

Si no se certifica un archivo 24 horas después de cargarlo, su estado pasará de **En progreso** a **Certificación pendiente** y recibirá un aviso por correo electrónico.

Autenticación certificación

Una vez acabada la certificación, el servicio creará una autenticación notarial para cada archivo. Esta autenticación es una prueba irrefutable de que el archivo se ha certificado ante notario en un determinado momento. La autenticación contiene:

- Información acerca de la certificación (nombre de archivo, hash, tamaño, marca de fecha y hora de la notarización, solicitante, GUID del solicitante, firmante, ID de la transacción de blockchain e ID del certificado)
- Instrucciones sobre cómo verificar el archivo manualmente sin utilizar el servicio de certificación

Nota


Tenga en cuenta que sus datos personales, como la dirección de correo electrónico o la dirección IP, se almacenarán en la pista de auditoría y serán accesibles para todos los firmantes.

Operaciones con archivos certificados ante notario

Cómo descargar un archivo del almacenamiento en la nube

1. Haga clic en **Archivos certificados ante notario**.
2. Busque el archivo en la lista.

Los archivos se pueden filtrar por estado y ordenar por nombre, estado, certificación y fechas de carga. También puede hacer una búsqueda.

3. Haga clic en  o en el nombre del archivo. Después, haga clic en **Descargar**.

Cómo visualizar la autenticación notarial de un archivo

1. Haga clic en **Archivos certificados ante notario**.
2. Busque el archivo en la lista. Las autenticaciones de certificación solo están disponibles en los archivos que tienen el estado **Certificado ante notario**.
Los archivos se pueden filtrar por estado y ordenar por nombre, estado, certificación y fechas de carga. También puede hacer una búsqueda.
3. Haga clic en el nombre del archivo.
4. Haga clic en **Ver y descargar certificado** para visualizar el certificado en una nueva pestaña.


Nota

Si hace clic en el icono Copiar al portapapeles que corresponda, podrá copiar los valores de **hash de archivo (SHA-256)**, **ID del certificado** o **RECIBO DE LA CADENA DE BLOQUES** de la autenticación notarial.

Cómo descargar la autenticación notarial de un archivo

1. Haga clic en **Archivos certificados ante notario**.
2. Busque el archivo en la lista. Las autenticaciones de certificación solo están disponibles en los archivos que tienen el estado **Certificado ante notario**.
Los archivos se pueden filtrar por estado y ordenar por nombre, estado, certificación y fechas de carga. También puede hacer una búsqueda.
3. Haga clic en el nombre del archivo.
4. Haga clic en **Ver y descargar certificado** para visualizar el certificado en una nueva pestaña.
5. En la nueva pestaña, haga clic en **Descargar certificado**.

Cómo eliminar un archivo del almacenamiento en la nube

1. Haga clic en **Archivos certificados ante notario**.
2. Busque el archivo en la lista.
Los archivos se pueden filtrar por estado y ordenar por nombre, estado, certificación y fechas de carga. También puede hacer una búsqueda.
3. Haga clic en  o en el nombre del archivo. Después, haga clic en **Eliminar**.
Si se trata de un archivo certificado ante notario, su estado no se alterará. Se recomienda que guarde la autenticación notarial o el enlace directo a ella antes de confirmar la eliminación.

Importante

Si la certificación está en progreso, no se cancelará. Sin embargo, no se podrá ver ni descargar la autenticación notarial.

4. Haga clic en **Eliminar** de nuevo para confirmar su decisión.

Verificación de la autenticidad de los archivos

Se puede verificar la autenticidad de un archivo cargándolo al almacenamiento en la nube o utilizando el recibo de cadena de bloques de la autenticación notarial del archivo.

Los archivos que se cargan para su verificación no utilizan la cuota de **Almacenamiento de Notary**, sino que se eliminan del almacenamiento en la nube una vez completado el proceso de verificación.

Cómo verificar la autenticidad de un archivo cargándolo al almacenamiento en la nube

1. Acceda a la autenticación notarial tal y como se describe en el apartado "[Cómo visualizar la autenticación notarial de un archivo](#)".
2. Encuentre el ID del certificado y cópielo.
3. En la consola de certificación, haga clic en **Verificación**.
4. Haga clic en **Examinar** y, a continuación, seleccione el archivo cuya autenticidad desee verificar. Puede seleccionar varios archivos.
Cuando seleccione un archivo, el software empezará a cargarlo en el almacenamiento en la nube.
5. Especifique el ID del certificado del archivo para confirmar su derecho a la verificación del archivo.
6. Haga clic en **Verificar**.
7. El software muestra los informes de verificación de los archivos seleccionados.
 - Si el archivo es auténtico, su estado es **Certificado ante notario**.
 - Si, por el contrario, el archivo no es auténtico, su estado es **Sin certificar ante notario**.
 - Si el archivo aún está en proceso de certificación, su estado es **En progreso**.

Cómo verificar un archivo mediante un recibo de cadena de bloques

1. Acceda a la autenticación notarial tal y como se describe en el apartado "[Cómo visualizar la autenticación notarial de un archivo](#)".
2. Busque la sección **recibo de cadena de bloques** y copie lo siguiente, incluidos los corchetes:

```
{
  "key": "filename.pdf",
  "eTag": "52bf7a18744b384afba39f3646d8e245...",
  "size": 1267387,
  "sequencer": "B56C3FE5ED984F5337"
}
```


Estas cadenas presentan el nombre del archivo, el hash SHA-256, el tamaño en bytes y el número de transacción de cadena de bloques.

3. En la consola de certificación, haga clic en **Verificación**.
4. Haga clic en **Verificar mediante el uso del recibo de la cadena de bloques**.
5. Pegue los contenidos que copió de la sección **Recibo de cadena de bloques** en el campo en blanco.
6. Haga clic en **Verificar**.
7. El software muestra el informe de verificación.
 - Si el archivo es auténtico, su estado es **Certificado ante notario**.
 - Si, por el contrario, el archivo no es auténtico o no se ha certificado, su estado es **Sin certificar ante notario**.
 - Si el archivo aún está en proceso de certificación, su estado es **En progreso**.

Para verificar un archivo mediante un hash del archivo:

1. Acceda a la autenticación notarial tal y como se describe en el apartado "[Cómo visualizar la autenticación notarial de un archivo](#)".
2. Encuentre el ID del certificado y el hash del archivo y cópielos.
3. En la consola de certificación, haga clic en **Verificación**.
4. Haga clic en **Verificar mediante el uso del hash del archivo**.
5. Especifique el hash del archivo.
6. Especifique el ID del certificado del archivo para confirmar su derecho a la verificación del archivo.
7. Haga clic en **Verificar**.
8. El software muestra el informe de verificación.
 - Si el archivo es auténtico, su estado es **Certificado ante notario**.
 - Si, por el contrario, el archivo no es auténtico o no se ha certificado, su estado es **Sin certificar ante notario**.
 - Si el archivo aún está en proceso de certificación, su estado es **En progreso**.

Página pública de verificación

Existe también una página pública de verificación en la que un usuario puede verificar la autenticidad de un archivo mediante uno de los tres métodos siguientes:

- Con la carga de un archivo y el ID del certificado
- A través de la especificación del hash y el ID del certificado de un archivo
- Al proporcionar un recibo de cadena de bloques y el ID del certificado

Firmado de archivos

El servicio de certificación le permite enviar un archivo a varias personas para que lo firmen electrónicamente o hacerlo por su cuenta como firmante único.

Para que se firme un archivo, debe cargarlo en el almacenamiento en la nube o crearlo desde una plantilla.

En aquellos archivos que no se pueden convertir a formato de archivo .pdf, se pueden incrustar como imágenes en el documento firmado la firma o las iniciales de los firmantes escritas a mano o convertidas en texto. En ese caso, el contenido del archivo firmado se guarda con las firmas electrónicas incrustadas en el archivo .pdf del certificado de firma y ese archivo se certifica ante notario posteriormente mediante el servicio de certificación. Esta función se admite para los siguientes formatos de archivo: .txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx y .pdf.

Puede usar las firmas electrónicas incrustadas para firmar electrónicamente los siguientes tipos de documentos:

- Contratos de concesión o de alquiler
- Contratos de ventas
- Contratos de adquisición de activos
- Contratos de préstamos
- Formularios de permisos
- Documentos financieros
- Documentos del seguro
- Exenciones de responsabilidad
- Documentos de salud
- Documentos de investigación
- Certificados de autenticidad del producto
- Acuerdos de confidencialidad
- Cartas de oferta
- Acuerdos de confidencialidad
- Acuerdos de contratista independiente

Para los archivos que no se pueden convertir a formato .pdf, una vez que se haya firmado el archivo, el servicio de certificación generará un certificado de firma que contenga una recopilación de las firmas. A continuación, el certificado quedará autenticado por parte del servicio de certificación ante notario. Los archivos firmados no están certificados ante notario.

Pasos para firmar un archivo como el único firmante

Puede cargar un archivo y firmarlo electrónicamente como único firmante.

Cómo cargar un archivo y firmarlo electrónicamente como único firmante

1. Haga clic en **Archivos firmados**.
2. [Opcional] Si desea añadir un nuevo archivo para firmarlo, haga clic en **Examinar** o en **Añadir archivo** y, a continuación, en **Examinar**.
3. Seleccione el archivo que tiene que firmar.
Cuando seleccione un archivo, el software empezará a cargarlo en el almacenamiento en la nube.
4. En el cuadro de diálogo **Añadir firmantes**, seleccione **Soy el único firmante** y luego haga clic en **Siguiente**.
5. En el cuadro de diálogo **Añadir campos al documento**, arrastre y suelte los campos que quiera añadir al documento.
6. Haga clic en **Previsualizar y enviar**.
7. Previsualice el documento y haga clic en **Enviar**.
El documento aparece en la lista Archivos firmados con el estado **Esperándome**.
8. En la pestaña **Archivos**, haga clic en el documento y, después, en **Firmar**.
9. En el cuadro de diálogo **Escriba su nombre, iniciales y firma electrónica**, seleccione el método que quiere usar para firmar el archivo.
 - **Firma electrónica e iniciales recomendadas:** la firma electrónica y las iniciales se generan automáticamente. Se pueden modificar manualmente si fuera necesario.
 - **Firma electrónica e iniciales manuscritas:** usted dibuja su firma y sus iniciales en los campos correspondientes y se incluyen como imágenes en el documento firmado.

Nota

Esta opción se admite para los siguientes formatos de archivo: .txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx y .pdf.

10. Seleccione la casilla de verificación **He leído y acepto** y haga clic en **Siguiente**.
11. En el cuadro de diálogo **Firmar documento**, haga clic en el campo **Firma electrónica** para completarlo con su firma electrónica.
12. Haga clic en **Previsualizar y firmar**.
13. Previsualice el documento y haga clic en **Firmar**.
El archivo firmado se guarda como formato de archivo .pdf.
14. Cuando el proceso haya terminado, seleccione el archivo firmado y haga clic en la pestaña **Certificado de firma electrónica** y, a continuación, en **Certificado de firma electrónica** para descargar un documento PDF que contiene:
 - La sección **Certificado de firma electrónica** con una recopilación de todas las firmas.
 - La sección **Pista de auditoría** con un historial de actividades: cuándo se envió la invitación a los firmantes, cuándo firmó el archivo cada firmante y otros datos.

15. Haga clic en **Ver y descargar certificado** y, a continuación, en **Ver y descargar certificado** para descargar la autenticación notarial del certificado de firma electrónica. Una vez terminado el proceso de firma, la autenticación notarial estará disponible en un plazo de 70 minutos.

Enviar un archivo para que lo firmen varias personas

Puede cargar un archivo y enviarlo para que lo firmen varias personas electrónicamente.

Pasos para enviar un archivo para que lo firmen varias personas

1. Haga clic en **Archivos firmados**.
2. Si no hay archivos firmados, haga clic en **Examinar**. De lo contrario, haga clic en **Añadir archivo** y a continuación en **Examinar**.
3. Seleccione el archivo que tiene que firmar.
Cuando seleccione un archivo, el software empezará a cargarlo en el almacenamiento en la nube.
4. Haga clic en **Añadir firmantes** en el cuadro de diálogo del mismo nombre y, a continuación, escriba sus direcciones de correo electrónico. Repita este paso para cada firmante que quiera añadir.

Importante

No es posible añadir ni eliminar firmantes una vez enviadas las invitaciones. Para eliminar a un firmante, haga clic en el icono de cubo de basura correspondiente. Asegúrese de que la lista de firmantes esté completa antes de proceder al siguiente paso.

5. Haga clic en **Siguiente**.
6. En el cuadro de diálogo **Añadir campos al documento**, añada los campos personalizados y de firmante que correspondan.
7. Haga clic en **Previsualizar y enviar**.
8. Previsualice el documento y haga clic en **Enviar** para enviar las invitaciones a los firmantes.
Cada firmante recibe un mensaje de correo electrónico con la solicitud de la firma. Recibirá una notificación cuando cada firmante firme el archivo y cuando todo el proceso se haya completado.
9. Cuando el proceso haya terminado, seleccione el archivo firmado y haga clic en la pestaña **Certificado de firma electrónica** y en **Certificado de firma electrónica** para descargar un documento PDF que contiene:
 - La sección **Certificado de firma electrónica** con una recopilación de todas las firmas.
 - La sección **Pista de auditoría** con un historial de actividades: cuándo se envió la invitación a los firmantes, cuándo firmó el archivo cada firmante y otros datos.


Una vez que el proceso se haya completado, cada firmante recibirá una notificación que contiene:

- Un enlace al archivo firmado.
- Un enlace al certificado de firma electrónica.


- Un enlace a la autenticación notarial del certificado de firma electrónica. Una vez terminado el proceso de firma, la autenticación notarial estará disponible en un plazo de 70 minutos.

Operaciones con archivos firmados

Cómo descargar un archivo firmado del almacenamiento en la nube

1. Haga clic en **Archivos firmados**.
2. En la lista, busque el archivo que necesite.
Los archivos se pueden filtrar por estado y ordenar por nombre, estado, firma y fechas de carga. También puede hacer una búsqueda.
3. Haga clic en  o en el nombre del archivo. Después, haga clic en **Descargar**.

Cómo eliminar un archivo firmado del almacenamiento en la nube

1. Al eliminar un archivo firmado del almacenamiento en la nube, también se borrará su certificado de firma electrónica. Si es posible que vaya a necesitar el certificado de firma electrónica, asegúrese de que haya guardado una copia local del mismo, tal y como se describe en el paso 6 del apartado "[Cómo firmar un archivo](#)".
El certificado de firma se mantendrá certificado ante notario.
2. Haga clic en **Archivos firmados**.
3. En la lista, busque el archivo que necesite.
Los archivos se pueden filtrar por estado y ordenar por nombre, estado, firma y fechas de carga. También puede hacer una búsqueda.
4. Haga clic en  o en el nombre del archivo. Después, haga clic en **Eliminar**.
5. Confirme su decisión.
Se recomienda descargar la autenticación notarial del certificado de firma electrónica o guardar el enlace directo a ella antes de confirmar la eliminación.

Plantillas de documento

Puede crear plantillas de documento y utilizarlas para facilitar el proceso de creación de archivos nuevos para la firma electrónica.

La plantilla de documento es un modelo para transacciones que se repiten. Con las plantillas de documento, puede crear el contenido del documento, incluido un conjunto de campos obligatorios u opcionales, y asignar los firmantes exactos más tarde. Los destinatarios y firmantes pueden cambiar cada vez que utilice una plantilla de documento para crear un archivo nuevo.

Cree una plantilla de documento de la siguiente forma:

1. suba un archivo en formato PDF o en un formato de archivo que pueda convertirse a PDF: TXT, DOC, DOCX, XLS, XLSX, PPT, PPTX, y PDF.
2. añada al menos un campo de firmante a la plantilla
3. añada campos para cada firmante adicional, si fuese necesario

4. añada campos personalizados, si fuese necesario
5. guarde la plantilla

Nota

Solo puede guardar una plantilla de documento si incluye al menos un campo de firmante.

Campos de la plantilla de documento

El proceso de creación de una plantilla de documento consiste en cargar un archivo que contenga la información principal y añadir campos predefinidos o personalizados de plantilla.

Hay dos tipos de campos de la plantilla de documento: Campos de **Firmante** y campos **personalizados**.

Los campos de firmante están estrictamente predefinidos para la información del firmante. Puede añadir o eliminar campos de firmante de una plantilla y configurar si son obligatorios u opcionales, pero no puede cambiar su nombre.

Nombre de campo de firmante	Descripción
Nombre	Nombre del firmante del documento.
Firma	Firma del firmante del archivo. De forma predeterminada, el campo es obligatorio. Para hacerlo opcional, seleccione la casilla de verificación Opcional .
Iniciales	Iniciales del firmante del archivo. De forma predeterminada, el campo es obligatorio. Para hacerlo opcional, seleccione la casilla de verificación Opcional .

Los campos personalizados son campos de texto libres que puede añadir a la plantilla en función de sus necesidades. Puede establecer el nombre del campo personalizado (por ejemplo, **Fecha**, o **Dirección de facturación**) al crear la plantilla y rellenar su contenido cuando cree un nuevo archivo a partir de la plantilla.

Nota

El contenido de los campos personalizados siempre aparece con la misma fuente y tamaño.

Creación de una plantilla de documento

Puede crear una plantilla y utilizarla para generar fácilmente archivos nuevos para la firma electrónica.

Pasos para crear una plantilla de documento

1. Haga clic en **Archivos firmados>Plantillas**.
2. Haga clic en **Crear plantilla**.

3. En la ventana **Cargue el documento para su plantilla**, utilice una de las siguientes opciones para cargar el archivo:
 - Arrastre y suelte el archivo.
 - Haga clic en **Examinar**, busque el archivo y selecciónelo.

4. **Importante**

El formato del archivo de la plantilla debe ser PDF, TXT, DOC, DOCX, XLS, XLSX, PPT o PPTX.

5. En la pestaña **Firmantes**, haga clic en al menos uno de los campos predefinidos para el **Firmante 1**.

Nota

Cuando haga clic en un campo, aparecerá en la plantilla. Puede arrastrar el campo para cambiar su posición en la plantilla. También puede arrastrar los correspondientes bordes del campo para cambiar su tamaño.

6. [Opcional] Para cada firmante adicional que quiera añadir:
 - a. Haga clic en **Añadir firmante**.
 - b. Añada al menos uno de los campos de firmante a la plantilla.
7. [Opcional] Para añadir un campo personalizado, en la pestaña **Campos personalizados**:
 - a. Haga clic en el icono de lápiz situado al lado de la etiqueta del Campo personalizado.
 - b. En la ventana **Cambiar el nombre del campo personalizado**, escriba un nombre para el campo personalizado. La longitud máxima permitida para el nombre es de 30 caracteres.
 - c. Haga clic en el campo para añadirlo a la plantilla de documento y utilice el ratón para moverlo a la posición adecuada.
8. [Opcional] Para cada campo personalizado adicional que quiera añadir:
 - a. Haga clic en **Agregar campo personalizado**.
 - b. Haga clic en el icono de lápiz situado al lado de la etiqueta del Campo personalizado.
 - c. En la ventana **Cambiar el nombre del campo personalizado**, escriba un nombre para el campo personalizado. La longitud máxima permitida para el nombre es de 30 caracteres.
 - d. Haga clic en el campo para añadirlo a la plantilla de documento y utilice el ratón para moverlo a la posición adecuada.
9. Haga clic en **Previsualizar y crear**.
10. Si la información de la plantilla es correcta, haga clic en **Crear**.

La nueva plantilla aparece ahora en la página **Plantillas**. Para obtener más información acerca de las acciones que puede ejecutar desde la página **Plantillas**, consulte "Gestión de plantillas de documento" (p. 15).

Gestión de plantillas de documento

Cuando cree una plantilla, aparecerá en la página **Plantillas**. En la página **Plantillas**, puede ver más información sobre las plantillas existentes y ejecutar las siguientes acciones:


- [Previsualizar una plantilla de documento](#)
- [Crear un archivo desde una plantilla](#)
- [Cambiar el nombre de una plantilla de documento](#)
- [Eliminar una plantilla de documento](#)

En la siguiente tabla se describe la información disponible en la página **Plantillas**.

Nombre de la columna	Descripción
Nombre de la plantilla	Nombre de la plantilla.
Documento cargado	Nombre del archivo desde el que se creó la plantilla.
Documentos creados	Número de archivos creados con esta plantilla.
Creada	La fecha y la hora en las que se cargó la plantilla.
ID	Número de identificación del sistema de la plantilla. Se genera automáticamente.


Previsualizar una plantilla de documento

Pasos para previsualizar una plantilla de documento

1. En **Archivos firmados > Plantillas**, busque la plantilla de la que desea previsualizar.
2. Haga clic en  y en **Vista previa**.
3. Cuando acabe el proceso de previsualización, haga clic en **Listo**.


Cambiar el nombre de una plantilla de documento

Pasos para cambiar el nombre de una plantilla de documento

1. En **Archivos firmados > Plantillas**, busque la plantilla a la que desee cambiarle el nombre.
2. Haga clic en  y en **Cambiar nombre**.
3. En el campo **Nombre de la plantilla**, actualice el nombre de la plantilla.
4. Haga clic en **Cambiar nombre**.

Eliminar una plantilla de documento


Pasos para eliminar una plantilla de documento

1. En **Archivos firmados > Plantillas**, busque la plantilla que desee eliminar.
2. Haga clic en  y en **Eliminar**.

Creación de un documento desde una plantilla

Puede crear fácilmente un nuevo documento desde una plantilla existente y enviarlo para firmarlo electrónicamente.

Pasos para crear un documento desde una plantilla

1. Haga clic en **Archivos firmados>Plantillas**.
2. En la lista de plantillas de documento, busque la plantilla que desea utilizar.
3. Haga clic en  y, a continuación, en **Crear documento**.
4. En la ventana **Crear documento desde la plantilla**, en el campo **Nombre del documento**, escriba el nombre del archivo.
5. Escriba las direcciones de correo electrónico de los firmantes del documento.

Nota

Las direcciones de correo electrónico que indique se utilizarán para enviar un correo electrónico a todos los firmantes del archivo. Este correo electrónico contiene un enlace que deberán utilizar los signatarios para ver y firmar el archivo electrónicamente.

6. Si la plantilla incluye campos personalizados, haga clic en **Siguiente**. Si no, vaya al paso 8.
7. Rellene la información de los campos personalizados.

Nota

La longitud de los campos personalizados está limitada a 250 símbolos.

8. Haga clic en **Previsualizar y crear**.
9. Si la información del archivo es correcta, haga clic en **Crear**.

Nota

Se crea el archivo y aparece visible en **Archivos firmados > Archivos**. Puede ver el nombre de la plantilla que ha utilizado para crear el documento en la columna **Nombre de la plantilla**.

Se envía un correo electrónico a los firmantes del documento que contiene un enlace para ver y firmar el archivo electrónicamente. Cada firmante del documento puede firmarlo siguiendo el procedimiento de "Firmar un archivo creado desde una plantilla" (p. 17).

Firmar un archivo creado desde una plantilla

Cuando cree un archivo desde una plantilla, todos los firmantes recibirán un correo electrónico con un enlace que pueden utilizar para firmar el archivo electrónicamente.

Pasos para firmar electrónicamente un archivo creado desde una plantilla

1. En el correo electrónico, busque un correo del remitente notaryacronissg@gmail.com y ábralo.
2. Haga clic en **Revisar y firmar**.

3. En la ventana **Introduzca su nombre, firma e iniciales**, introduzca su nombre, firma electrónica e iniciales.
4. Seleccione **He leído y acepto**.
5. Haga clic en **Listo**.
6. En la ventana **Firmar documento**, haga clic en los campos importantes para completar el contenido desde el paso 3.
7. Haga clic en **Previsualizar y firmar**.
8. Cuando haya acabado de previsualizar, haga clic en **Firmar**.

El archivo firmado se guarda como formato PDF. Se crea un certificado de firma y un certificado de autenticación notarial del certificado de firma. Una vez terminado el proceso de firma, la autenticación notarial estará disponible en un plazo de 70 minutos. Puede descargar el archivo y los certificados.

Utilización del servicio de certificación como administrador de certificación

Cuando trabaja con plantillas y archivos certificados ante notario y firmados electrónicamente de su propiedad, el administrador de certificación puede ejecutar las mismas funciones que un usuario de certificación. Para obtener más información, consulte "Utilizar el servicio de certificación como usuario de certificación" (p. 5).

Asimismo, el administrador de certificación puede ejecutar varias funciones que no están disponibles para el usuario de certificación:

- Ver las plantillas y los archivos certificados ante notario y firmados electrónicamente creados por el resto de usuarios o administradores del inquilino de cliente.
- Ver el propietario de todas las plantillas y los archivos certificados ante notario y firmados electrónicamente del inquilino de cliente. El propietario es visible en la columna **Propietario** de la consola del servicio de certificación, en las pestañas **Archivos certificados ante notario**, **Archivos firmados** y **Plantillas**.
- Ver el progreso del proceso de firma de todos los documentos creados por el resto de usuarios o administradores del inquilino de cliente.

Nota

El administrador no puede firmar documentos en nombre de otros usuarios. El administrador solo puede firmar documentos cuando se le añade como firmante.

- Volver a enviar invitaciones a los firmantes de un documento creado por otro usuario o administrador en el inquilino de cliente.
- Descargar las plantillas originales y los archivos certificados ante notario y firmados electrónicamente creados por el resto de usuarios o administradores del inquilino de cliente.

- Descargar los archivos certificados firmados electrónicamente (si se ha completado el proceso de firma del documento mediante la firma electrónica) creados por el resto de usuarios o administradores del inquilino de cliente.
- Descargar los archivos del certificado de firma (si se ha completado el proceso de firma del documento mediante la firma electrónica) de los archivos firmados electrónicamente y creados por el resto de usuarios o administradores del inquilino de cliente.
- Eliminar las plantillas y los archivos certificados ante notario y firmados electrónicamente creados por el resto de usuarios o administradores del inquilino de cliente. Se notifica a los propietarios de las plantillas o archivos eliminados por correo electrónico.
- Crear nuevos documentos a partir de plantillas de documentos creadas por el resto de usuarios o administradores del inquilino de cliente. Se notifica a los propietarios de las plantillas de documentos mediante correo electrónico.

Administración del servicio de certificación

En este apartado se describe la funcionalidad que solo está disponible para los administradores del servicio de certificación.

Gestión de claves de API

El servicio de certificación puede integrarse con sistemas de terceros mediante la interfaz de programación de aplicaciones (API) del servicio de certificación. Para obtener más información acerca del uso de la API, consulte la guía del desarrollador en <https://developer.acronis.com/doc/notary/v2/guide/>.

Un administrador del servicio de certificación puede crear y gestionar claves de la API para las integraciones.


Cómo crear una clave de la API

1. Haga clic en **Claves de la API > Crear clave de la API**.
2. Cree e introduzca un nombre único para la clave de API.
3. Haga clic en **Crear**.
4. De forma predeterminada, la clave de API se crea con el estado **Habilitada**.


Importante

Copie y guarde la clave. Por motivos de seguridad, la clave solo se muestra una vez. No hay ninguna forma de recuperar la clave si la pierde.


Cómo deshabilitar una clave de API

1. Haga clic en **Claves de API**.
2. En la lista, busque la clave que necesite.
Puede filtrar las claves por estado y ordenarlas por nombre, estado y fecha de creación.
3. Haga clic en  y en **Deshabilitar**.
4. Confirme su decisión.
Todas las integraciones que usen esta clave dejarán de funcionar. La clave se podrá volver a habilitar en cualquier momento.


Cómo habilitar una clave de API deshabilitada

1. Haga clic en **Claves de API**.
2. En la lista, busque la clave que necesite.
Puede filtrar las claves por estado y ordenarlas por nombre, estado y fecha de creación.
3. Haga clic en  y en **Habilitar**.

Cómo eliminar una clave de API

1. Haga clic en **Claves de API**.
2. En la lista, busque la clave que necesite.
Puede filtrar las claves por estado y ordenarlas por nombre, estado y fecha de creación.
3. Haga clic en  y en **Eliminar**.
4. Confirme su decisión.
Todas las integraciones que usen esta clave dejarán de funcionar. No hay manera de recuperar una clave de API eliminada.

Administración de cuentas de usuario y cuotas

La administración de cuentas de usuario y de cuotas de uso del servicio está disponible en el portal de gestión. Para acceder al portal de administración, haga clic en **Portal de gestión** cuando inicie sesión en el servicio Notary, o bien haga clic en el icono  de la esquina superior derecha y en **Portal de gestión**. Solo aquellos usuarios a los que se les ha asignado la función de administrador de empresa pueden acceder a este portal.

Para obtener información sobre la administración de cuentas de usuario y sus cuotas, consulte la Guía del administrador del portal de gestión. Para acceder a este documento, haga clic en el icono del signo de interrogación en el portal de gestión.

En este apartado se proporciona información adicional relacionada con la gestión del servicio de certificación.

Cuotas

Las cuotas le permiten limitar la capacidad de los usuarios de utilizar el servicio. Para establecer las cuotas, seleccione el usuario en la pestaña **Usuarios** 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 "blanda". Esto significa que no se aplican restricciones para usar el servicio de certificación.

También puede especificar usos por encima del límite de la cuota. Un uso por encima del límite permite al usuario sobrepasar la cuota en un valor especificado. Cuando se exceda el límite, se aplicarán restricciones en el uso del servicio de certificación.

Los proveedores de servicios gestionados también pueden especificar cuotas para las empresas de sus clientes de una forma similar.

Están disponibles las cuotas siguientes:

- **Almacenamiento de Notary**

El almacenamiento de Notary es el almacenamiento en la nube donde se guardan los archivos certificados ante notario, los firmados y aquellos cuya certificación está en progreso. Esta cuota define el espacio máximo que pueden ocupar estos archivos.

Para reducir el uso de esta cuota, puede eliminar los archivos ya certificados ante notario o firmados del almacenamiento de Notary.

- **Notarizaciones**

Esta cuota 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**

Esta cuota define el número máximo de archivos que se pueden firmar con el servicio de certificación. Un archivo se considera firmado desde el momento en el que se envía para su firma.

- **Plantillas de documento**

Esta cuota define el número máximo de plantillas de documento que puede guardar el cliente.

Notificaciones

Para cambiar los ajustes de notificaciones para un usuario, seleccione el usuario en la pestaña **Usuarios** y haga clic en el icono del lápiz en la sección **Configuración**. Están disponibles los siguientes ajustes de notificaciones:

- **Notificaciones de uso excesivo de las cuotas** (habilitado de forma predeterminada)

Las notificaciones sobre cuotas superadas.

- **Informes de uso planificados**

Informes de uso descritos a continuación que se envían el primer día de cada mes.

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

Informes de uso

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

- Tamaño de los archivos guardados en el almacenamiento de Notary (salvo aquellos que se están verificando) por unidad y por usuario.
- Número de notarizaciones por unidad y por usuario.
- Número de archivos firmados por unidad y por usuario.
- Tamaño total de los archivos guardados en el almacenamiento de Notary (salvo aquellos que se están verificando).
- El número total de notarizaciones.
- El número total de archivos firmados.

Índice

A

Acceso a la interfaz web del servicio de certificación 5

Acerca del servicio de certificación 3

Activación de la cuenta 5

Administración de cuentas de usuario y cuotas 21

Administración del servicio de certificación 20

Autenticación certificación 6

C

Campos de la plantilla de documento 14

Certificación de archivos 5

Cómo funciona la certificación 3

Creación de un documento desde una plantilla 17

Creación de una plantilla de documento 14

Cuotas 21

E

Enviar un archivo para que lo firmen varias personas 12

F

Firmado de archivos 10

Firmar un archivo creado desde una plantilla 17

G

Gestión de claves de API 20

Gestión de plantillas de documento 15

I

Informes de uso 22

L

Limitaciones 4

N

Navegadores web compatibles 4

Notificaciones 22

O

Operaciones con archivos certificados ante notario 6

Operaciones con archivos firmados 13

P

Página pública de verificación 9

Pasos para firmar un archivo como el único firmante 10

Plantillas de documento 13

R

Roles de usuario 3

U

Utilización del servicio de certificación 5

Utilización del servicio de certificación como administrador de certificación 18

Utilizar el servicio de certificación como usuario de certificación 5

V

Verificación de la autenticidad de los
archivos 8