Portal de gestión

25.06

Guía del administrador de la empresa

REVISIÓN: 08/07/2025

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.

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.

Mi bandeja de entrada

La página Mi bandeja de entrada está diseñada para agilizar su comunicación dentro de la aplicación. Con esta guía, puede gestionar sus mensajes de forma eficaz, mantenerse organizado y mejorar su productividad. La bandeja de entrada del producto es su centro de operaciones en el que recibir y gestionar comunicaciones dentro de la aplicación. Le permite mantenerse informado sobre actualizaciones importantes, mensajes y alertas dentro de su flujo de trabajo.

Información general

La pestaña **Mi bandeja de entrada** cuenta con una función de contador de notificaciones que muestra la cantidad de notificaciones sin leer. Al hacer clic en este contador, se muestran las notificaciones sin leer, lo que facilita el seguimiento de los elementos pendientes. Además, las funciones de contadores junto a cada filtro (categoría, importancia, acción) muestran la cantidad de notificaciones disponibles en ese filtro específico, lo que le ayuda a comprender cuántas notificaciones entran en cada categoría.

En su bandeja de entrada, recibirá varias notificaciones, cada una diseñada para fines específicos según su configuración de cuenta y contexto: anuncios de funciones, nuevos cursos de formación disponibles, invitaciones a eventos y seminarios web, recordatorios de vencimiento de certificados, promociones, avisos de mantenimiento, encuestas y otros.

Comprobación de sus notificaciones

Comprobación de la sección de notificaciones

1. Inicie la sesión en la consola de Cyber Protect Cloud.
2. En el panel de navegación, seleccione el elemento de menú **Mi bandeja de entrada**.

Búsqueda en Mi bandeja de entrada

Pasos para buscar mensajes no leídos

1. Haga clic en el elemento de menú **Mi bandeja de entrada**.
2. En la esquina superior derecha, cambie el interruptor **Mostrar solo no leídos**.

Pasos para buscar información importante en su bandeja de entrada

1. Acceda a **Mi bandeja de entrada** desde el panel de control de Cyber Protect Cloud.
2. En la vista de la bandeja de entrada, busque la barra de **búsqueda** en la parte superior.
3. Introduzca palabras clave o nombres de remitentes relevantes para filtrar los mensajes.
4. Pulse **Intro** para ver los resultados de la búsqueda.

Los resultados mostrarán todas las notificaciones que coincidan con los criterios de búsqueda.

Cuentas y unidades

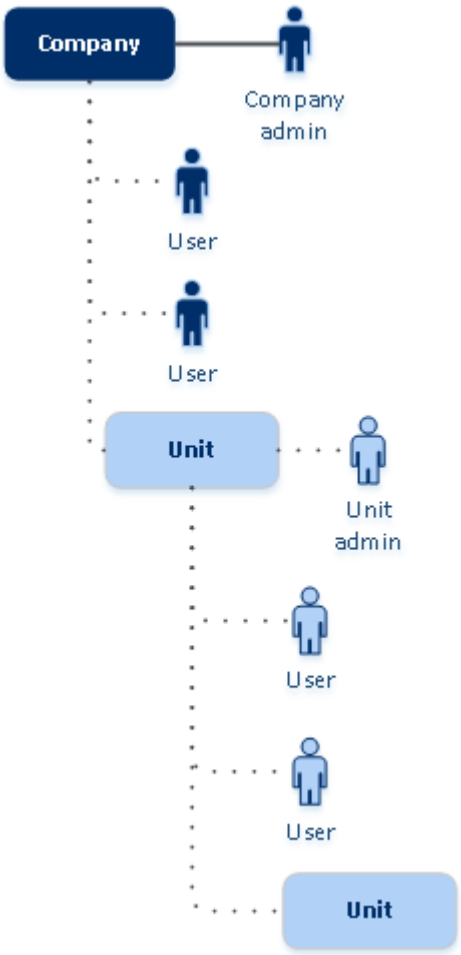
Hay dos tipos de cuentas de usuario: las cuentas de administrador y las cuentas de usuario.

- 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.

Importante
Los valores del uso de almacenamiento que se muestran en la interfaz de usuario del producto están en unidades de bytes binarios: mebibyte (MiB), gibibyte (GiB) y tebibyte (TiB), aunque las etiquetas muestren MB, GB y TB, respectivamente. Por ejemplo, si el uso real es de 3105886629888 bytes, el valor que aparece en la interfaz de usuario se muestra correctamente como 2,82, pero se etiqueta con TB en lugar de TiB.

Visualización de cuotas para su organización

En el portal de administración, vaya a **Supervisión** > **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**
  El proveedor de servicios aplica esta cuota a toda la empresa. Los administradores de la empresa pueden ver la cuota y su uso en el portal de administración. Cuando se excede la cuota estricta, los planes de copias de seguridad no se pueden aplicar a nuevos puestos.
  La facturación de esta cuota depende del modo de facturación seleccionado para Cyber Protection.

- En el modo de facturación **Por gigabyte**, la facturación se basa únicamente en el uso del almacenamiento y no se cuentan los puestos.
- En el modo de facturación **Por recursos informáticos**, la facturación se basa en el número de puestos protegidos de Microsoft 365. El uso de almacenamiento se factura solo para los puestos no protegidos.

  La siguiente tabla resume el modo de facturación **Por recursos informáticos**.

	Ubicación de la copia de seguridad	
	Almacenamiento alojado por Acronis **Almacenamiento alojado por partners**	**Microsoft Azure Storage** **Almacenamiento de Google**
Puesto protegido	La facturación se realiza según el número de puestos protegidos. No se factura el espacio de almacenamiento que se utiliza para las copias de seguridad de los puestos protegidos.	Se facturan tanto los puestos protegidos como el almacenamiento utilizado.
Puesto no protegido	No se facturan los puestos no protegidos. Se facturará el espacio de almacenamiento que se utilice para las copias de seguridad de los puestos no protegidos.	No se facturan los puestos no protegidos. Se facturará el espacio de almacenamiento que se utilice para las copias de seguridad de los puestos no protegidos.

  * Se aplica la política de uso justo de Acronis Storage. Los términos y condiciones están disponibles en https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage.

Se considera que un puesto está protegido cuando un usuario de Microsoft 365 tiene cualquiera de los siguientes elementos:

- Buzón de correo al que se aplica un plan de copias de seguridad
- OneDrive al que se aplica un plan de copias de seguridad
- Acceso a un recurso de nivel de empresa protegido, como a 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.

Un puesto queda desprotegido en los siguientes casos:

- Se revoca el acceso a un recurso de nivel de empresa protegido, como un sitio de Microsoft 365 SharePoint Online o Microsoft 365 Teams, para un usuario.
- Se revocan todos los planes de copias de seguridad del buzón de correo o OneDrive de un

usuario.

- Se ha eliminado un usuario en la organización de Microsoft 365.

Los siguientes recursos de Microsoft 365 no se le cobrarán y no requieren una licencia por puesto:

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

Nota
No se cobra a los usuarios de Microsoft 365 bloqueados que no tienen un buzón de correo personal o un OneDrive protegidos y que solo pueden acceder a recursos compartidos (buzones de correo compartidos, sitios de SharePoint y Microsoft Teams). Los usuarios bloqueados son aquellos que no tienen unas credenciales válidas 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. 15).

Importante
El agente local y el agente de la nube consumen cuotas independientes. Si lleva a cabo la copia de seguridad de los mismos recursos informáticos 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.

Para consultar las preguntas frecuentes sobre las licencias de Microsoft 365, consulte Cyber Protect Cloud: Licencias de Microsoft 365 por GB y Cyber Protect Cloud: Cambios en las licencias y precios de Microsoft 365.

- **Microsoft 365 SharePoint Online**

  Esta cuota la aplica el proveedor de servicios a toda la empresa. Esta cuota habilita la protección de los sitios de 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 en el portal de administración. También pueden ver la cuota junto con la cantidad de almacenamiento que utilizan las copias de seguridad de SharePoint Online en los informes de uso.

- **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.

- **Licencias de archivado de correo electrónico de Microsoft 365**

  La cuota de **Licencias de archivado de correo electrónico de Microsoft 365** habilita o deshabilita la capacidad de crear el archivado de correos electrónicos y establece el número máximo de buzones de correo que se pueden agregar al archivo.
- **Licencias de archivado de correo electrónico (obsoleto)**

  Esta cuota está obsoleta y no puede habilitarla al crear nuevos inquilinos en el portal de administración.

  Para los inquilinos existentes, solo puede deshabilitar la cuota si ya estaba habilitada, pero ya no puede habilitarla.

Importante

Al crear nuevos clientes-inquilinos, utilice la cuota de **Licencias de archivado de Microsoft 365**.

Para clientes existentes, la cuota de **Licencias de archivado de correo electrónico (obsoleto)** se reemplazará automáticamente por la cuota de **Licencias de archivado de Microsoft 365**. Cualquier uso existente de las **Licencias de archivado de correo electrónico (obsoleto)** se transferirá a **Licencias de archivado de Microsoft 365**.

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.

Se considera que una licencia de Google Workspace está protegida si se aplica, como mínimo, un plan de copias de seguridad al buzón de correo o al Google Drive del usuario.

Cuando se excede la cuota estricta, un administrador de la empresa no puede aplicar un plan de copias de seguridad a nuevos puestos.

- **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.

Cuotas de almacenamiento

Importante
Los valores del uso de almacenamiento que se muestran en la interfaz de usuario del producto están en unidades de bytes binarios: mebibyte (MiB), gibibyte (GiB) y tebibyte (TiB), aunque las etiquetas muestren MB, GB y TB, respectivamente. Por ejemplo, si el uso real es de 3105886629888 bytes, el valor que aparece en la interfaz de usuario se muestra correctamente como 2,82, pero se etiqueta con TB en lugar de TiB.

- **Recursos en la nube**
  - **Almacenamiento de la copia de seguridad**
    - **Almacenamiento de la copia de seguridad**

      Esta cuota limita el tamaño total de las copias de seguridad que se encuentran en el almacenamiento en la nube. Cuando se excede la cuota estricta del almacenamiento de copia de seguridad, la operación de copia de seguridad no se iniciará.

      En el modo de facturación **Por carga de trabajo**, esta cuota se aplica solo a las copias de seguridad de cargas de trabajo que no sean de Microsoft 365 y Google Workspace.

      El almacenamiento de copias de seguridad para cargas de trabajo de Microsoft 365 y Google Workspace es ilimitado*. Si se elimina una cuota de licencias, como **Licencias de Microsoft 365** o **Licencias de Google Workspace**, de una carga de trabajo, el almacenamiento de copias de seguridad seguirá siendo ilimitado, pero se cobrará su uso.

      Con el modo de facturación **Por gigabyte**, esta cuota se aplica a todas las copias de seguridad, incluidas las copias de seguridad de los recursos informáticos de Microsoft 365 y Google Workspace.

      * Se aplica la política de uso justo de Acronis Storage. Los términos y condiciones están disponibles en https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage.
    - **Almacenamiento de archivos comprimidos**

      Esta cuota limita el tamaño total del archivo comprimido de correos electrónicos en la infraestructura en la nube.
  - **Advanced Disaster Recovery**

    Esta sección contiene las cuotas relacionadas con la recuperación ante desastres.
- **Recursos locales**
  - **Copia de seguridad local**

    La cuota de **Copia de seguridad local** limita el tamaño total de las copias de seguridad en discos locales, recursos compartidos de red y nubes públicas, como S3 compatible, Azure, AWS, Wasabi e Impossible Cloud.
    - Para esta cuota no se puede establecer un uso por encima del límite.
    - No se puede aplicar una cuota estricta a las copias de seguridad locales.

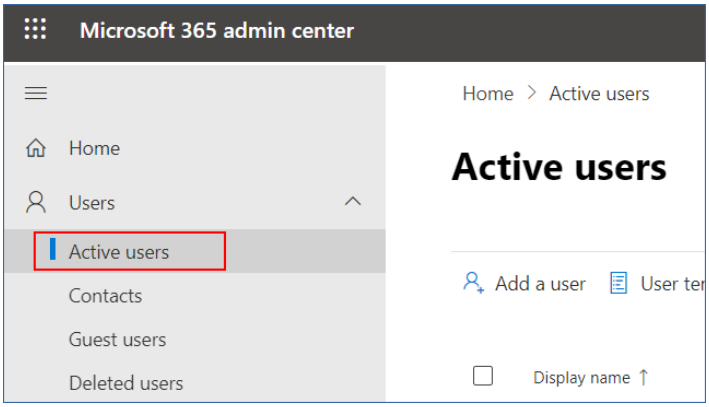
Nota
Deshabilitar la cuota de **Copia de seguridad local** deshabilitará las copias de seguridad locales, las copias de seguridad en recursos compartidos de red y las copias de seguridad en nubes públicas.

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.

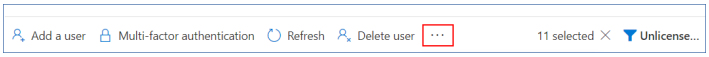
Para impedir que los usuarios sin licencia inicien sesión

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 Disaster Recovery

Nota
Los artículos de oferta de Disaster Recovery solo están disponibles con el complemento de Disaster Recovery.

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.

Para Disaster Recovery en Microsoft Azure, están disponibles los siguientes elementos de oferta:

- **DR y copia de seguridad directa en Azure**
  Habilita Advanced Disaster Recovery y la copia de seguridad directa en la suscripción de Azure del cliente. Se asigna una cuota a cada carga de trabajo protegida.

Para Disaster Recovery en Cyber Protect Cloud, están disponibles los siguientes elementos de oferta:

- **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 **Mi empresa** 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

Importante
Los valores del uso de almacenamiento que se muestran en la interfaz de usuario del producto están en unidades de bytes binarios: mebibyte (MiB), gibibyte (GiB) y tebibyte (TiB), aunque las etiquetas muestren MB, GB y TB, respectivamente. Por ejemplo, si el uso real es de 3105886629888 bytes, el valor que aparece en la interfaz de usuario se muestra correctamente como 2,82, pero se etiqueta con TB en lugar de TiB.

- **Almacenamiento de la copia 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 la nube. 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 los mismos recursos informáticos 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.

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. 21).

Requisitos de contraseña

La complejidad de las contraseñas se comprueba durante el registro del usuario y se clasifican en una de las siguientes categorías:

- Débil
- Medio
- Fuerte

No puede guardar una contraseña débil, incluso aunque sea lo suficientemente larga. 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.

Nota
Los requisitos de contraseña están sujetos a cambios.

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.

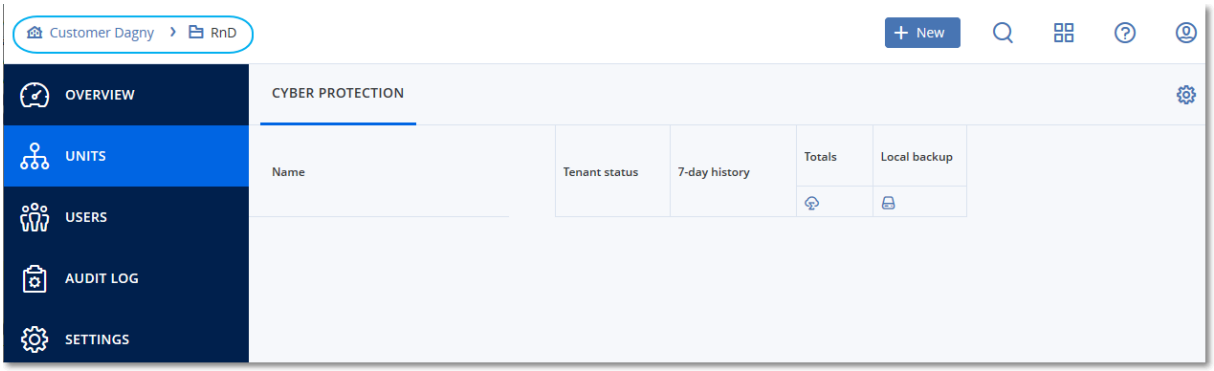
Cambiar del portal de administración a las consolas de servicio y viceversa

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

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

- Cuenta de administrador de empresa: para compartir las funciones de gestión con otras personas.
- Cuentas de administrador de unidad: para delegar la gestión de los servicios en otras personas cuyos permisos de acceso estarán estrictamente limitados a la unidad correspondiente.
- Cuentas de usuario en el cliente o un inquilino de unidad: 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**.
   De manera alternativa, vaya a **Mi empresa** > **Usuarios** y haga clic en **+ Nuevo**.
4. Especifique la siguiente información de contacto para la cuenta:
   - Si prefiere utilizar un inicio de sesión distinto del correo electrónico, marque la casilla de verificación **Utilizar un inicio de sesión distinto del correo electrónico** y, a continuación, introduzca un **Inicio de sesión** y un **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.

     Importante
     Debe haber únicamente un usuario en cada cuenta.

   - [Opcional] **Nombre**
   - [Opcional] **Apellido**
   -
   - En el campo **Idioma**, cambie el idioma predeterminado de las notificaciones, los informes y el software de esta cuenta.
5. [Opcional] Especifique los contactos de la empresa.
   - **Facturación**: el contacto que recibirá actualizaciones sobre cambios importantes en la creación de informes de uso en la plataforma.
   - **Técnico**: el contacto que recibirá actualizaciones sobre cambios técnicos importantes en la plataforma.
   - **Comercial**: el contacto que recibirá actualizaciones sobre cambios comerciales importantes en la plataforma.
     Puede asignar más de un contacto de la empresa a un usuario.

   Puede ver los contactos de empresa asignados para un usuario en la lista **Usuarios**, en la columna **Contactos de la empresa**, y editar la cuenta de usuario para cambiar los contactos de empresa si es necesario.
6. [No disponible cuando se crea una cuenta en un inquilino de partner o carpeta] Seleccione los servicios a los que el usuario tendrá acceso y los roles en cada servicio.
   Los servicios disponibles dependen de los servicios habilitados para el inquilino en el que se ha creado la cuenta de usuario.
   - Si selecciona la opción **Administrador de la empresa**, el usuario tendrá acceso al portal de gestión y a la función de administrador en todos los servicios actualmente habilitados para el inquilino. El usuario también tendrá la función de administrador en todos los servicios que se

habiliten para el inquilino en el futuro.
- 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 asignadas en los servicios que habilite para ese usuario.

7. Haga clic en **Crear**.

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

Si desea modificar la configuración del usuario o especificar parámetros de notificación o cuotas para el usuario (no disponible para administradores de partners y carpetas), seleccione al usuario en la pestaña **Usuarios** y 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 **Mi empresa** > **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.

Ahora la cuenta puede utilizarse en 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.

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 en una cuenta de servicio

1. En el portal de administración, vaya a **Mi empresa** > **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.

Nota
Los servicios que están disponibles para usted están configurados por su proveedor de servicios.

Servicio	Rol	Descripción
n/d	Administrador de la empresa	Este rol concede todos los derechos de administrador de todos los servicios. Este rol garantiza acceso a la lista de permitidos corporativa. Si el complemento Disaster Recovery del servicio de protección está activado para la empresa, este rol también garantiza el acceso a la funcionalidad de recuperación ante desastres.
	Administrador de la unidad Nivel de unidad	Este rol otorga los permisos más altos posibles a todos los servicios aplicables en la unidad. El rol no da acceso a la funcionalidad de Disaster Recovery.
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.
	Administrador de solo lectura	Este rol proporciona acceso de solo lectura a todos los objetos del portal de administración de toda la empresa. Consulte "Función de administrador de solo lectura" (p. 29).
	Administrador de solo lectura Nivel de unidad	Este rol proporciona acceso de solo lectura a todos los objetos del portal de administración de la unidad y subunidades de la empresa. Consulte "Función de administrador de solo lectura" (p. 29).
Portal de proveedores	Desarrollador	Este rol proporciona acceso completo al portal de proveedores. Los desarrolladores pueden crear y gestionar CyberApps, CyberApp Descriptions y CyberApp Versions. También pueden enviar solicitudes de despliegue y supervisar los parámetros de CyberApp.
	Usuario	Este rol permite al usuario crear, gestionar y solicitar aprobaciones de CyberApp Descriptions.
	Usuario de solo lectura	Este rol proporciona acceso de solo lectura al portal de proveedores.

Protección	

	Administrador	Este rol permite configurar y gestionar el servicio de protección para sus clientes. Este rol es necesario para: • la configuración y gestión de la funcionalidad Disaster Recovery. • la configuración y gestión de la lista de permitidos corporativa. • la realización de la detección automática de dispositivos. • la realización de todas las acciones relacionadas con el despliegue de software mediante el uso de DeployPilot (trabajar con planes de despliegue de software, repositorios de software, paquetes de software y realizar acciones de despliegue rápido).
	Administrador de cibernética	Además de los derechos del rol de administrador, este rol permite configurar y gestionar el servicio de protección, así como aprobar acciones en programación cibernética. El rol de administrador de cibernética solo está disponible para los inquilinos con el paquete de RMM habilitado.
	Administrador de solo lectura	La función proporciona acceso de solo lectura a todos los objetos del servicio de protección. Consulte "Función de administrador de solo lectura" (p. 29).
	Usuario	Esta función permite el uso del servicio de 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.
	Operador de restauración	Aplicable a organizaciones con Microsoft 365 y Google Workspace, el rol da acceso a las copias de seguridad y permite su recuperación, mientras restringe el acceso al contenido sensible dentro de las copias de seguridad. Consulte "Rol de operador de restauración" (p. 30).
	Analista de seguridad	El rol solo se puede asignar en los inquilinos de clientes para los que está habilitado el paquete Advanced Security + EDR o Advanced Security + XDR. Proporciona acceso a la consola de

		ciberprotección y permite al usuario gestionar incidentes de EDR y llevar a cabo acciones de respuesta.
	Operador de soporte para DR	Esta función proporciona acceso de solo lectura a todos los objetos del servicio de Protección en la organización, así como acceso al entorno de Disaster Recovery, y permite llevar a cabo una solución de problemas avanzada.
File Sync & Share	Administrador	Esta función permite configurar y gestionar File Sync & Share para sus usuarios.
Cyber Infrastructure	Administrador	Esta función permite configurar y gestionar Cyber Infrastructure para sus usuarios.
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.

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

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.
- Cuando Advanced Seguridad + XDR está habilitado, los administradores de solo lectura pueden acceder a la pestaña Acciones de respuesta en la pantalla de incidentes EDR, pero no pueden ejecutar ninguna acción.
- El acceso a los datos de otros usuarios de la organización en modo de solo lectura.

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.
- Configura y gestiona la funcionalidad Disaster Recovery o la lista de permitidos corporativa, y tiene acceso de solo lectura a los planes de despliegue de software, los repositorios de software y los paquetes de software.
- 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 eliminar copias de seguridad ni eliminar, actualizar o reconstruir índices de búsqueda para copias de seguridad de la nube a la nube.

  Nota
  En el portal de administración, los administradores de solo lectura pueden iniciar la creación de nuevos inquilinos secundarios y configurar todas sus propiedades con fines de demostración, pero no pueden guardarlas.

- Guarde cualquier cambio en los planes de scripts, los planes de supervisión o los planes de agentes.

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.

Rol de operador de restauración

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

Un operador de restauración puede:

- Ver alertas y actividades.
- Ver y actualizar la lista de copias de seguridad.
- Ver la lista de puntos de recuperación.

- Examinar copias de seguridad sin acceder al contenido.

  Nota
  Los operadores de restauración pueden ver los nombres de los archivos de la copia de seguridad y el asunto y los emisores de 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 únicamente a su 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.
- 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

Puede configurar qué notificaciones recibirá un usuario por correo electrónico, si el servicio Cyber Protection está habilitado para el inquilino donde se crea el usuario.

Para configurar las notificaciones para un usuario

1. Navegue a **Mi empresa** > **Usuarios**.
2. Haga clic en el usuario para el que desee configurar las notificaciones y, a continuación, en la pestaña **Servicios**, en la sección **Notificaciones por correo electrónico**, haga clic en el icono del lápiz.
3. Marque las casillas de verificación de las notificaciones por correo electrónico que desee habilitar.

Notificaciones	Descripción
Notificaciones de mantenimiento	Notificaciones que informan a los usuarios partner, a los inquilinos secundarios (partners y clientes) y a los usuarios individuales sobre las próximas actividades de mantenimiento en el centro de datos Cyber Protect. Estas notificaciones pueden habilitarlas los usuarios partner para sus inquilinos secundarios, y los usuarios partner o administradores de la empresa para los usuarios individuales dentro de su organización.
Notificaciones de uso excesivo de las cuotas	Notificaciones sobre cuotas superadas.
Informes de uso planificados	Informes de uso que se envían el primer día de cada mes.
Notificaciones de adaptación de marca de URL	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 cuenta atrás de cambio de producción	Notificaciones sobre la expiración de la prueba del cliente que se enviarán 10 días antes de que expire la prueba y 3 días antes de que expire la prueba.
Notificación de activación del modo de producción	Notificaciones sobre la activación del modo de producción.
Notificaciones de error	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.
Notificaciones de advertencia	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.
Notificaciones de éxitos	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	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

Notificaciones	Descripción
	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	Notificaciones de los intentos de utilizar dispositivos periféricos y puertos limitados por planes de protección con el módulo de control de dispositivos habilitado.
Notificaciones sobre los nuevos dispositivos descubiertos	Notificaciones sobre dispositivos recién descubiertos. Estas notificaciones se envían todos los lunes y jueves.
Notificaciones de recuperación	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	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	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 pertinentes para las alertas de incidentes de Endpoint Detection and Response (EDR), alertas EDR de fuentes de información sobre amenazas, y alertas individuales (para cargas de trabajo que no tienen EDR habilitado en ellas). 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	Notificaciones sobre problemas con la infraestructura de Disaster Recovery: cuando la infraestructura de Disaster Recovery o los túneles VPN no están disponibles.

Nota

Los usuarios de VMware Cloud Director pueden recibir las siguientes notificaciones: notificaciones de uso excesivo de cuota, informes de uso programados (si se han configurado dichos informes para la organización) y resumen diario sobre alertas activas.

Configuración predeterminada de notificaciones habilitadas por tipo de notificación y rol de usuario

Las notificaciones que están habilitadas o deshabilitadas por defecto dependen del tipo de notificación y del rol del usuario.

Tipo de notificación/función de usuario	Cliente, administradores de unidad (autoservicio)	Cliente, administradores de unidad (gestionado por el proveedor de servicios)
Notificaciones de mantenimiento	No	No
Notificaciones de uso excesivo de las cuotas	Sí	No
Notificaciones de informes de uso planificados	Sí	No
Notificaciones de adaptación de marca de URL	No	No
Notificaciones de error	No	No
Notificaciones de advertencia	No	No
Notificaciones de acciones realizadas correctamente	No	No
Resumen diario de alertas activas	Sí	No
Notificaciones de control de dispositivos	No	No
Notificaciones de recuperación	No	No
Notificaciones de prevención de pérdida de datos	No	No
Notificaciones de	No	No

incidentes de seguridad: Mitigado		
Notificaciones de incidentes de seguridad: No mitigado	No	No
Notificaciones de infraestructura	No	No

Notificaciones habilitadas por defecto según el tipo de dispositivo y el rol del usuario

Tipo de dispositivo\Rol de usuario	Usuario	Administrador de clientes
Notificaciones de los dispositivos propios	Sí	Sí
Notificaciones de todos los dispositivos de la organización	n/d	Sí
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.

Nota
Todos los dispositivos asociados al usuario deshabilitado ya no estarán protegidos porque no se les aplicará ninguna cuota. Para continuar con la protección de estos dispositivos, asígnelos a un usuario activo.

Para habilitar una cuenta de usuario deshabilitado

1. En el portal de administración, vaya a **Usuarios**.
2. Seleccione el usuario deshabilitado de la lista de usuarios y, a continuación, haga clic en el icono de puntos suspensivos > **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.

Nota
Puede reutilizar el inicio de sesión de un usuario eliminado después de eliminarlo.

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.

Nota
Para los inquilinos de partners en modo de producción, la autenticación de doble factor está habilitada de forma predeterminada y no se puede deshabilitar.

Para los inquilinos de cliente, la autenticación de doble factor es opcional y se puede deshabilitar.

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:

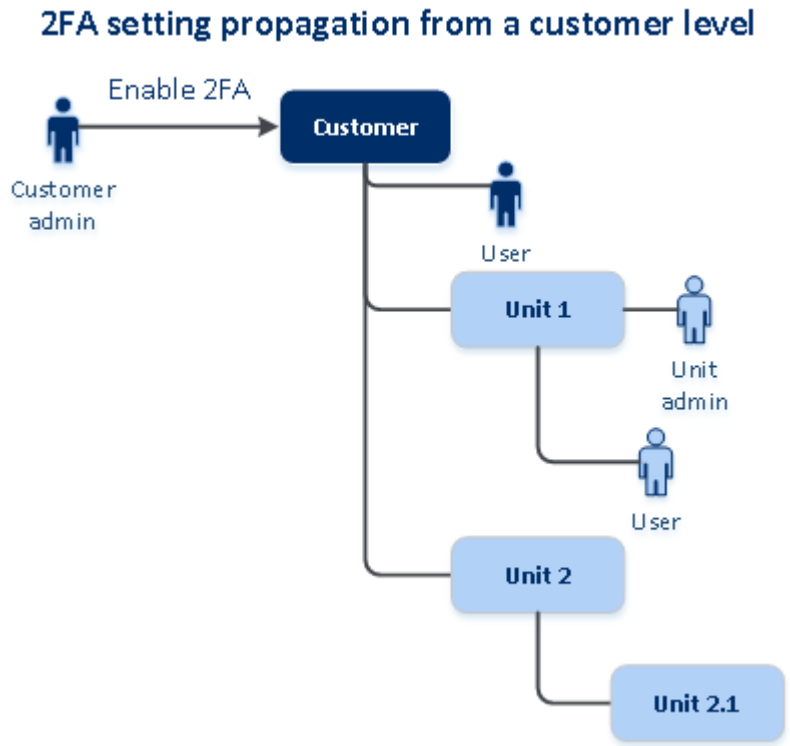
1. Utilice un nuevo dispositivo móvil.
2. Utilice el archivo PDF almacenado para enlazar un nuevo dispositivo (el nombre predeterminado del archivo es `cyberprotect-2fa-backupcode.pdf`).
3. Restaure el acceso a su cuenta desde la copia de seguridad. Asegúrese de que las copias de seguridad son compatibles 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 los inquilinos

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

Pasos para habilitar la autenticación de doble factor

Rol necesario: administrador de empresa

1. Inicie sesión en el portal de gestión.
2. Vaya a **Configuración** > **Seguridad**.
3. 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 **My empresa** > **Usuarios** y consulte la columna **Estado de la autenticación de doble factor**. El estado de autenticación de doble factor 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.

Pasos para deshabilitar la autenticación de doble factor

Rol necesario: administrador de empresa

1. Inicie sesión en el portal de gestión.
2. Vaya a **Configuración** > **Seguridad**.
3. Para deshabilitar la autenticación de doble factor, desactive el control deslizante y haga clic en **Deshabilitar**.
4. [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 **Mi empresa** > **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 **Mi empresa** > **Usuarios**.

Supervisión

En el portal de administración, en **Mi empresa** > **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 **Mi empresa** > **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 **Mi empresa** > **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 **Mi empresa** > **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 **Mi empresa** > **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.

Configuración de las automáticas del agente de Cyber Protection

Importante
Puede acceder a la funcionalidad de gestión de actualizaciones de agentes si tiene el servicio de Protección habilitado.

Este procedimiento se aplica a las actualizaciones de los siguientes agentes de Cyber Protection: Agente para Windows, Agente para Linux, Agente para Mac y Agente de Cyber Files Cloud para File Sync & Share.

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 las actualizaciones manuales o automáticas y sin supervisión de todos los agentes en todos los equipos.

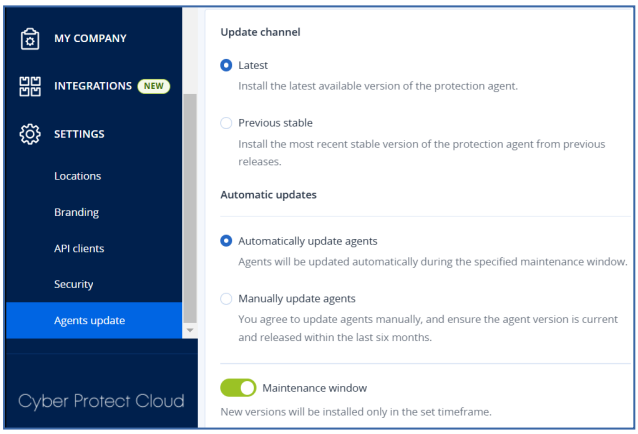
Nota
Para gestionar agentes en cada equipo y personalizar la configuración de actualización automática desde la consola de Cyber Protect, consulte la sección Actualización de agentes en la Cyber Protect Guía del usuario.

Actualizaciones automáticas

Nota
Si no tiene habilitado el servicio de Protección, la configuración de las actualizaciones automáticas del Agente para File Sync & Share se heredan de su proveedor de servicios.

Para ajustar la configuración predeterminada de las actualizaciones automáticas de los agentes en el portal de administración

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



2. En **Canal de actualización**, seleccione qué versión utilizar para las actualizaciones automáticas.

Opción	Descripción
Más reciente (seleccionada de manera predeterminada)	Instale la versión más reciente disponible del agente de Cyber Protection.
Anterior estable	Instale la versión estable más reciente de las versiones anteriores del agente de Cyber Protection.

3. Compruebe que la opción **Actualizar agentes automáticamente** esté activada.

Nota
Las actualizaciones automáticas solo están disponibles para los siguientes agentes:

- Agentes de Cyber Protect de la versiones 26986 (publicada en mayo de 2021) o posteriores.
- 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.

4. [Opcional] Establezca la ventana de mantenimiento.
   La ventana predeterminada es diaria, de 23:00 a 08:00 en el equipo donde está instalado el agente.

   Nota
   Aunque las actualizaciones de los agentes son rápidas y fluidas, 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. Haga clic en **Guardar**.

Actualizaciones manuales

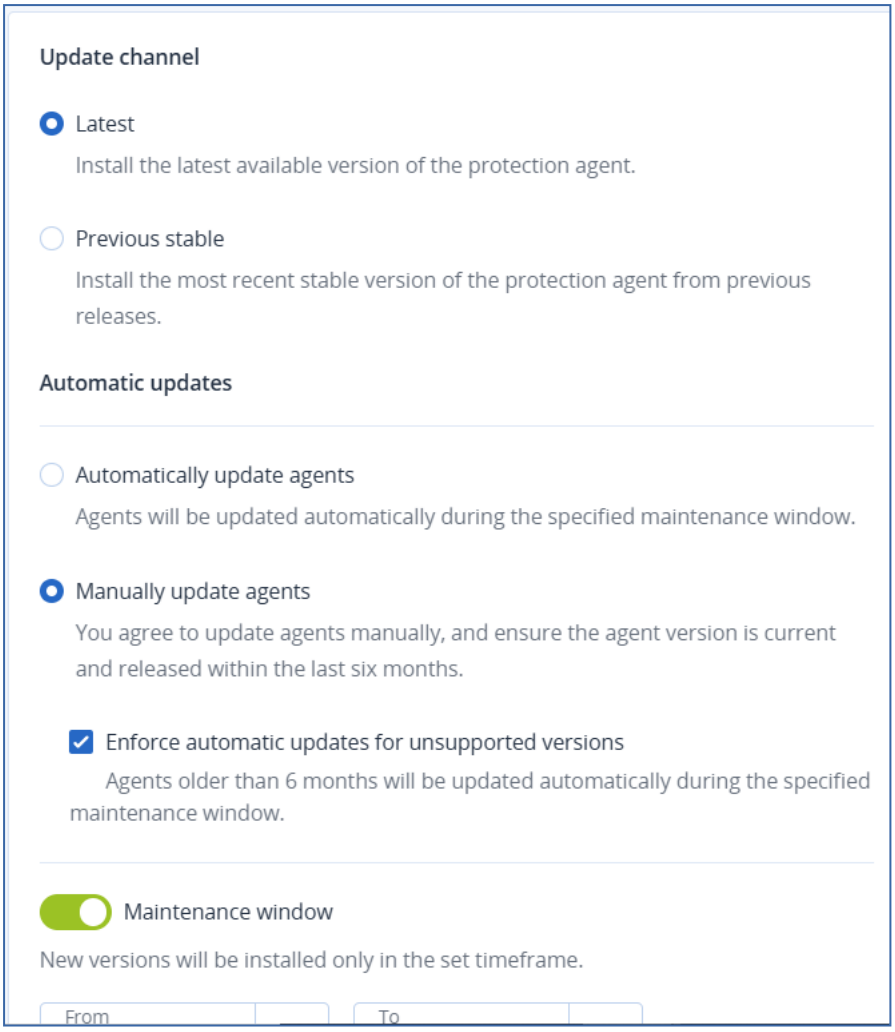
Importante
Le recomendamos encarecidamente que habilite las actualizaciones automáticas para sus agentes. Las actualizaciones periódicas garantizan que sus agentes estén actualizados, tengan un mejor rendimiento, solucionen errores y mejoren las funciones de protección y seguridad.

Para ajustar la configuración predeterminada para las actualizaciones manuales de los agentes en el portal de administración

1. Vaya a **Configuración** > **Actualización de agentes**.
2. En **Canal de actualización**, seleccione qué versión utilizar para las actualizaciones automáticas.

Opción	Descripción
Más reciente (seleccionada de manera predeterminada)	Instale la versión más reciente disponible del agente de Cyber Protection.
Anterior estable	Instale la versión estable más reciente de las versiones anteriores del agente de Cyber Protection.

3. Seleccione **Actualizar agentes manualmente.**



4. [Opcional] Para prevenir riesgos de seguridad, garantizar el acceso a las últimas funciones y minimizar los problemas técnicos causados por agentes significativamente obsoletos, habilite las actualizaciones automáticas de los agentes que tengan más de 6 meses.
   a. Seleccione **Imponer actualizaciones automáticas para las versiones no compatibles**.

      Importante
      Si de cara a la versión C25.02 no ha habilitado las actualizaciones automáticas de los agentes, esta opción se actualizará automáticamente para todos los inquilinos de su entorno.

   b. [Opcional] Establezca la ventana de mantenimiento.
      La ventana de mantenimiento predeterminada es diaria, de 23:00 a 08:00 en el equipo donde está instalado el agente.

      Nota
      Aunque las actualizaciones de los agentes son rápidas y fluidas, 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. Haga clic en **Guardar.**

Supervisión de las actualizaciones del agente

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

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

Almacenamiento inmutable

El almacenamiento inmutable es un tipo de almacenamiento de datos que impide que las copias de seguridad se alteren, modifiquen o eliminen durante un período definido. Garantiza que los datos permanezcan seguros e inalterables, para lo que proporciona una capa adicional de protección contra modificaciones no autorizadas o no intencionadas o ataques de ransomware. El almacenamiento inmutable está disponible para todas las copias de seguridad en la nube almacenadas en una instancia de almacenamiento en la nube compatible. Consulte "Almacenamientos y agentes admitidos" (p. 49).

Con el almacenamiento inmutable, puede acceder a copias de seguridad eliminadas durante el período 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 desaparecen 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.

Modos de almacenamiento inmutables

Un administrador puede deshabilitar y volver a habilitar el almacenamiento inmutable, así como cambiar el modo y el período de retención.

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.

Nota
A partir de la versión de septiembre de 2024, el modo de gobierno de almacenamiento inmutable con un período de retención de 14 días podría habilitarse automáticamente para su empresa. Consulte con su proveedor de servicios para obtener más información.

- **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.

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 por 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).

Configuración del almacenamiento inmutable

A partir de septiembre de 2024, el modo de gobierno de almacenamiento inmutable con un período de retención de 14 días está habilitado de forma predeterminada. Puede modificar la configuración predeterminada de su organización si es necesario.

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 cambiar el período de retención o el modo de almacenamiento inmutable

1. Inicie sesión en el portal de administración como administrador y vaya a **Configuración** > **Seguridad**.

2. Compruebe que el interruptor **Almacenamiento inmutable** esté activado.
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, si se le solicita, confirme su elección.
   - **Modo de gobierno**

     Este modo garantiza que el ransomware o los actores malintencionados no puedan manipular ni borrar los datos de copia de seguridad, ya que todas las copias de seguridad eliminadas se mantienen en el almacenamiento inmutable durante el período de retención que haya especificado. También garantiza la integridad de los datos de copia de seguridad, lo cual es fundamental para la recuperación ante desastres.

     En este modo, puede deshabilitar y volver a habilitar el almacenamiento inmutable, cambiar el período de retención o cambiar al modo de cumplimiento.
   - **Modo de cumplimiento normativo**

     Además de los beneficios del modo de gobierno, el modo de cumplimiento ayuda a las organizaciones a cumplir con los requisitos reglamentarios para la retención y la seguridad de los datos al evitar la manipulación de los mismos.

     Advertencia.
     La selección del modo de cumplimiento es irreversible. Después de seleccionar este modo, no puede deshabilitar el almacenamiento inmutable, cambiar el período de retención o volver al modo de gobierno.
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 agregar un archivo comprimido existente al almacenamiento inmutable, cree una nueva copia de seguridad en ese archivo comprimido al ejecutar el plan de protección correspondiente de forma manual o según un horario.

   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.
Deshabilitar el almacenamiento inmutable no entra en vigor de inmediato. Durante un periodo de gracia de 14 días (336 horas), puede acceder a las copias de seguridad eliminadas según su periodo de retención original.

Cuando finaliza el periodo de gracia, todas las copias de seguridad en el almacenamiento inmutable se eliminan de forma permanente. Por ejemplo, si desactiva el almacenamiento inmutable el 1 de octubre a las 10:00, todas las copias de seguridad que sigan en el almacenamiento inmutable el 15 de octubre a las 10:00 se eliminarán de forma permanente.

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

Visualización del uso del almacenamiento inmutable

Puede ver cuánto espacio utiliza el almacenamiento inmutable en la consola de Cyber Protect o en el informe de **Uso actual** que puede generar en el portal de administración.

Limitaciones

- El valor notificado incluye el tamaño total de todas las copias de seguridad eliminadas y los metadatos de los archivos de copia de seguridad en el almacenamiento. Los metadatos pueden ser hasta el 10 % del valor notificado.
- El valor muestra los datos de uso de hasta 24 horas antes.
- Si el uso real es inferior a 0,01 GB, se muestra como 0,0 GB.

Pasos para ver el uso del almacenamiento inmutable

En la consola de Cyber Protect

1. Inicie sesión en la consola de Cyber Protect.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad** y luego seleccione una ubicación de almacenamiento en la nube que admita almacenamiento inmutable.
3. Compruebe la columna **Almacenamiento inmutable y metadatos**.

En el informe de Uso actual

1. Inicie sesión en el portal de administración como administrador.
2. Vaya a **Informes** > **Uso**.
3. Seleccione **Uso actual** y haga clic en **Generar y enviar**.
   Se envía un informe en formato CSV y HTML a su dirección de correo electrónico.
   El archivo HTML se incluye en un archivo zip.
4. En el informe, compruebe la columna **Nombre del parámetro**.

Puede ver el uso del almacenamiento inmutable en la fila **Almacenamiento en la nube - Inmutable**.

Ejemplo de facturación para el almacenamiento inmutable

El siguiente ejemplo muestra una copia de seguridad eliminada que va al almacenamiento inmutable durante 14 días, que es el periodo de retención. Durante este periodo, la copia de seguridad eliminada utiliza espacio de almacenamiento. Cuando finalice el periodo de retención, la copia de seguridad eliminada se eliminará de forma permanente y el uso del almacenamiento disminuirá. Se cobrará el uso de almacenamiento correspondiente cada mes.

Fecha	Copias de seguridad	Uso de almacenamiento	Facturación
1 de abril	Se ha creado la copia de seguridad A (10 GB) Se ha creado la copia de seguridad B (1 GB)	10 GB + 1 GB = 11 GB	
20 de abril	Se ha eliminado la copia de seguridad B e irá al almacenamiento inmutable (con un período de retención de 14 días)	10 GB + 1 GB = 11 GB	
30 de abril			Se han facturado 11 GB para abril
4 de mayo	La copia de seguridad B se ha eliminado de forma permanente porque el periodo de retención ha terminado	11 GB - 1 GB = 10 GB	
31 de mayo			Se han facturado 10 GB para mayo

Habilitación de la formación avanzada en concienciación sobre seguridad para los usuarios de su organización

La formación en concienciación sobre seguridad es proporcionada por un proveedor de servicios de terceros, Wizer, como una integración en la consola de Cyber Protect Cloud. Si su proveedor de servicios ha habilitado el servicio para su organización, debe habilitar la integración para permitir que sus usuarios accedan a los materiales de formación.

Pasos para habilitar la integración con Wizer para una organización

Rol necesario: administrador de clientes, administrador de protección o administrador de cibernética.

Nota
La configuración inicial se realiza solo una vez.

1. Inicie sesión en la consola de Cyber Protect Cloud.
2. En el menú de navegación, haga clic en **Formación de concienciación sobre seguridad** > **Panel de control de concienciación**.
3. Haga clic en **Habilitar integración**.
4. Haga clic en **Habilitar** para confirmar.

Una vez que la integración está habilitada, se aprovisiona un nuevo inquilino para la organización en la plataforma de Wizer. Si ya tiene una cuenta en Wizer y desea utilizar esa cuenta en lugar de un nuevo inquilino, póngase en contacto con su proveedor de servicios.

Puede acceder al panel de administración de Wizer y añadir usuarios manualmente al importar un archivo CSV o configurar SSO con Active Directory, Octa, Google u otro proveedor de identidades. Consulte Cómo añadir usuarios.

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.

Importante
Al habilitar el control de inicio de sesión, se evita la recuperación desde el almacenamiento en la nube mediante el uso de un dispositivo de arranque no registrado. Consulte este artículo de la base de conocimiento.

Nota
- Esta restricción también se aplica al acceso al portal de administración mediante la API.
- Esta restricción se aplica solo en el nivel donde se establece. No se aplica a los miembros de los inquilinos secundarios.

Para limitar el acceso a la interfaz web

1. Inicie sesión en el portal de administración.
2. Vaya hasta la unidad en la que desee limitar el acceso.
3. Haga clic en **Configuración** > **Seguridad**.
4. Habilite el conmutador **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

Puede limitar el acceso a su empresa para los administradores de nivel superior.

Si, como administrador del portal de administración, limita el acceso a su empresa, los administradores de su partner proveedor de servicios solo podrán modificar las propiedades y las cuotas de su empresa y obtener informes de uso de ella y de sus clientes. No tendrán acceso a:

- Cualquier cosa dentro de su inquilino.
- Sus clientes, sus usuarios, servicios, copias de seguridad y otros recursos.

Pasos para limitar el acceso a su empresa

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

Gestión de tareas

Si su cuenta incluye el acceso al servicio Advanced Automation (PSA), 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 (PSA) 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 (PSA) 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 de ticket**, puede añadir destinatarios a los campos **Para** y **Cc**. También puede añadir comentarios y descripciones de texto enriquecido (incluyendo 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 la opción **Enviar correo electrónico al solicitante** para asegurarse de que cualquier actualización de ticket se envíe por correo electrónico al solicitante. Tenga en cuenta que cuando también se añaden destinatarios a los campos **Para** y **Cc**, las notificaciones solo se envían a estos destinatarios cuando se actualiza el ticket, no cuando se crea.
- 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 (PSA) 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. 55).

     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. 55).
4. Haga clic en **Guardar cambios**.

   Tenga en cuenta que si el interruptor **Enviar correo electrónico al solicitante** está habilitado, se envía un correo electrónico al usuario correspondiente y a cualquier destinatario definido en los campos **Para** y **Cc**.

Envío de tickets del servicio de asistencia a través del portal de tickets

El portal para enviar tickets permite a los clientes notificar problemas o solicitar asistencia técnica al enviar un formulario sencillo y de acceso público, sin necesidad de registrarse o iniciar sesión en el sistema.

Cuando se envía, se crea un nuevo ticket y se asigna automáticamente a un agente de asistencia del proveedor.

Nota
El proveedor habilita o deshabilita el formulario, al que pueden acceder usuarios registrados o no registrados. Tenga en cuenta que el proveedor también puede optar por restringir y no procesar solicitudes de usuarios no registrados.

Pasos para enviar un ticket a través del portal de tickets públicos

1. Vaya a la URL del portal de tickets públicos compartida por el proveedor.
2. En el diálogo Crear nuevo ticket, defina lo siguiente:

- En el campo **Título del ticket**, añada el título del ticket.
- En el campo **Dirección de correo electrónico**, introduzca su dirección de correo electrónico.
  Si el sistema reconoce la dirección de correo electrónico o el proveedor ha seleccionado no restringir las solicitudes de usuarios no registrados, se creará el ticket.
  Si no se reconoce la dirección de correo electrónico y el proveedor ha seleccionado no procesar solicitudes de usuarios no registrados, no se creará el ticket.
- [Opcional] En el campo **Número de teléfono**, introduzca un número de teléfono.
- En la sección **Detalles del ticket**, añada una descripción y comentarios (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 aparece.
- [Opcional] 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

3. Haga clic en **Enviar**.
   Aparece un mensaje de confirmación de que se ha creado el ticket. También se le notificará de lo mismo por correo electrónico.

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 del servicio y a través de ella se puede acceder a los servicios del inquilino en el que está operando.

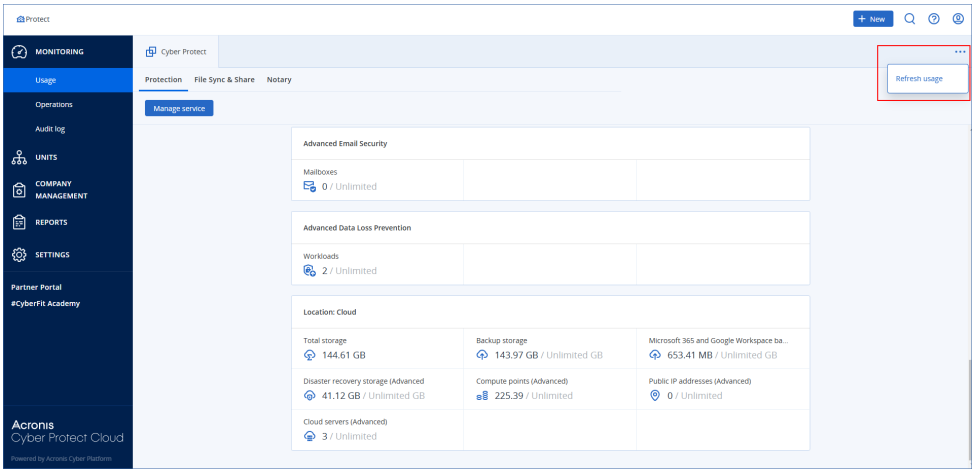
El uso de datos incluye las características estándar y avanzadas.

Importante
Los valores del uso de almacenamiento que se muestran en la interfaz de usuario del producto están en unidades de bytes binarios: mebibyte (MiB), gibibyte (GiB) y tebibyte (TiB), aunque las etiquetas muestren MB, GB y TB, respectivamente. Por ejemplo, si el uso real es de 3105886629888 bytes, el valor que aparece en la interfaz de usuario se muestra correctamente como 2,82, pero se etiqueta con TB en lugar de TiB.

El uso de almacenamiento de los recursos informáticos de Microsoft 365 y Google Workspace se informa por separado del almacenamiento general de copias de seguridad y se muestra en la sección **Copias de seguridad de Microsoft 365 y Google Workspace**.

Para actualizar los datos de uso que se muestran en la tabla, haga clic en el icono de elipsis (...) situado en la parte 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.



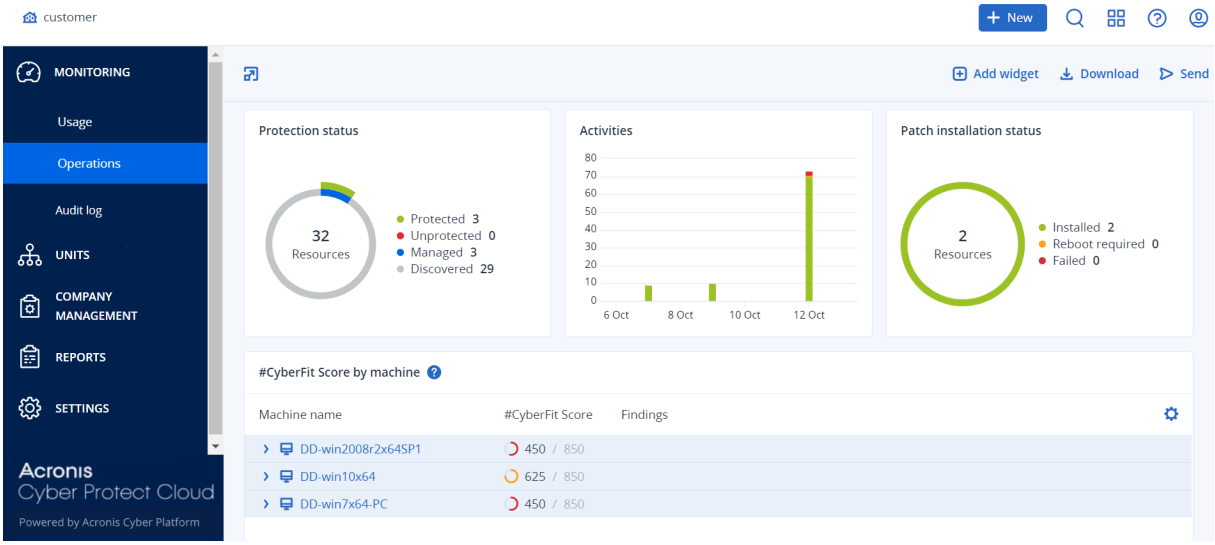
Panel de control de operaciones

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

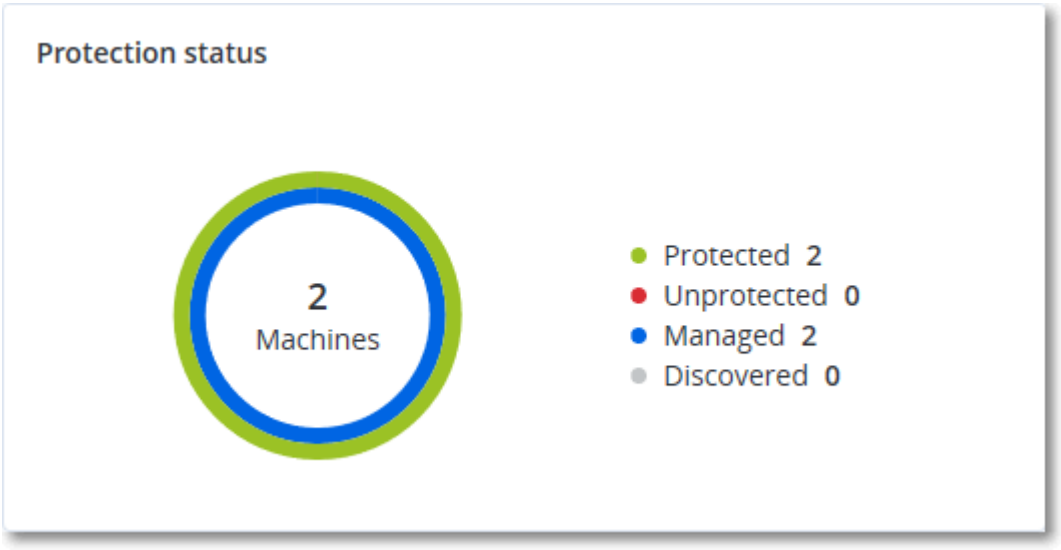
Estado de la protección

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

Un equipo puede encontrarse en uno de los siguientes estados:

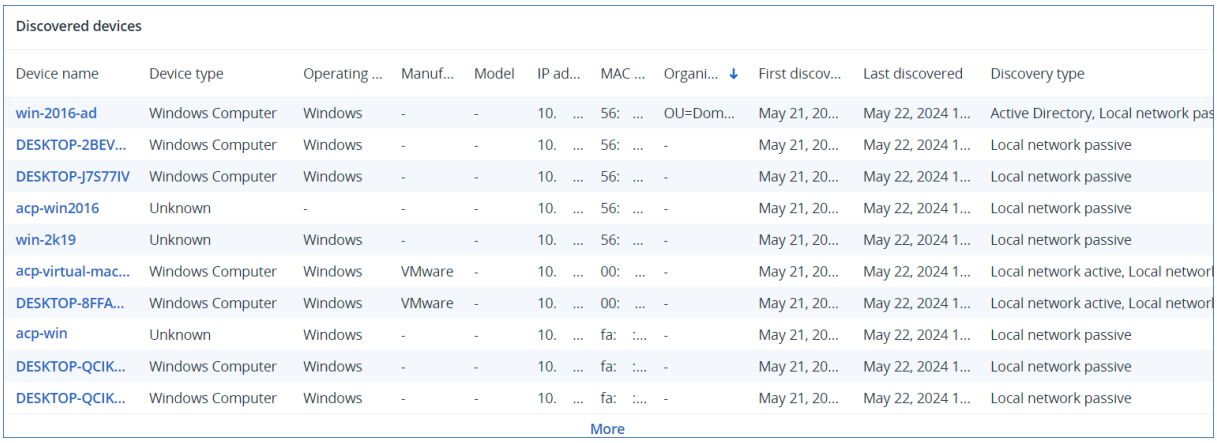
- **Protegido**: equipos con un plan de protección aplicado.
- **Sin protección**: equipos sin un plan de protección aplicado. Incluyen tanto a los equipos detectados como a los gestionados en los que no hay ningún plan de protección aplicado.
- **Gestionado**: equipos en los que está instalado un agente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



Dispositivos detectados

Este widget muestra información detallada acerca de los dispositivos que se detectaron en las redes de la organización. La información del dispositivo incluye el tipo de dispositivo, el fabricante, el sistema operativo, la dirección IP, la dirección MAC, la fecha de detección, etc.



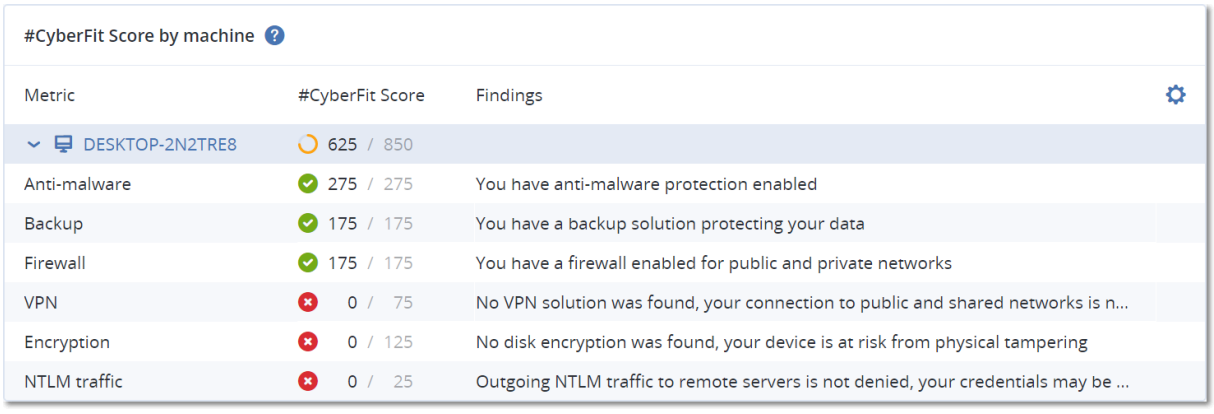
#CyberFit Score por equipo

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)

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

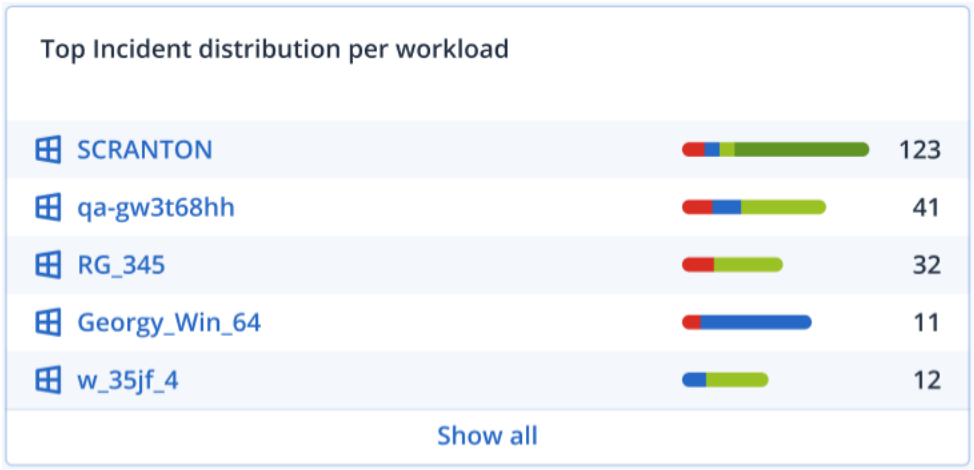
Los widgets disponibles son los siguientes:

- 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.

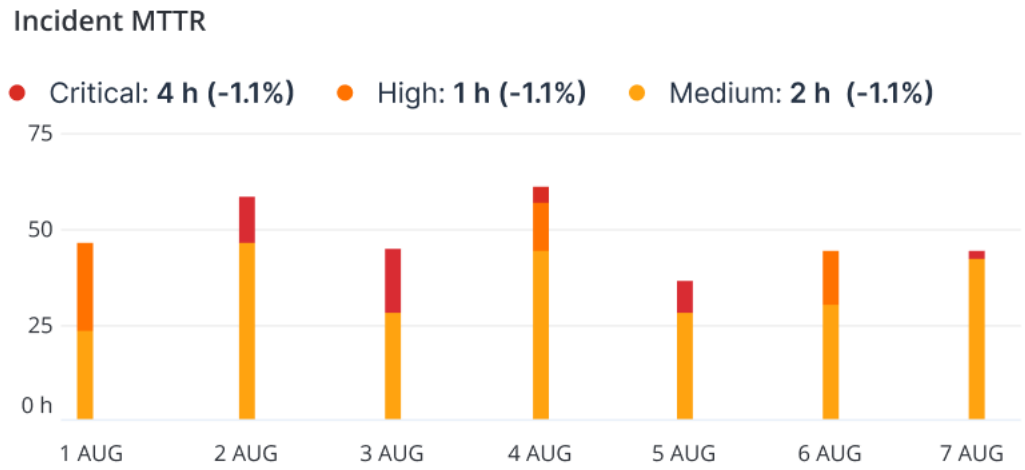
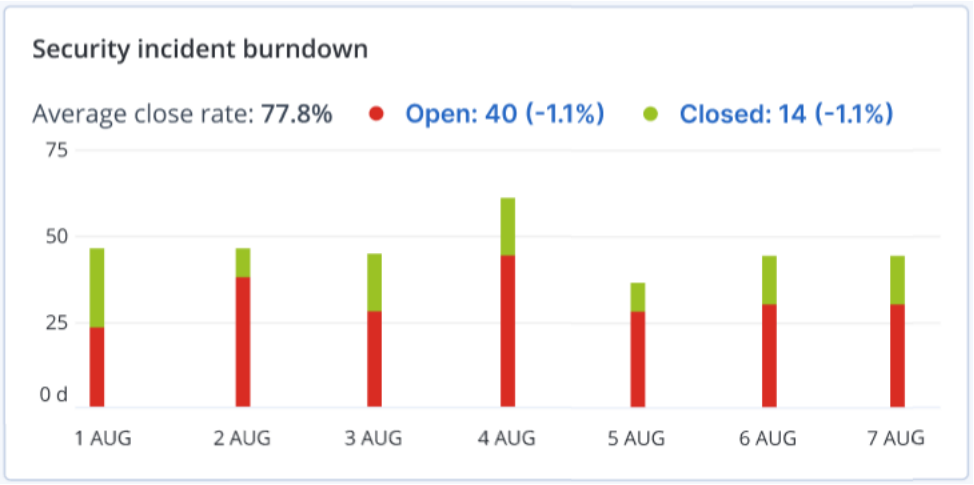


Gráfico de quemado de incidentes de seguridad

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**).

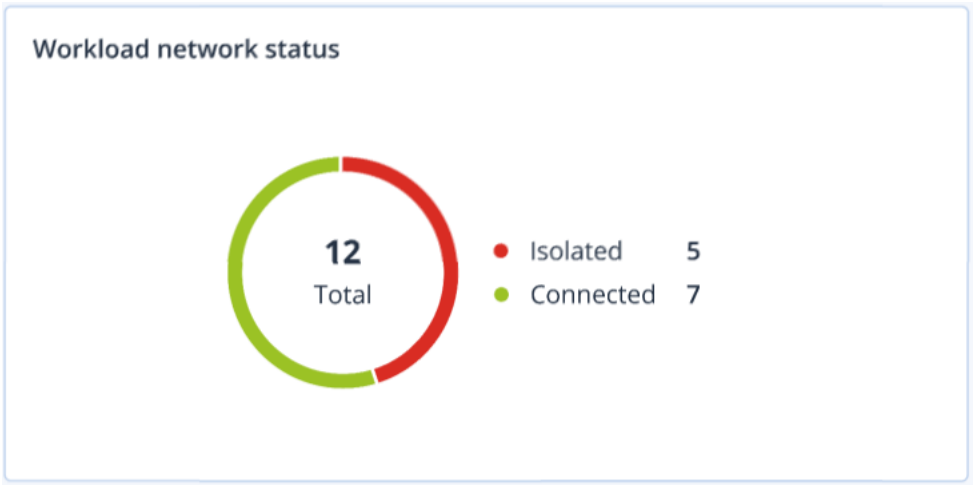
El valor % mostrado entre paréntesis indica el aumento o descenso en comparación con el periodo de tiempo anterior.



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.
- No se admiten los dispositivos de almacenamiento externos.

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 %.

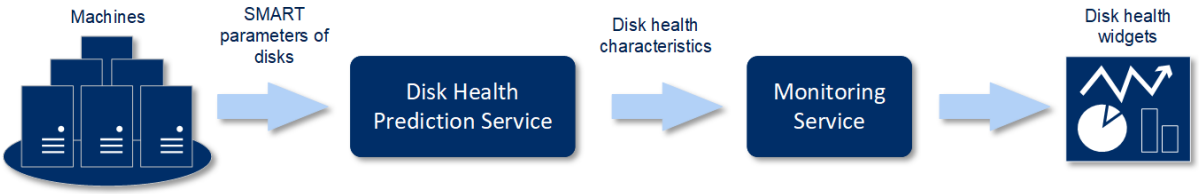
- **Crítico**:
  El estado del disco se encuentra entre el 0 y el 30 %.
- **Calculando datos del disco**:
  Se están calculando tanto el estado del disco actual como su previsión.

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.

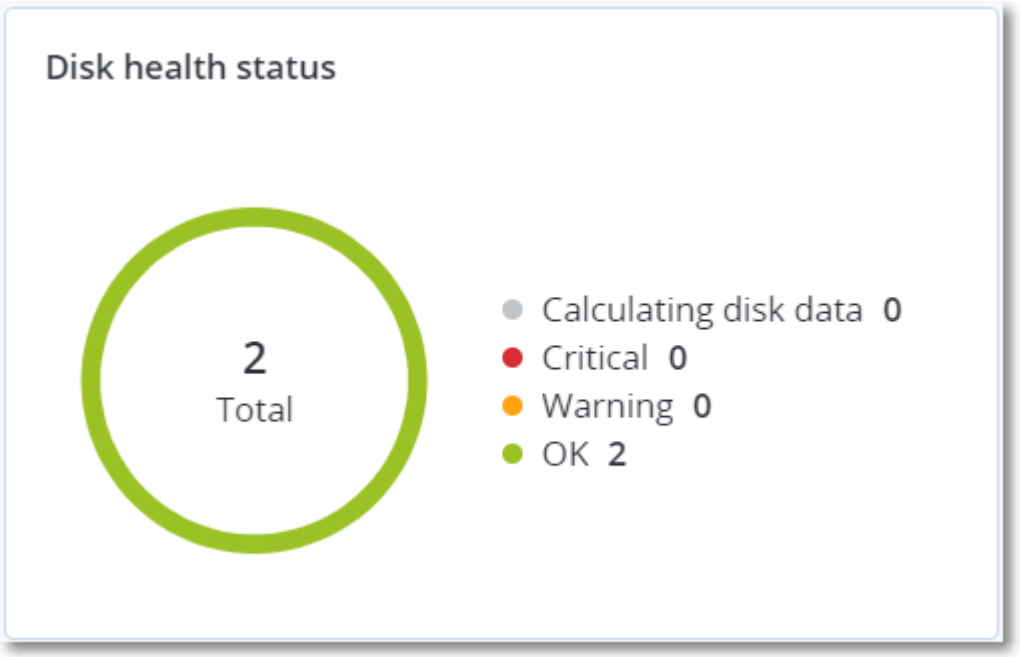
- **Resumen del estado del disco**: Es un widget en estructura de árbol con dos niveles de datos que se pueden cambiar al desplazarse.
  - Nivel de equipo:
    Muestra información resumida sobre el estado del disco de los equipos de los clientes

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:

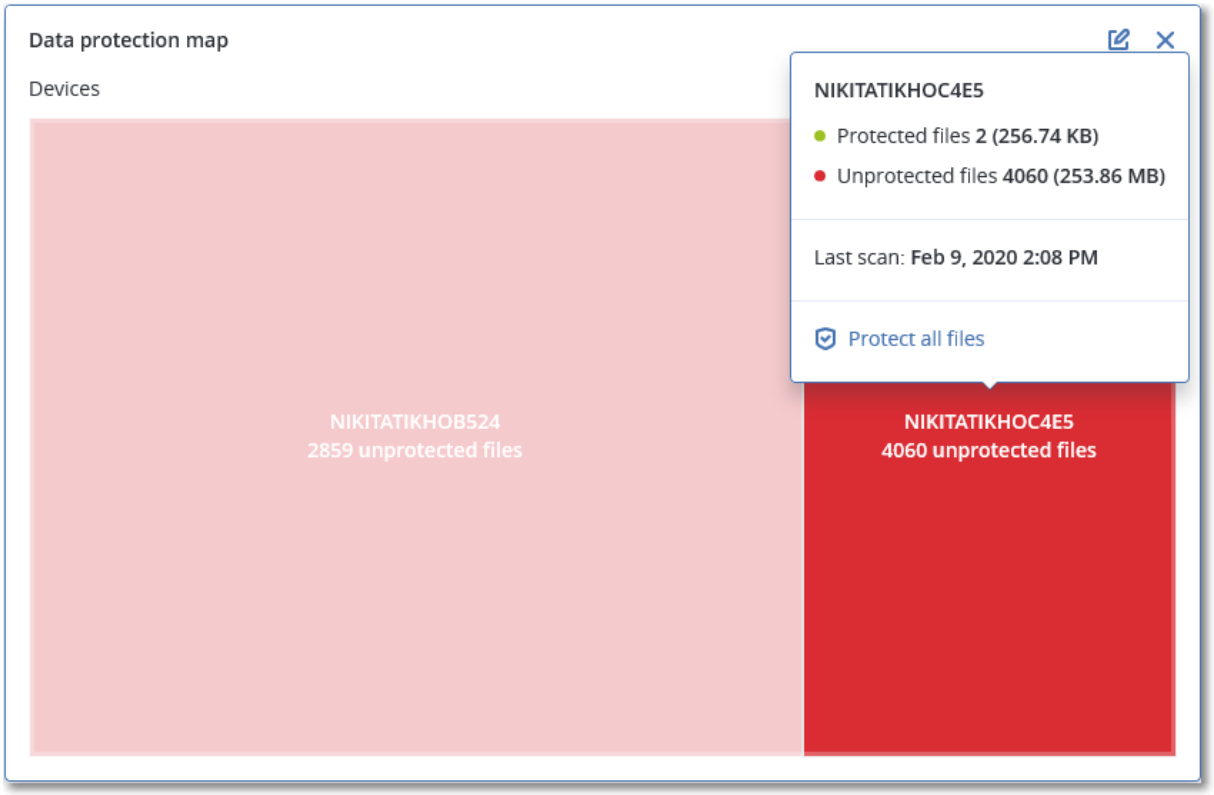
- **Crítico**: hay entre un 51 y un 100 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ni se va a realizar ninguna copia de seguridad con la configuración de copias de seguridad existentes para la ubicación, el inquilino cliente o el equipo seleccionado.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

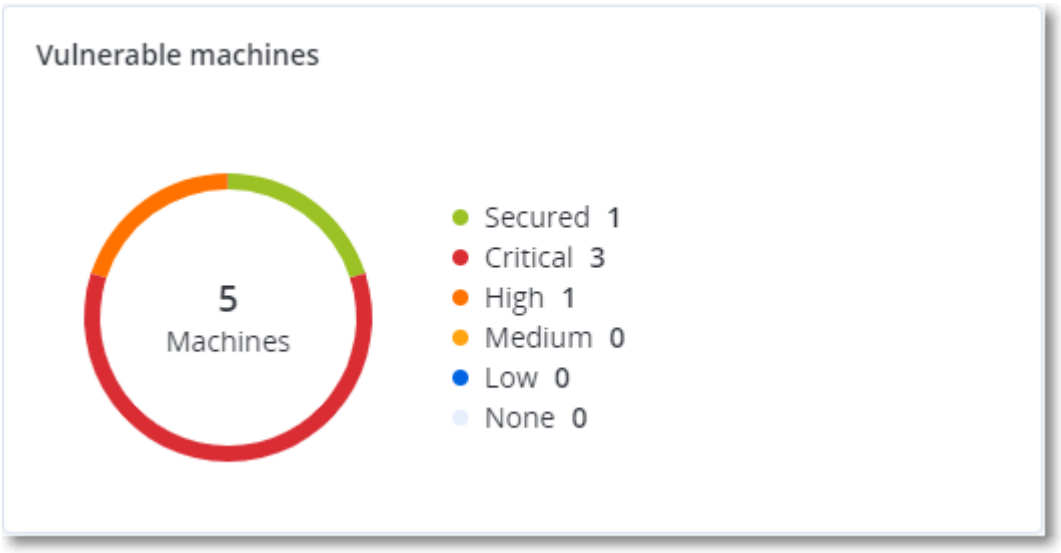
Widgets de evaluación de vulnerabilidades

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

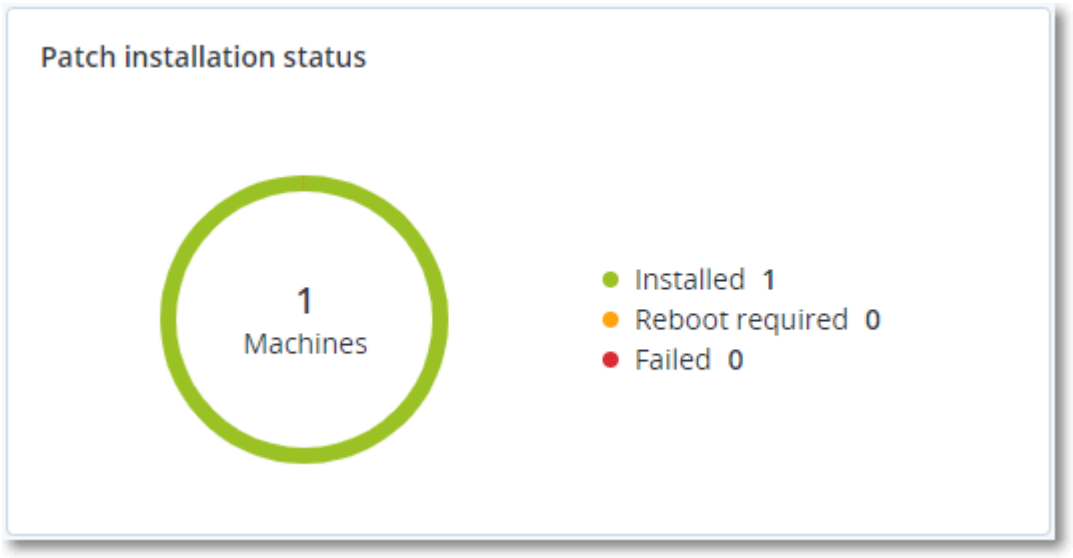
Widgets de instalación de parches

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

Estado de instalación del parche

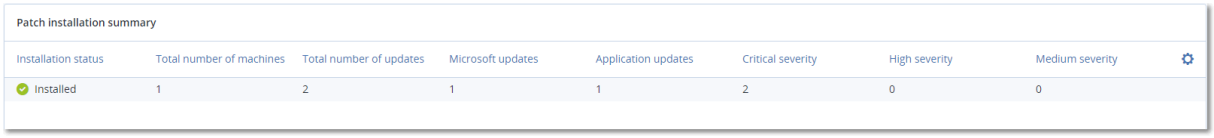
Este widget muestra el número de equipos agrupados por estado de instalación de parches.

- **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.

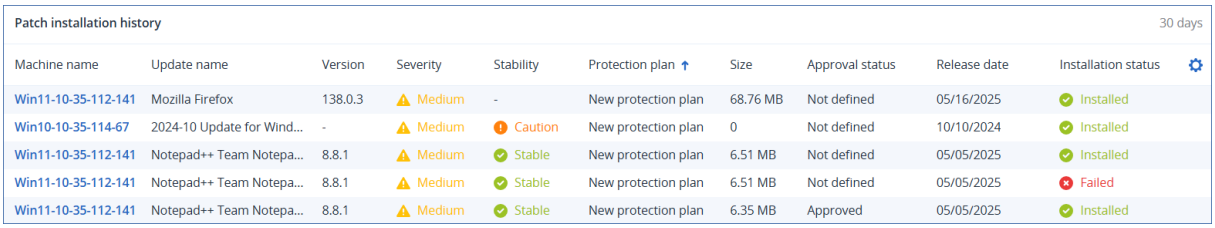


Patch installation summary

Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

Historial de instalación de parches

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



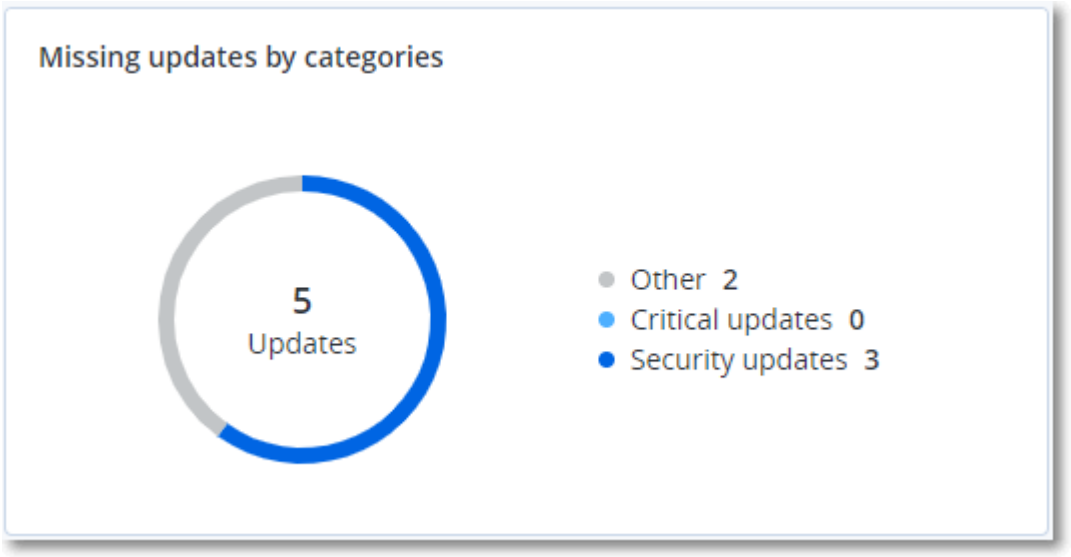
Patch installation history — 30 days

Machine name	Update name	Version	Severity	Stability	Protection plan	Size	Approval status	Release date	Installation status
Win11-10-35-112-141	Mozilla Firefox	138.0.3	Medium	-	New protection plan	68.76 MB	Not defined	05/16/2025	Installed
Win10-10-35-114-67	2024-10 Update for Wind...	-	Medium	Caution	New protection plan	0	Not defined	10/10/2024	Installed
Win11-10-35-112-141	Notepad++ Team Notepa...	8.8.1	Medium	Stable	New protection plan	6.51 MB	Not defined	05/05/2025	Installed
Win11-10-35-112-141	Notepad++ Team Notepa...	8.8.1	Medium	Stable	New protection plan	6.51 MB	Not defined	05/05/2025	Failed
Win11-10-35-112-141	Notepad++ Team Notepa...	8.8.1	Medium	Stable	New protection plan	6.35 MB	Approved	05/05/2025	Installed

Actualizaciones que faltan por categoría

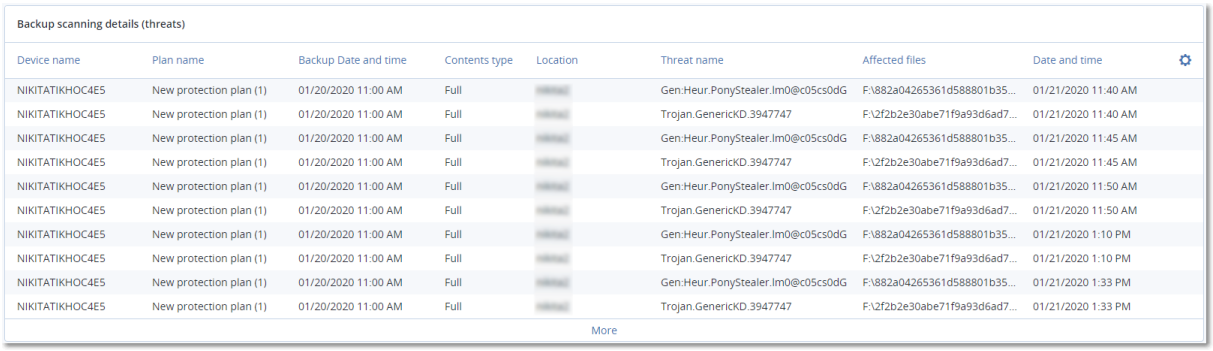
Este widget muestra el número de actualizaciones que faltan por categoría. Se muestran las siguientes categorías:

- Actualizaciones de seguridad
- Actualizaciones críticas
- Otros



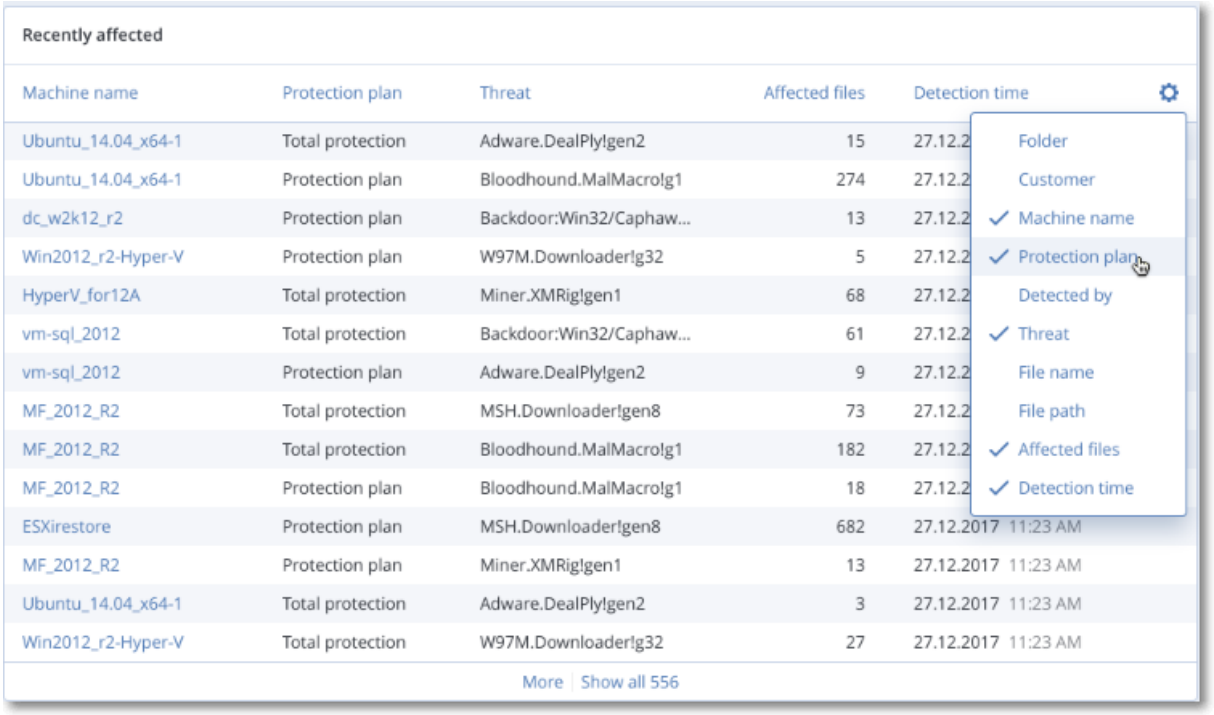
Detalles del análisis de copias de seguridad

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

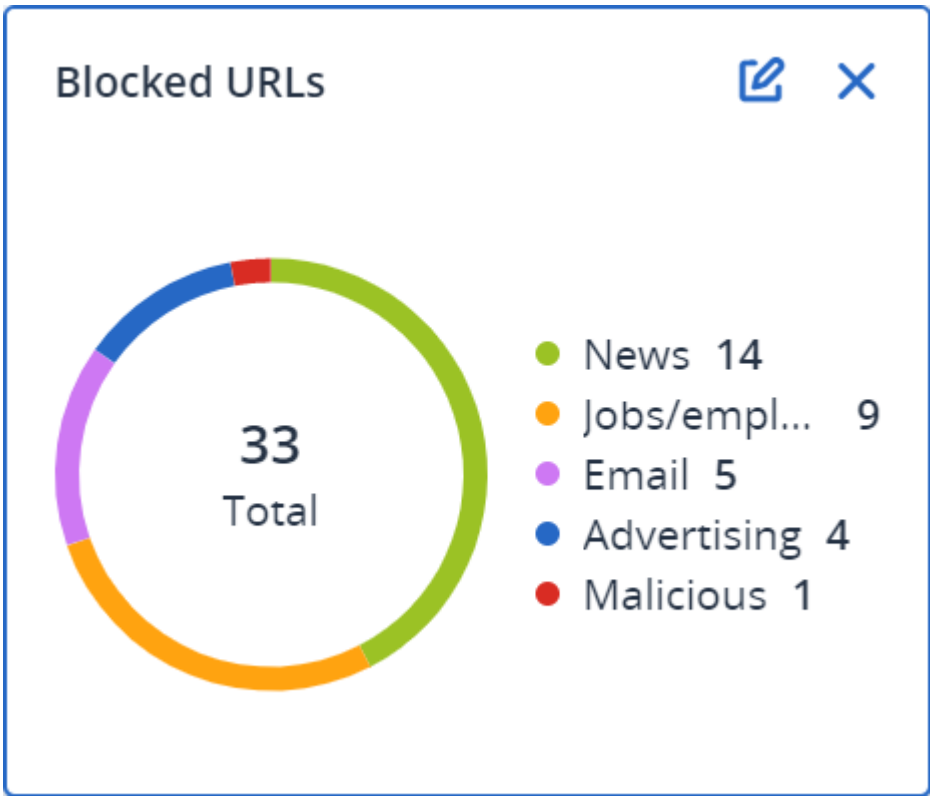
Puede descargar los datos de las cargas de trabajo que se han visto afectadas, generar un archivo CSV y enviarlo a los destinatarios que especifique.

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.

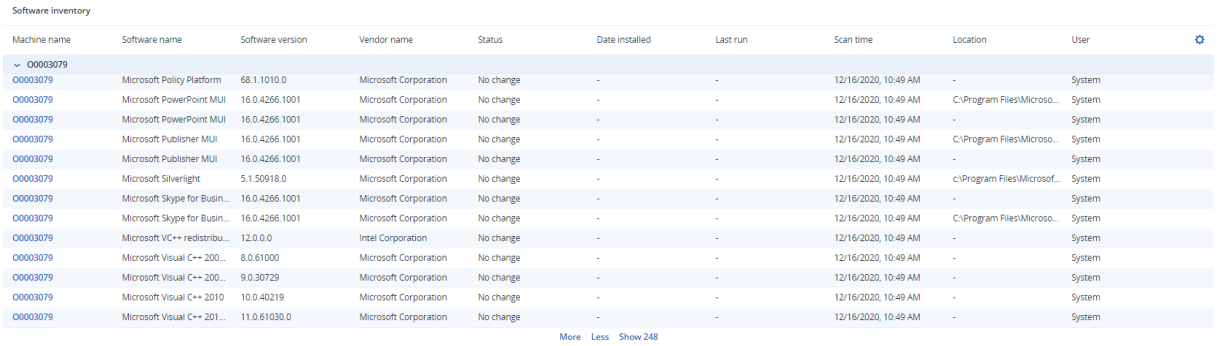
URL bloqueadas

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 guía del usuario de ciberprotección.



Widgets de inventario de software

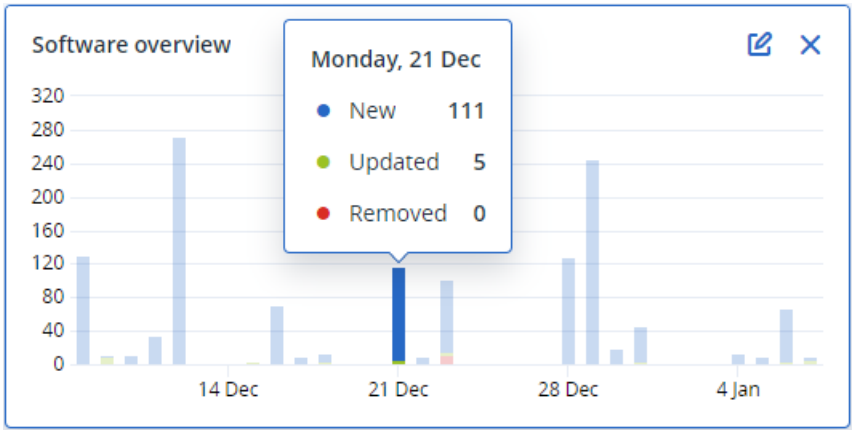
El widget de tabla de **Inventario de software** muestra información detallada sobre todo el software que se ha instalado en dispositivos de Windows y macOS en su organización.


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.

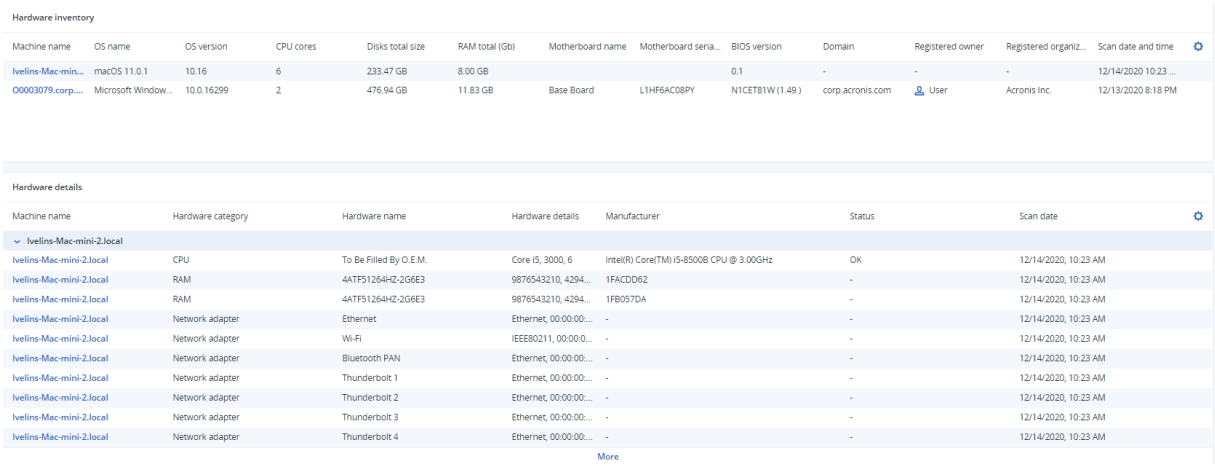
Actualizadas: el número de aplicaciones actualizadas.

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

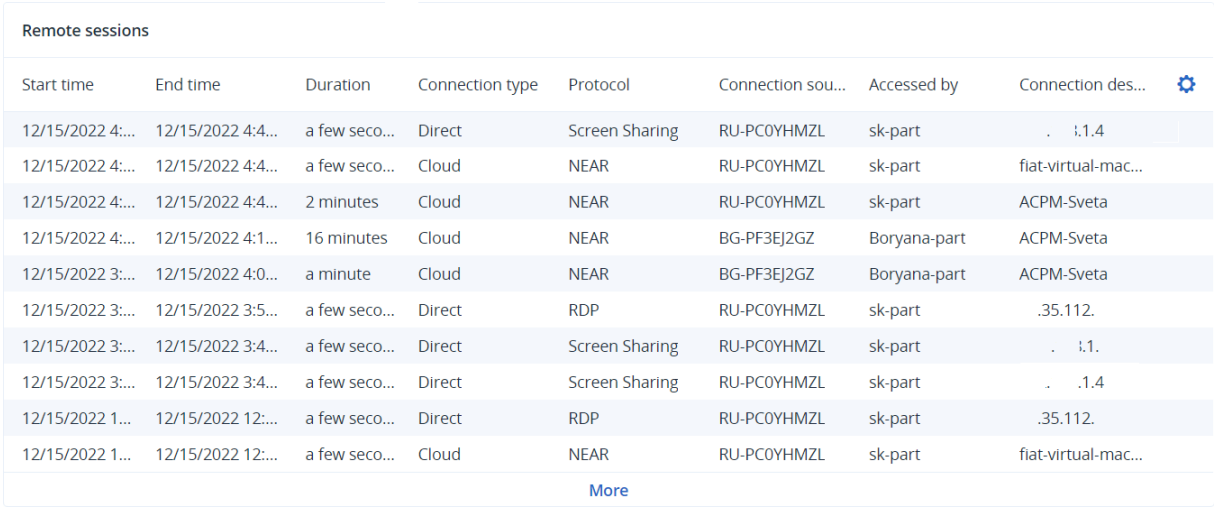
Los widgets de tablas de **inventario de hardware** y de **detalles de hardware** muestran información sobre todo el hardware instalado en dispositivos físicos y virtuales de Windows y macOS en su organización.



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).

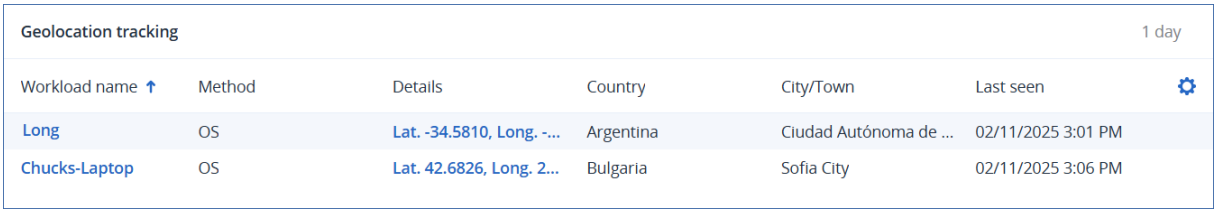
Historial de sesión

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.



Widget de seguimiento de geolocalización

En el widget de **Seguimiento de geolocalización**, puede ver detalles sobre la ubicación de las cargas de trabajo de su organización, como el país, la ciudad o la población, las coordenadas, la última vez que se vio y el método de seguimiento de geolocalización.

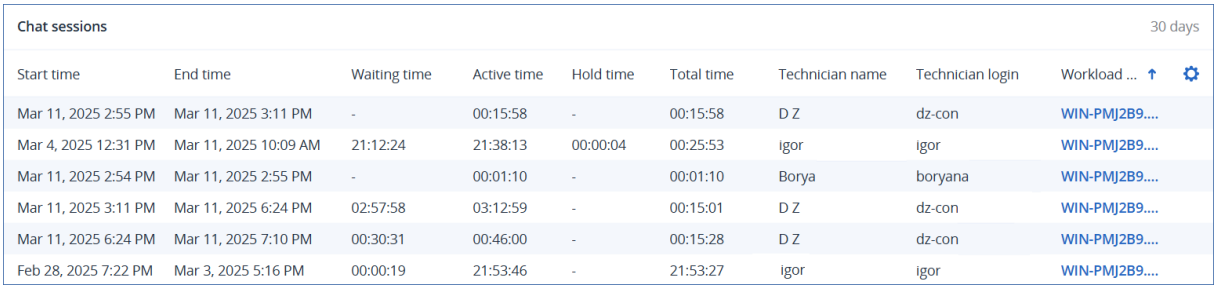


Geolocation tracking — 1 day

Workload name	Method	Details	Country	City/Town	Last seen
Long	OS	Lat. -34.5810, Long. -...	Argentina	Ciudad Autónoma de ...	02/11/2025 3:01 PM
Chucks-Laptop	OS	Lat. 42.6826, Long. 2...	Bulgaria	Sofia City	02/11/2025 3:06 PM

Widget de sesiones de chat

En el widget **Sesiones de chat**, puede ver detalles sobre las sesiones de chat remotas en su organización durante un período especificado.

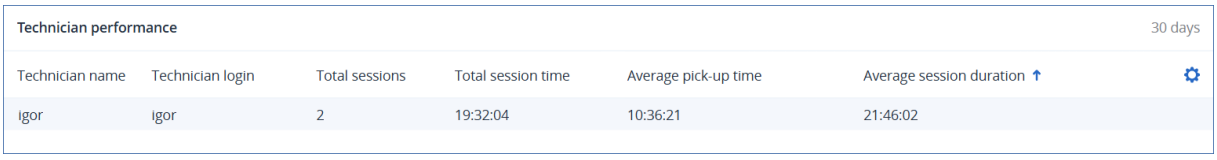


Chat sessions — 30 days

Start time	End time	Waiting time	Active time	Hold time	Total time	Technician name	Technician login	Workload ...
Mar 11, 2025 2:55 PM	Mar 11, 2025 3:11 PM	-	00:15:58	-	00:15:58	D Z	dz-con	WIN-PMJ2B9....
Mar 4, 2025 12:31 PM	Mar 11, 2025 10:09 AM	21:12:24	21:38:13	00:00:04	00:25:53	igor	igor	WIN-PMJ2B9....
Mar 11, 2025 2:54 PM	Mar 11, 2025 2:55 PM	-	00:01:10	-	00:01:10	Borya	boryana	WIN-PMJ2B9....
Mar 11, 2025 3:11 PM	Mar 11, 2025 6:24 PM	02:57:58	03:12:59	-	00:15:01	D Z	dz-con	WIN-PMJ2B9....
Mar 11, 2025 6:24 PM	Mar 11, 2025 7:10 PM	00:30:31	00:46:00	-	00:15:28	D Z	dz-con	WIN-PMJ2B9....
Feb 28, 2025 7:22 PM	Mar 3, 2025 5:16 PM	00:00:19	21:53:46	-	21:53:27	igor	igor	WIN-PMJ2B9....

Widget de rendimiento técnico

En el widget **Rendimiento del técnico**, puede ver detalles sobre el rendimiento de cada técnico en su organización durante un período determinado.



Technician performance — 30 days

Technician name	Technician login	Total sessions	Total session time	Average pick-up time	Average session duration
igor	igor	2	19:32:04	10:36:21	21:46:02

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

- Operaciones relacionadas con el archivado de correos electrónicos
- 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:

- **Suceso**
  Descripción breve del evento. Por ejemplo, **Se ha creado el inquilino**, **Se ha eliminado el inquilino**, **Se ha creado el usuario**, **Se ha eliminado el 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 el inquilino**, **Se ha eliminado el usuario** o **Se ha alcanzado la cuota**.
  - **Aviso**
    Indica que es posible que un evento requiera atención. Por ejemplo, **Se ha actualizado el inquilino** o **Se ha actualizado el usuario**.
  - **Informativo**
    Indica una acción o un cambio informativo neutral. Por ejemplo, **Se ha creado el inquilino**, **Se ha creado el 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 el 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 el 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.

Recopilación de datos de rendimiento para los agentes de Cyber Protection

Para los equipos Windows protegidos en su entorno, puede recopilar los registros de rendimiento manualmente o habilitar la recopilación automática de datos de diagnóstico si el rendimiento del sistema cae por debajo de los umbrales definidos de fábrica. Consulte "Umbrales de rendimiento para la recopilación de datos ETL" (p. 83).

Los registros recopilados se anonimizan antes de enviarse para su análisis al proveedor. Se eliminarán los siguientes datos de todos los registros, mensajes, alertas y mensajes de error:

- Cuenta de usuario
- Nombre de la empresa
- Nombre de la carga de trabajo protegida

Como administrador de la empresa, puede habilitar la recopilación automática de registros para agentes seleccionados aleatoriamente o para agentes específicos en su organización.

Nota
- La recopilación de datos automatizada en cargas de trabajo individuales es posible con la versión 24.4.37758 o posterior del agente Cyber Protection para Windows.
- La recopilación de datos de rendimiento a nivel de inquilino es posible con la versión 25.03.XXXXX o posterior del agente Cyber Protection para Windows.

Para garantizar que nuestras recomendaciones de soporte estén bien fundamentadas, recopilamos datos de aproximadamente el 10 % de los agentes en el entorno para su análisis.

Esto no anula la configuración de las cargas de trabajo individuales. Por ejemplo, si la recopilación de datos automática está deshabilitada en una carga de trabajo específica, esa carga de trabajo no se incluirá en la recopilación de datos masiva.

Recopilación automatizada para varios agentes

Para habilitar la recopilación automatizada de datos de rendimiento para varios agentes en un inquilino

Rol necesario: Administrador de clientes

1. En la consola de Cyber Protect Cloud, vaya a **Configuración** > **Agentes**.
2. En el menú **Acciones** de la derecha, haga clic en **Editar la configuración del monitor de rendimiento**.
3. En la sección **Monitor de rendimiento**, active el conmutador **Recopilación y subida automáticas de registros de rendimiento**.

Los datos recopilados automáticamente se almacenan en los discos locales de los equipos protegidos, en la carpeta `C:\ProgramData\Acronis\ETLTool\ETL\`, anonimizados, y se envían al proveedor de servicios para su análisis.

Nota
El límite para enviar registros de ETL a la nube es de 3 veces en 24 horas.

Recopilación automática para un solo agente

Para habilitar la recopilación automatizada de datos de rendimiento para un agente específico

1. A nivel de empresa, en la consola de Cyber Protect Cloud, navegue a **Configuración** > **Agentes**.
2. En la lista **Agentes**, busque el agente para el que desee habilitar la supervisión de rendimiento.
3. En el menú **Acciones** de la derecha, haga clic en **Detalles**.
4. Desplácese hacia abajo hasta la sección **Monitor de rendimiento** y active el interruptor **Permitir que este agente recopile registros de rendimiento automáticamente**.

Los datos recopilados automáticamente se almacenan en el disco local del equipo protegido, en la carpeta `C:\ProgramData\Acronis\ETLTool\ETL\`.

Recopilación manual

Pasos para recopilar datos de rendimiento de forma manual

Puede recopilar datos de rendimiento bajo demanda, sin tener que habilitar la supervisión de rendimiento y la recopilación automatizada de datos de rendimiento.

1. Inicie sesión en el equipo protegido como usuario administrador.
2. En el símbolo del sistema, ejecute uno de los siguientes comandos:
   - `"C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o`
     La recopilación de un seguimiento ETL se ejecutará hasta que presione la tecla `S` del teclado o cuando se agote el límite de tiempo máximo de 3600 segundos.

- `"C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o -i X`
  Donde X es el límite de tiempo en segundos para la recopilación de datos, y el valor máximo es 3600. Puede detener la recopilación en cualquier momento al presionar la tecla `S` del teclado.

Los datos recopilados manualmente se almacenan en el disco local del equipo protegido, en la carpeta `C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\`

Pasos para recopilar los registros de rendimiento

1. Inicie sesión en el equipo protegido como usuario administrador.
2. Localice los datos que necesita:
   - Los datos de rendimiento recopilados automáticamente se encuentran en la carpeta `C:\ProgramData\Acronis\ETLTool\ETL\`
   - Los datos de rendimiento recopilados bajo demanda se encuentran en la carpeta `C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\`

Los seguimientos ETL también se incluyen en el paquete `sysinfo`.

Umbrales de rendimiento para la recopilación de datos ETL

Puede habilitar la recopilación automática de datos de rendimiento para los equipos Windows protegidos en su entorno. La supervisión se configura en la consola de Cyber Protect Cloud por agente y permite la recopilación automática de datos de diagnóstico si el rendimiento del sistema cae por debajo de los umbrales predefinidos.

La recopilación de datos automatizada comienza cuando se supera uno de los umbrales.

Umbrales predeterminados para la recopilación de datos de ETL

La siguiente tabla indica los umbrales que activan la recopilación automática de datos de ETL.

Parámetro	Descripción	Valor predeterminado
"process-memory-consumption"	Umbral de uso excesivo de memoria	
"allocated-memory-percent"		15
"minimum-allocated-memory-duration-seconds"		10
"allocated-memory-free-limit-seconds"		300
"process-disk-io"	Umbral de uso elevado de E/S del disco	
"maximum-operations-number"		10000

Parámetro	Descripción	Valor predeterminado
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-file-io"	Umbral de uso elevado de E/S del archivo	
"maximum-operations-number"		30000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-cpu-usage"	Umbral de consumo elevado de la CPU	
"cpu-percent"		15
"estimation-period-seconds"		10
"acronis-component-thresholds"	Rendimiento de los componentes del agente de protección	
"behavioral-engine"	Umbral del motor de comportamiento	
"average-system-utilization-percent"		50
"be-stats-event-number"		10
"avc-scan"	Umbral del componente de protección antivirus y antimalware	
"average-scan-duration-seconds"	Duración media máxima del análisis	3
"estimation-period-seconds"		10
"maximum-scan-duration-seconds"	Duración máxima de un único análisis	5

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.

Importante
Los valores del uso de almacenamiento que se muestran en la interfaz de usuario del producto están en unidades de bytes binarios: mebibyte (MiB), gibibyte (GiB) y tebibyte (TiB), aunque las etiquetas muestren MB, GB y TB, respectivamente. Por ejemplo, si el uso real es de 3105886629888 bytes, el valor que aparece en la interfaz de usuario se muestra correctamente como 2,82, pero se etiqueta con TB en lugar de TiB.

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.

  Nota
  Los datos de uso del almacenamiento local solo se comunican a nivel de unidad y de inquilino de cliente. Los usuarios no reciben información sobre el uso del almacenamiento local en los informes de resumen.

- **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 incluirá las métricas de uso del servicio para todos los inquilinos secundarios del inquilino en el que está operando y para todos los usuarios dentro de los inquilinos.

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.
- Tamaño total de las copias de seguridad.
- Número total de dispositivos protegidos.
- Precio total.

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

Importante
Los valores del uso de almacenamiento que se muestran en la interfaz de usuario del producto están en unidades de bytes binarios: mebibyte (MiB), gibibyte (GiB) y tebibyte (TiB), aunque las etiquetas muestren MB, GB y TB, respectivamente. Por ejemplo, si el uso real es de 3105886629888 bytes, el valor que aparece en la interfaz de usuario se muestra correctamente como 2,82, pero se etiqueta con TB en lugar de TiB.

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. 106).

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.
Dispositivos detectados	Muestra todos los dispositivos que se detectaron en las redes de su 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

Añadir

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.

Vista

Pasos para ver un informe

- Para ver un informe, haga clic en su nombre.

Editar

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.
3. En la esquina superior derecha de la pantalla, haga clic en **Configuración**.
4. Edite el informe y haga clic en **Guardar**.

Eliminar

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. En la esquina superior derecha de la pantalla, haga clic en el icono de elipsis (...) y luego en **Eliminar informe**.
4. Haga clic en **Eliminar** en la ventana de confirmación.

Planificación

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.
3. En la esquina superior derecha de la pantalla, haga clic en **Configuración**.
4. Junto a **Programado**, habilite el conmutador.
   - 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.
5. Haga clic en **Guardar**.

Descargar

Pasos para descargar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe.
3. En la esquina superior derecha de la pantalla, haga clic en **Descargar**.
4. Seleccione el formato del informe.

Como resultado, se descarga un archivo en el formato seleccionado a su equipo.

Si ha seleccionado **Excel y PDF**, se descargará un archivo ZIP en su equipo.

Enviar

Pasos para enviar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe.
3. En la esquina superior derecha de la pantalla, haga clic en **Enviar**.
4. Especifique las direcciones de correo electrónico de los destinatarios.

5. Seleccione el formato del informe.
6. Haga clic en **Enviar**.

Estructura de exportación

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. En la esquina superior derecha de la pantalla, haga clic en el icono de elipsis (...) y luego en **Exportar**.

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

Volcar datos

Para volcar los datos del informe

Puede exportar todos los datos de un periodo personalizado, sin filtrarlos, a un archivo CSV y enviar el archivo CSV a un destinatario de correo electrónico. El archivo CSV solo contiene datos acerca de los widgets que se incluyen en el informe.

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. En la esquina superior derecha de la pantalla, haga clic en el icono de elipsis (...) y luego 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, Disaster Recovery, 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 su organización 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 recursos informáticos Usuarios. La suma de estos recursos informáticos es 10 500, lo que excede el límite de 10 000 de un grupo de recursos informáticos. Por lo tanto, el widget ocultará los correspondientes tipos de recursos informáticos: 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 DR**: el número total de servidores protegidos por Disaster Recovery. **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).
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**.
Dispositivos detectados	El widget muestra la siguiente información acerca de los dispositivos que se descubrieron en las redes de su organización en un período especificado: **Nombre de dispositivo** **Tipo de dispositivo** **Sistema operativo** **Fabricante** **Modelo** **Dirección IP** **Dirección MAC** **Unidad organizativa** Puede editar el widget y filtrar la información que se muestra por unidad organizativa, tipo de dispositivo, tipo de detección, fecha de la primera detección, fecha de la última detección, dirección IP, dirección MAC y tipo de detección.

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 **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

Widget	Descripción
	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).
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.

Widget	Descripción
	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 almacenamiento de copia de seguridad	El widget muestra el número y el tamaño totales de las copias de 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

Widget	Descripción
	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 software

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

Widget	Descripción
Estado de instalación	Este widget muestra el número total de actividades de instalación, agrupadas por estado. Al hacer clic en un segmento del gráfico circular, se redirige a la página **Actividades**, donde solo se muestran las actividades con el estado correspondiente, ordenadas cronológicamente.
Estado de desinstalación	El widget muestra el número total de actividades de desinstalación, agrupadas por estado. Al hacer clic en un segmento del gráfico circular, se redirige a la página **Actividades**, donde solo se muestran las actividades con el estado correspondiente, ordenadas cronológicamente.
Historial de instalación de software	Este widget proporciona información detallada sobre el estado de las instalaciones de software remotas en sus dispositivos gestionados. Al hacer clic en un estado en la columna **Estado de la instalación**, se redirige a la página **Actividades**, donde se muestran las actividades con el estado correspondiente en orden cronológico.
Historial de desinstalación de software	El widget proporciona información detallada del estado de las desinstalaciones de software remotas de sus dispositivos gestionados. Al hacer clic en un estado en la columna **Estado de la desinstalación**, se redirige a la página **Actividades**, donde se muestran las actividades con el estado correspondiente en orden cronológico.

Widgets de Disaster Recovery

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

Widget	Descripción
Estadísticas de Disaster Recovery	El widget muestra los parámetros de rendimiento claves de Disaster Recovery 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 Disaster Recovery probados	El widget muestra información sobre los servidores protegidos por Disaster Recovery y comprobados con la conmutación por error de prueba. El widget muestra los siguientes parámetros: **Servidor protegido**: el número de servidores protegidos por Disaster Recovery (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 Disaster Recovery que se comprobaron con la conmutación por error de prueba durante el intervalo de tiempo seleccionado de entre todos los servidores protegidos por Disaster Recovery. **No probado**: el número de servidores protegidos por Disaster Recovery que no se comprobaron con la conmutación por error de prueba durante el intervalo de tiempo seleccionado de entre todos los servidores protegidos por Disaster Recovery. El widget también muestra el tamaño del almacenamiento de Disaster Recovery (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 Disaster Recovery	El widget muestra información sobre los servidores protegidos por Disaster Recovery y los servidores que no están protegidos. El widget muestra los siguientes parámetros: El número total de servidores registrados en el inquilino de cliente en el momento en que se generó el informe.

Widget	Descripción
	Protegido: el número de servidores protegidos por Disaster Recovery (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

Widget	Descripción
	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 • Más de 1000 archivos
Documentos	El widget muestra el número total de documentos y archivos firmados

Widget	Descripción
firmados electrónicamente por los usuarios finales	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. 102).

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 > Supervisión > 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 > Supervisión > 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
Dispositivos 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 de alertas histórico	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

Este capítulo proporciona la información que necesita para encontrar y activar integraciones.

Las integraciones ofrecen ciberprotección de terceros, gestión de endpoints, gestión de clientes, supervisión, análisis, etc., junto a los productos de consola estándar de Cyber Protect y, de igual forma, ofrecen nuestras soluciones a través de plataformas de software de terceros. Actualmente, más de 200 integraciones automatizan las rutinas diarias y aumentan la eficiencia de nuestros partners y sus clientes.

Las integraciones se enumeran en los catálogos de integración.

Nota
Algunas integraciones requieren un cliente de API para acceder a las interfaces de programación de aplicaciones (API).

Catálogos de integraciones

Los catálogos de integración enumeran las integraciones disponibles:

- Catálogo de aplicaciones.
  Este catálogo está disponible de forma pública. Las integraciones no se pueden activar desde este catálogo.
  Si ve una integración que desea utilizar, póngase en contacto con su partner para que la active.
- Catálogos de centro de datos.
  Estos catálogos son específicos del centro de datos. Las integraciones se pueden activar desde estos catálogos.
  Los administradores del portal de administración a nivel de partner pueden:
  - Vea todas las integraciones desplegadas en el centro de datos.
  - Active todas las integraciones desplegadas en el centro de datos, ya sea para usted o para sus clientes.

  Los administradores del portal de administración a nivel de cliente pueden:
  - Ver solo las integraciones que el desarrollador de la integración establece explícitamente como visibles para los clientes.
  - Activar solo las integraciones que el desarrollador de la integración permita explícitamente que los clientes activen.

    Nota
    El administrador del portal de administración a nivel de partner debe activar la integración a nivel de partner antes de que pueda activarla un administrador del portal de administración a nivel de cliente.

Entradas del catálogo

Las entradas del catálogo constan de dos partes:

- La tarjeta de catálogo proporciona una descripción general de la integración.
- La página de detalles del catálogo proporciona más información, como una descripción funcional completa, capturas de pantalla, vídeos, una lista de funciones, datos de contacto, enlaces a recursos de integración, etc.

Apertura del catálogo de integración de su centro de datos

En los catálogos de integración de centros de datos (DC), pase el ratón por encima de una tarjeta de catálogo para leer una breve descripción del producto, el botón **Configurar** y un enlace a **Más información**:

- El enlace a **Más información**

  Cada entrada del catálogo de integración también tiene una página con detalles de la integración, que incluyen, por ejemplo, una descripción funcional completa, capturas de pantalla, vídeos, una lista de funciones, detalles de contacto, enlaces a recursos de integración, etc.

  Haga clic en este enlace para abrir la página de detalles de la integración.
- El botón **Configurar**

  Haga clic en este botón para activar la integración.

Nota
Las tarjetas de catálogo que representan integraciones inactivas aparecen atenuadas y deshabilitadas.

Pasos para abrir su catálogo de integración de centros de datos

1. Abra el portal de administración.
2. Seleccione **Integraciones** del menú principal.

   La pestaña **Todas las integraciones** se abre de forma predeterminada. Esto muestra las tarjetas de catálogo de las integraciones que los administradores del portal de administración a nivel de cliente pueden habilitar.
3. [Opcional] Elija una categoría e introduzca texto en el campo de búsqueda para filtrar las tarjetas de catálogo.

Cómo abrir una página de detalles de integración

Pasos para abrir una página de detalles de integración

1. Abra el catálogo de integración en su centro de datos.
2. Busque la tarjeta del catálogo para la integración.
3. Pase el ratón por encima de la tarjeta del catálogo.
4. Haga clic en **Más información**.

Se abre la página de detalles de la integración.

Visualización de sus integraciones activadas

La pestaña **Integraciones en uso** del catálogo de integraciones muestra una tarjeta para cada integración que haya activado.

Pasos para ver sus integraciones activadas

1. Abra el catálogo de integración en su centro de datos.
2. Seleccione la pestaña **Integraciones en uso**.

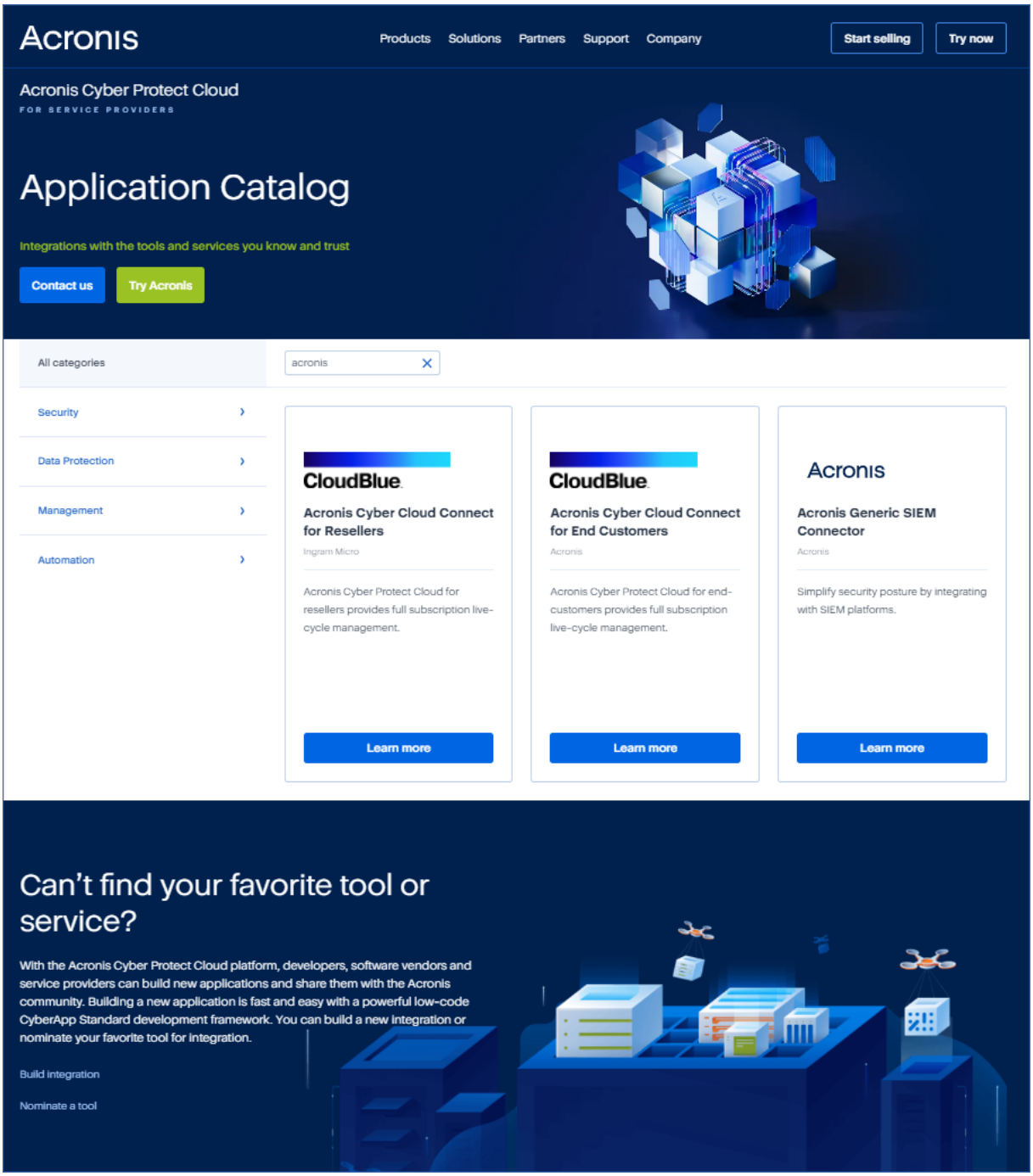
Cómo abrir el catálogo de aplicaciones

El catálogo de aplicaciones enumera todas las integraciones de Cyber Protect Cloud.

Nota
Si identifica una integración que desea utilizar, debe ponerse en contacto con su partner para que la active.

Pasos para abrir el catálogo de aplicaciones

1. Visite solutions.acronis.com.
   La vista inicial es una cuadrícula de todas las tarjetas de catálogo.
2. [Opcional] Elija una categoría e introduzca texto en el campo de búsqueda para filtrar las tarjetas de catálogo.



Cómo abrir una página de detalles de integración

Cada entrada del catálogo también tiene una página con detalles de la integración, como una descripción funcional completa, capturas de pantalla, vídeos, una lista de funciones, detalles de contacto, enlaces a recursos de integración, etc.

Pasos para abrir una página de detalles de integración

1. Visite solutions.acronis.com.
2. Busque la tarjeta de catálogo de la integración que le interese.

3. Haga clic en **Más información** en la tarjeta del catálogo.

Some features might not be available in your data center yet.

Acronis

Products Solutions Partners Support Company

Start selling Try now

Acronis Cyber Protect Cloud

FOR SERVICE PROVIDERS

Application Catalog

Integrations with the tools and services you know and trust

Contact us Try Acronis

← Back to integrations

Have a question or need help?

Acronis

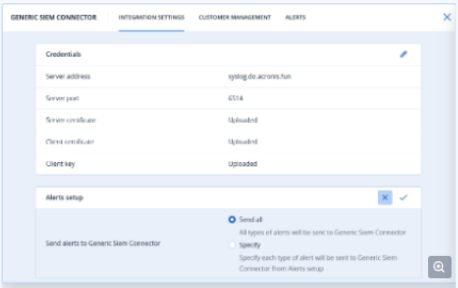
Integration: Acronis Generic SIEM Connector
Category: SIEM
Company: Acronis

Website

Acronis Generic SIEM Connector

SIEM (Security Information and Event Management) platforms are used by many MSPs for security incident investigation and remediation, threat hunting, and compliance. Acronis Generic SIEM Connector allows MSPs to forward Acronis Cyber Protect Cloud alerts to any SIEM system that supports the CEF event format over SYSLOG for further correlation and analysis to reveal patterns of activity that may indicate an attempt of intrusion.

Integration Overview



Simplify security posture by integrating with SIEM platforms.

SIEMs empower MSPs security specialists to identify attack rout across the network and get visibility into compromised files. Now with Acronis Generic SIEM connector, MSPs will gain extra visibility into customers networks, will be able to search for threats across all managed workloads, and correlate events from both security and data protection applications, and run response actions.

Features

Support of core event format
Acronis supports core event format - CEF (Common Event Format), enabling MSPs to work with any SIEM that supports CEF format out of the box. Alerts are transferred to SIEM via syslog server.

Threat hunting across all managed companies
Integration allows MSPs to select which customer tenants in Acronis should send alerts to SIEM. Since alerts are sent to the same SIEM instance, it's possible to run correlation, threat hunting and perform investigation for all customers in the same console. It also empowers MSPs to search for threats, that were discovered on one workload in one customer tenant, in other customers environments.

Simple integration enablement
It's very easy to enable the integration by obtaining server and client certificates, establishing connection to the server and specifying the server port.

Select data you want to see
It is possible to select which alerts should be sent to SIEM. With this functionality, MSPs benefit from reducing the amount of sent to SIEM data and, therefore, lower SIEM invoice. MSPs can select and work only with the data that is necessary.

Acronis

Acronis Generic SIEM Connector

Need help or support with an integration?

Contact Support

Can't find your favorite tool or service?

With the Acronis Cyber Protect Cloud platform, developers, software vendors and service providers can build new applications and share them with the Acronis community. Building a new application is fast and easy with a powerful low-code CyberApp Standard development framework. You can build a new integration or nominate your favorite tool for integration.

Build integration

Nominate a tool

Engage with Acronis

Acronis © 2003–2024 Acronis International GmbH. Legal information | Privacy policy

Activación de una integración

Nota
El administrador del portal de administración a nivel de partner debe activar la integración a nivel de partner antes de que pueda activarla un administrador del portal de administración a nivel de cliente.

Pasos para activar una integración

1. Abra el catálogo de integración en su centro de datos.
2. Busque la tarjeta de catálogo de la integración que desee activar.
   Pasos para filtrar las integraciones:
   - [Opcional] Seleccione una categoría.
   - [Opcional] Escriba una cadena en el campo de búsqueda.
3. Pase el ratón por encima de la tarjeta del catálogo.
4. Haga clic en **Configurar**.
5. Siga las instrucciones que aparecen en pantalla.

Configuración de una integración activa

Pasos para configurar una integración activa

1. Abra el catálogo de integración en su centro de datos.
2. Seleccione la pestaña **Integraciones en uso**.
3. Busque la tarjeta de catálogo de la integración que desea configurar.
4. Haga clic en **Gestionar**.
   Se abrirá la pantalla de configuración de la integración.
5. Siga las instrucciones en pantalla o consulte la documentación de integración.

   Nota
   La documentación suele estar disponible en la página de detalles del catálogo. Para obtener más información, consulte Abrir una página de detalles de integración.

Desactivación de una integración activa

Pasos para desactivar una integración

1. Abra el catálogo de integración en su centro de datos.
2. Seleccione la pestaña **Integraciones en uso**.
3. Busque la tarjeta de catálogo de la integración que desea deshabilitar.

4. Haga clic en **Desactivar**.
5. Haga clic en **Eliminar**.

Clientes API

Las integraciones de sistemas de terceros pueden utilizar las interfaces de programación de aplicaciones (API). El acceso a las API se habilita mediante clientes de API, que son una parte integral del marco de autorización OAuth 2.0 de la plataforma.

Un cliente de API es una cuenta especial de la plataforma que representa al sistema de terceros que debe autenticarse y autorizarse para acceder a los datos de la plataforma y de los servicios. El acceso del cliente de API está limitado al inquilino cuyo administrador del portal de administración crea el cliente y a cualquier subinquilino.

Nota
El cliente de API 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.

Credenciales de cliente de API

Las credenciales del cliente de API consisten en el identificador (ID) y un valor secreto. Estas credenciales no caducan y no se pueden utilizar para iniciar sesión en el portal de administración o en cualquier otra consola de servicios.

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

Flujo del cliente de API

1. Un administrador del portal de administración crea un cliente de API.
2. El administrador habilita el flujo de credenciales del cliente OAuth 2.0 en el sistema de terceros.
3. Según este flujo, antes de acceder al inquilino y sus servicios a través de la API, el sistema debe enviar primero las credenciales del cliente de API a la plataforma, utilizando la API de autorización.
4. La plataforma genera y devuelve un token de seguridad, la única cadena críptica asignada a este cliente concreto.
5. El sistema de terceros debe añadir este token a todas las solicitudes a la API.

Nota
El token de seguridad acaba con la necesidad de mandar las credenciales del cliente con las solicitudes a la API.
Para mayor seguridad, el token de seguridad caduca en dos horas.
Pasado este tiempo, todas las solicitudes de API con el token expirado fallarán y el sistema deberá solicitar un nuevo token de la plataforma.

Creación de un cliente API

Pasos para crear un cliente de API

1. Inicie sesión en el portal de administración.
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 de API se crea con estado **Habilitado**.
5. Copie y guarde el ID, el valor secreto del cliente de API 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. Se puede restablecer.

6. Haga clic en **Listo**.

Restablecimiento de un valor secreto de cliente de API

Si pierde su valor secreto del cliente de API, puede generar uno nuevo. El ID de cliente y la URL del centro de datos no cambian.

Importante
Si restablece el valor secreto, todos los tokens de seguridad asignados al cliente caducarán inmediatamente y las solicitudes de API con estos tokens fallarán.

Pasos para restablecer el valor secreto de un cliente de API

1. Inicie sesión en el portal de administración.
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. Haga clic en **Siguiente** para confirmar su decisión.
6. Copie y guarde el nuevo valor secreto del cliente de API.

Nota
Por motivos de seguridad, la clave solo se muestra una vez. No hay ninguna forma de recuperar este valor si lo pierde. Se puede restablecer mediante la repetición de estos pasos.

7. Haga clic en **Listo**.

Deshabilitación de un cliente API

Puede deshabilitar los clientes de API. Si lo hace, las solicitudes de API con tokens de seguridad que se asignan al cliente fallarán, pero los tokens no expirarán inmediatamente.

Nota
El hecho de deshabilitar el cliente no afecta a la fecha de caducidad de los tokens.

Puede volver a habilitar el cliente de API en cualquier momento.

Pasos para deshabilitar un cliente de API

1. Inicie sesión en el portal de administración.
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.

Habilitación de un cliente API deshabilitado

Si habilita un cliente de API previamente deshabilitado, las solicitudes de API con tokens de seguridad que se asignan al cliente se ejecutarán correctamente **si estos tokens aún no han expirado**.

Pasos para habilitar un cliente de API deshabilitado

1. Inicie sesión en el portal de administración.
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 de API cambiará a **Activo**.

Eliminación de un cliente API

Si elimina un cliente de API, todos los tokens de seguridad asignados a este cliente caducarán inmediatamente y las solicitudes de API con estos tokens fallarán.

Importante
No hay manera de recuperar un cliente eliminado.

Pasos para eliminar un cliente de API

1. Inicie sesión en el portal de administración.
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.

Creación de una integración

Si tiene datos o servicios que desea integrar con Cyber Protect Cloud, puede crear un CyberApp nativo mediante el portal de proveedores o utilizar llamadas a la API.

CyberApp

El portal de proveedores es una plataforma en línea que permite a los proveedores de software de terceros integrar productos y servicios de forma nativa en Cyber Protect Cloud, de acuerdo con nuestras mejores prácticas CyberApp Standard. Las integraciones del portal de proveedores se denominan CyberApps.

Nota
Para obtener más información sobre CyberApps y el portal de proveedores, consulte la Guía de integración.

Integraciónes API

Existe un conjunto completo de API para integraciones.

Nota
Para obtener más información sobre las API, consulte el capítulo de las API de la plataforma de la Guía de integración.

Índice