
Aranda Data Safe

Bienvenido al tutorial de introducción a Aranda Datasafe. Si es nuevo en Aranda Datasafe, este es el lugar perfecto para aprender a:

- Descubrir sus dispositivos y sus datos.
- Configurar sus equipos, repositorios y conector de Active Directory.
- Crear políticas para configurar las opciones de Respaldo y Prevención de pérdida de datos.
- Ejecutar copias de seguridad y restauraciones.
- Aprender a utilizar las funciones de Prevención de pérdida de datos, como Cifrado local, Borrado remoto y Geolocalización.
- Aprender a utilizar la función de migración remota completa.

El tutorial se divide en una serie de pasos. Debe completarlos en secuencia, comenzando con el Paso 1 Activación Cuenta de Administrador

Iniciando Data Safe

Requerimientos del Sistema

Requermimientos de Hardware

Requerimientos de hardware para Bóveda de Almacenamiento

Los requisitos de hardware para la Bóveda de almacenamiento pueden variar según la cantidad de dispositivos que se requiera proteger. Las siguientes tablas muestran nuestras recomendaciones.

Especificación	1-250 Usuarios	251-500 Usuarios	500-800 Usuarios
Sistema Operativo	- Windows Server 2016 - 2019 - CentOS 6.x – 9.x - Debian 6.x – 11.x - Ubuntu 22.04 o posterior	- Windows Server 2016 - 2019 - CentOS 6.x – 9.x - Debian 6.x – 11.x - Ubuntu 22.04 o posterior	- Windows Server 2016 - 2019 - CentOS 6.x – 9.x - Debian 6.x – 11.x - Ubuntu 22.04 o posterior
CPU	CPU 4 Cores	6 Cores / vCPUs	8 Cores / vCPUs
Memoria	6 GB	8 GB	16 GB
Almacenamiento - Bóveda(~20 GB por usuario)	5 TB	10 TB	16 TB +
Almacenamiento – Índice de Bóveda	N/A	50GB SSD	50GB SSD

Requerimientos del Agente

Estos son los requisitos del sistema recomendados para que los dispositivos ejecuten correctamente el Agente de Aranda:

Especificación	Descripción
Sistema Operativo	Windows 10/11 Pro o Enterprise
CPU	Intel i3, i5, i7 o AMD equivalente
RAM	384 MB disponibles para el agente
Almacenamiento	500MB libres *Unidad de estado sólido para un mejor rendimiento.

Requermimientos de Red

Requerimiento	Descripción
Resolver el nombre DNS del tenant de EPC	nslookup endpointcloud.com
Permitir acceso por Internet hacia el tenant	El firewall y el proxy deben permitir la comunicación con: .endpointcloud.com Permitir comunicación saliente en el puerto 443.
El Firewall debe permitir la comunicación desde los dispositivos cliente al servidor de la bóveda de almacenamiento.	Entrante y saliente por el puerto 9000 en el servidor de la bóveda de almacenamiento.

Requermimientos para Conector de Active Directory

El Conector de AD se podrá instalará en el mismo hardware que la Bóveda de almacenamiento. Si no tienes una Bóveda On Premises / local, entonces necesitarás las siguientes especificaciones mínimas de hardware para la instalación del Conector de AD:

Requerimiento	Descripción
Sistema Operativo	Windows Server 2016 - 2019
CPU	4 Cores / vCPUs
RAM	4 GB (incluye requerimiento de SO)
Storage	500MB free.

Requermimientos de Active Directory y Acceso

Se deben cumplir los siguientes requisitos para proporcionar acceso:

Requisitos	Descripción
Dominio de AD para autenticación de usuarios	Dominio de AD para autenticación de usuarios Para la integración de AD, se requiere un dominio de AD. No se requiere Dominio para la implementación de grupo de trabajo.
El Conector de AD debe estar instalado en un servidor unido al dominio de directorio activo.	Debe ser el mismo dominio de AD que se utiliza para autenticar al usuario.
La cuenta de administrador de Windows Server debe tener permisos suficientes.	Debe tener permisos para: Instalar software y servicios. Registrar un registro SPN en el dominio. Acceder a https://endpointcloud.com
Los Firewalls deben permitir que los dispositivos del cliente se comuniquen con la Bóveda de almacenamiento.	Puerto 9000 de entrada y salida.

Active su Cuenta de Administrador

Para comenzar, active su cuenta de administrador para que pueda iniciar sesión y configurar Aranda Datasafe.

> ⚐ **Nota:** Cuando su organización se registre en Aranda Datasafe, un administrador de cuenta le enviará una invitación por correo electrónico. Si no recibe el correo electrónico, revise sus carpetas de correo no deseado. Si aún no puede encontrar el correo electrónico, comuníquese con el servicio de atención al cliente de Aranda reportedecasos@arandasoft.com. Cuando tenga el correo electrónico, haga clic en **Activar cuenta**. Su navegador abre la página web de activación. La primera vez que acceda a Aranda Datasafe, debe ingresar una contraseña y luego volver a ingresarla para confirmar. Haga clic en **Activar** para iniciar sesión. Si es el primer administrador en iniciar sesión, se le asignará automáticamente el rol de **Oficial de seguridad**. Si no es el primero, se le asigna un rol de **administrador**. (Esto se puede cambiar más adelante si es necesario). El rol de Oficial de seguridad es el rol de mayor rango y le permite descargar y registrar el conector AD que se usa para la autenticación de usuarios.

Instalar Agente de Descubrimiento

Puede utilizar la aplicación gratuita Discovery Agent para que Aranda Datasafe detecte los dispositivos de sus usuarios automáticamente.

Para configurar Discovery Agent, descárguelo y luego instálelo en cada dispositivo de usuario final. No lo instale en su servidor.

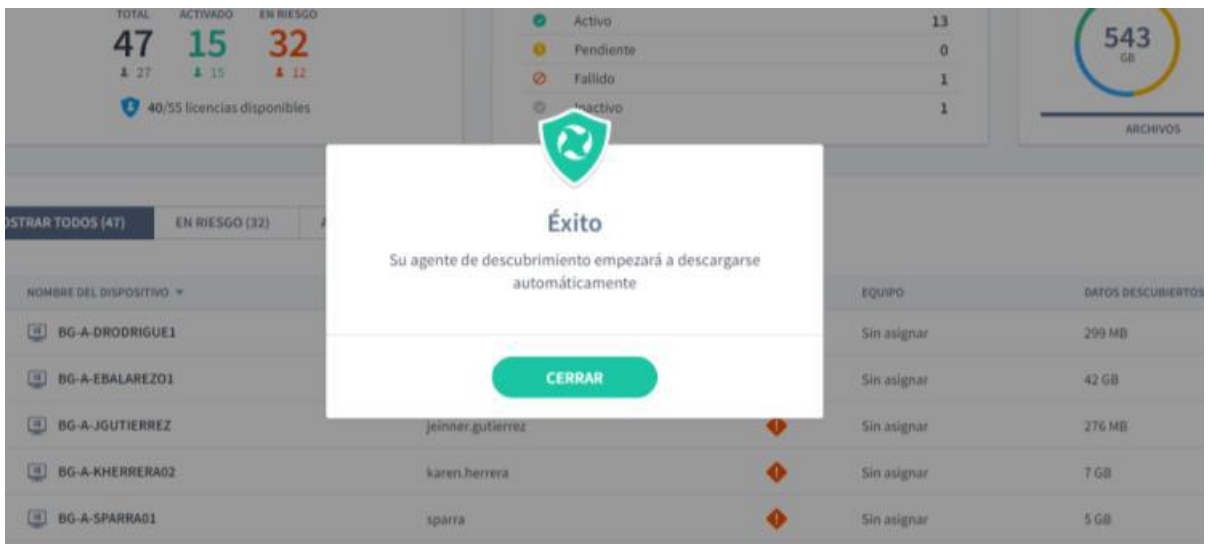
Descargue Discovery Agent

Puede descargar Discovery Agent desde su Consola Aranda Datasafe:

1. Inicie sesión como administrador. Cuando inicia sesión como administrador por primera vez, el Inventario se selecciona de forma predeterminada. En esta etapa, Aranda Datasafe no ha descubierto ningún dispositivo.

2. Haga clic en Descargar Discovery Agent. El paquete Discovery Agent MSI se descarga en su navegador. Discovery Agent es específico para su instancia de Aranda

Datasafe.



Instale Discovery Agent en sus dispositivos de usuario

Instale el paquete Discovery Agent MSI en cada dispositivo de usuario (computadora de escritorio, computadora portátil, etc.). El agente de descubrimiento realizará un inventario de dispositivos y datos, y luego cargará de forma segura la información en Aranda Datasafe.

Prerrequisitos

- Los dispositivos del usuario deben tener acceso a Internet ya que Discovery Agent necesita conectarse a Aranda Datasafe.
- Los dispositivos del usuario deben utilizar un sistema operativo Windows, Windows 7 o posterior. Pronto habrá una versión para Mac.
- Los firewalls y los servidores proxy deben permitir las conexiones. Es posible que deba incluir en la lista blanca endpointcloud.com y la ruta completa a la URL de tenant de Aranda Datasafe. Ejemplo: https://arandasoftware.endpointcloud.com donde “arandasoftware” se reemplaza por el nombre de su organización.

Puede instalar Discovery Agent de forma manual o remota en cada dispositivo.

Instalación manual del agente

Discovery Agent se puede instalar ejecutando el paquete MSI en cada dispositivo de usuario.

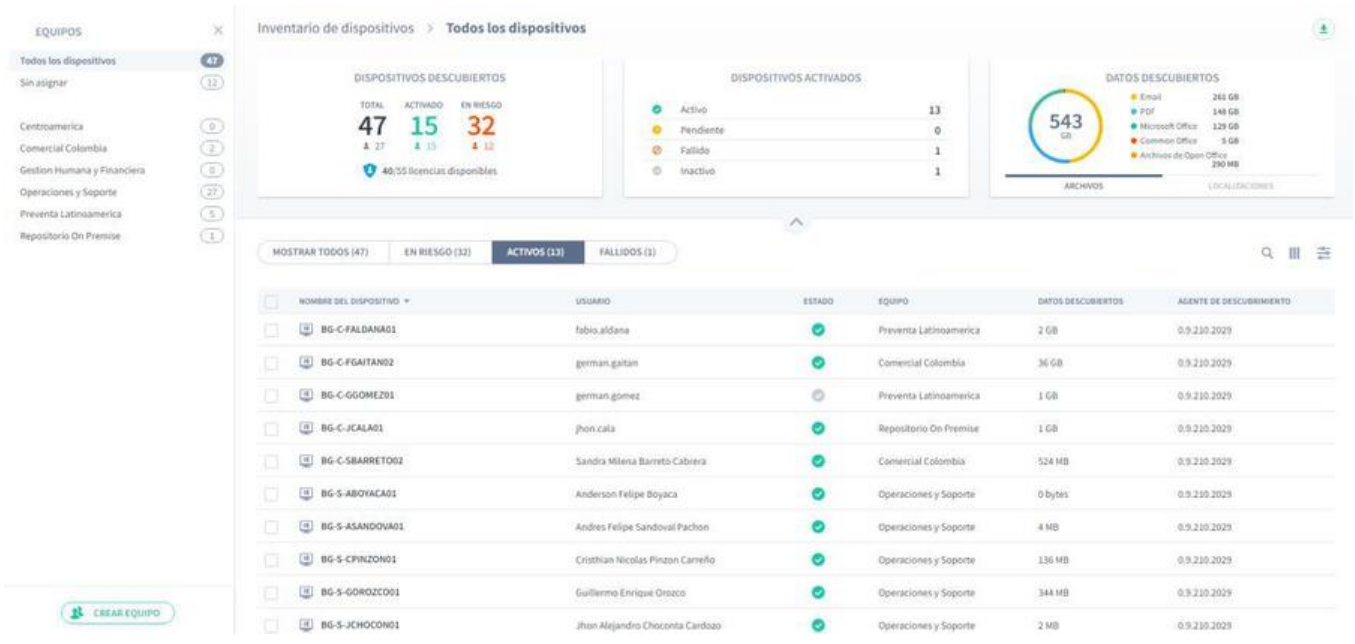
Es posible que desee mover el paquete MSI a una carpeta compartida a la que puedan acceder todos los dispositivos. Alternativamente, puede colocar el paquete MSI en una tarjeta de memoria y transferirlo entre dispositivos de esa manera.

Instalación remota del agente

Puede instalar el paquete MSI en los dispositivos de forma remota, utilizando la función de directiva de grupo de Active Directory o una aplicación de terceros. Para obtener más detalles, comuníquese con el soporte de Aranda (reportedecasos@arandasoft.com).

Inventario

Cuando sus dispositivos tengan instalado Discovery Agent, reportarán a su tenant de Aranda Datasafe. Verá que los dispositivos aparecen en la lista de Inventario y que el tablero se completa con datos.



Visualice la información de cada una de las secciones.

1. **Dispositivos descubiertos**: cuántos dispositivos se han descubierto, cuántos se han activado para protección y cuántos todavía están en riesgo.

2. **Dispositivos activados**: Útil una vez que comenzamos a activar dispositivos. Nos muestra cuántos dispositivos quedan pendientes de activación y cuántos han fallado.

3. **Datos descubiertos**: la cantidad de datos descubiertos. Puede ver la cantidad según los tipos de archivos o según las ubicaciones de los archivos.

También hay una lista de dispositivos que muestra todos los dispositivos que Discovery Agent ha descubierto. Hay un breve resumen del dispositivo, incluida la cuenta de usuario del dispositivo y la cantidad de datos descubiertos.

Puede acceder a información más detallada para cada dispositivo.

1. Haga clic en un dispositivo de la lista de dispositivos. Aparece un panel deslizante que contiene un resumen más detallado del dispositivo y la cuenta de usuario asociada a él.

2. Haga clic en el ícono de perfil para mostrar los detalles completos del dispositivo.

3. Haga clic en la flecha hacia atrás junto al nombre de usuario en la parte superior de la pantalla para regresar al **Inventario**.

Es posible que haya notado que en el lado izquierdo del Inventario hay una lista de **Equipos**. Lo usará para crear nuevos equipos y organizar sus dispositivos en el siguiente paso.

Organización de Dispositivos en Equipos

Cuando sus dispositivos se conectan a Aranda Datasafe por primera vez, están "sin asignar". Esto significa que no están en un equipo. Puede crear equipos y usarlos para organizar sus dispositivos en grupos significativos.

Con Equipos, puede:

- Asignar una política para controlar la configuración de respaldo y protección para un grupo de dispositivos.
- Asignar un repositorio donde el equipo hará copias de seguridad.
- Filtre la información por un equipo para que pueda ver información sobre los dispositivos que se utilizan en la misma área de su negocio, por ejemplo, podría tener un Equipo que muestre todos los dispositivos utilizados por marketing.

Te mostraremos cómo funciona. Creará su propio equipo, le asignará dispositivos y luego podrá visualizar la información sobre los dispositivos de ese equipo.

Crear un Equipo

Para crear un equipo:

1. Haga clic en **Inventario**.

2. Haga clic en **Crear equipo** (esquina inferior izquierda de la pantalla Inventario).

3. Ingrese un nombre para el nuevo equipo.

4. Ignore la configuración de Asignar una política y Asignar un repositorio por ahora. Volverá a ellos después de haber creado una Política y un repositorio.

5. Haga clic en Guardar equipo.

Asignar un dispositivo a un equipo

Cuando haya configurado sus equipos, puede usarlos para organizar sus dispositivos descubiertos:

1. Pase el cursor sobre un dispositivo en la lista de dispositivos.

2. Haga clic en el botón de opción del dispositivo (...).

3. Haga clic en Asignar equipo.

4. Asigne el dispositivo a un equipo de la lista.

5. Haga clic en Asignar.

La página se actualizará automáticamente y el dispositivo se asignará a su equipo seleccionado. Ahora puede usar el Inventario para ver información sobre todos los dispositivos, dispositivos no asignados o dispositivos en cada uno de sus equipos.

Ver los dispositivos de un Equipo

Cuando tenga sus dispositivos organizados en equipos, puede filtrar el inventario para que solo muestre información sobre los dispositivos en un equipo en particular.

1. Haga clic en Inventario.

2. En la sección Equipos, haga clic en:

- **Todos los dispositivos** para mostrar información sobre todos los dispositivos en todos los equipos

- **Sin asignar** para mostrar información solo para aquellos dispositivos que aún no están asignados a un equipo
- **** para mostrar información sobre los dispositivos de un equipo específico. Seleccione varios dispositivos manteniendo presionada la tecla CTRL y haciendo clic en los equipos.

Instalar Repositorio

Debe configurar un repositorio en la que se realizarán copias de seguridad de sus dispositivos.

Un repositorio es un área de almacenamiento que se puede instalar en un servidor en sus instalaciones o en un servidor remoto en un centro de datos. Almacena de forma segura los datos de respaldo de sus dispositivos activados.

Nota: El software Private Cloud Vault está disponible para Windows Server 2019 de 64 bits.

Descargue e instale el paquete Private Cloud Vault - Windows

Para registrar un repositorio, deberá tener la dirección de correo electrónico y la contraseña de una cuenta de usuario de Aranda Datasafe con el rol de administrador o oficial de seguridad.

Para descargar e instalar el paquete Private Cloud Vault:

1. Haga clic en repositorio.

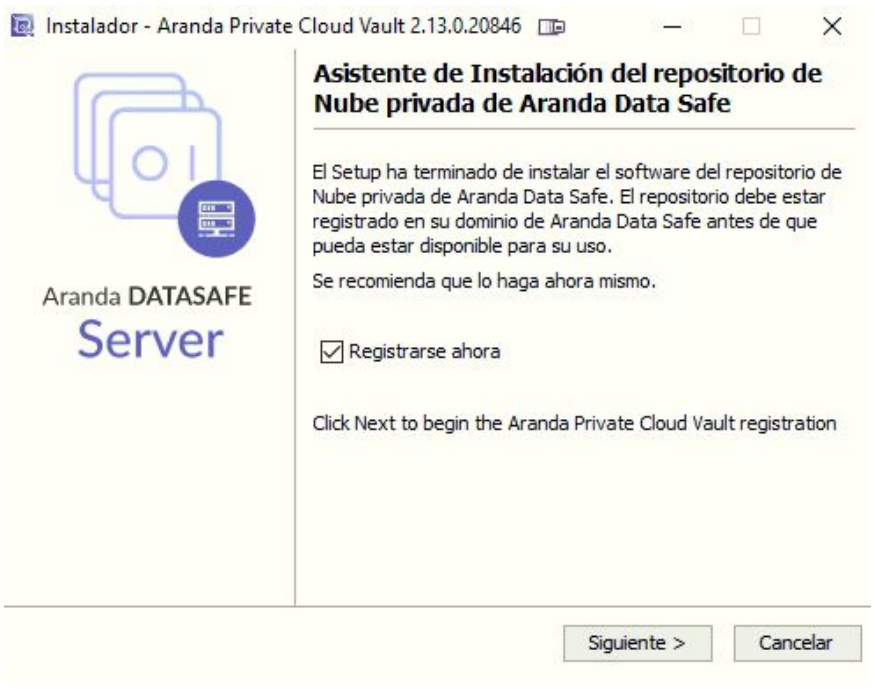
2. Haga clic en Descargar Private Cloud Vault.

3. Cuando se descargue el paquete Private Cloud Vault, búsquelo en su computadora y cópielo en su servidor.

4. En el servidor, instale el software Private Cloud Vault. Puede instalarlo en la ubicación predeterminada o elegir otra ubicación si lo prefiere.

Siga los pasos del asistente de instalación.

Cuando haya instalado el software, asegúrese de que**Registrarse ahora** esté marcado y luego haga clic en**Siguiente**.



5. Ingrese los detalles de registro:

-

Campo	Descripción
Dominio	El nombre de su tenant de Aranda Datasafe. Este suele ser el nombre de su organización y es la primera parte de la dirección de su Aranda Datasafe.
Nombre de usuario	Ingrese la dirección de correo electrónico de una cuenta de Aranda Datasafe que tenga el rol de Administrador u Oficial de seguridad. Solo estas cuentas de usuario tienen permiso para registrar un repositorio.
Contraseña	Ingrese la contraseña para la cuenta de Aranda Datasafe.
Nombre de host / IP	Ingrese el nombre o la dirección IP del servidor que tiene instalado el software de repositorio. Si el servidor está en una dirección de Internet, ingrese la URL en su lugar.
Puerto	9000. (Puede seleccionar el puerto de su elección, pero recomendamos usar 9000).
Alias	Ingrese el nombre del repositorio como aparecerá en Aranda Datasafe.

⚠ **Importante:** Los agentes de descubrimiento y los agentes de protección deben poder comunicarse en el puerto 9000.

6. Haga clic en Registrarse y finalizar.

Instalar Conector de Active Directory

Active Directory Connector (AD Connector) es una aplicación que Aranda Datasafe usa para autenticar sus cuentas de usuario, de modo que sus datos cifrados solo estén disponibles para usuarios autorizados.

Debe instalar AD Connector en un servidor de Windows unido a un dominio que se encuentre en las instalaciones de su empresa.

Para descargar, instalar y registrar el software AD Connector:

1. Haga clic en **Configuración**.

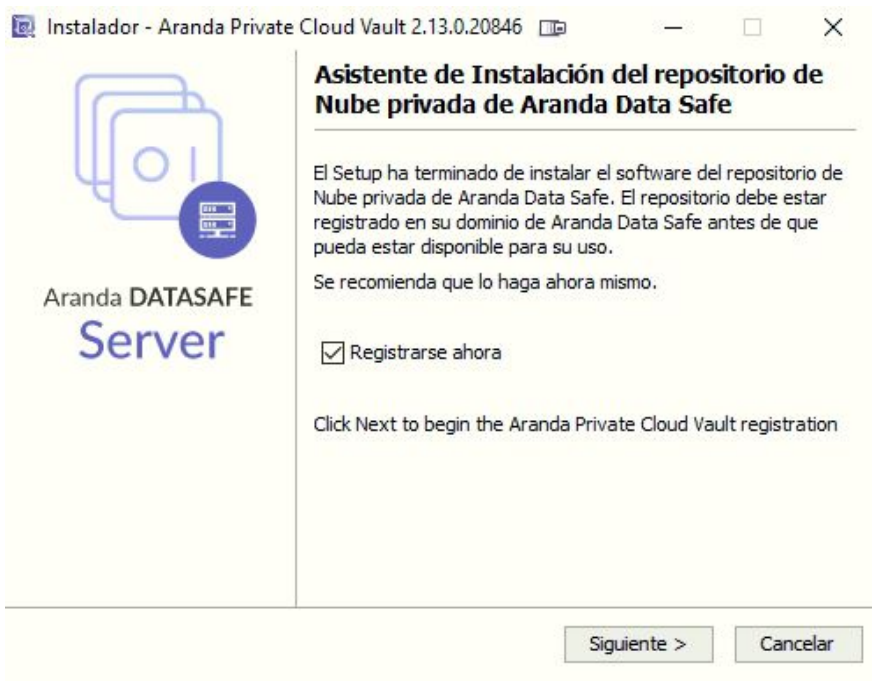
2. Haga clic en **Active Directory**.

3. Haga clic en Conectar **Ad** para descargar el archivo ejecutable adconnector. Deberá copiar este archivo a su servidor local.

4. Inicie sesión en el servidor en el que se ejecutará AD Connector. Debe iniciar sesión a través de una cuenta de usuario de administrador de dominio que tenga permiso para registrar un nombre principal de servicio (SPN) para la autenticación Kerberos.

5. Copie el archivo ejecutable de adconnector en el servidor y luego ejecútelo.

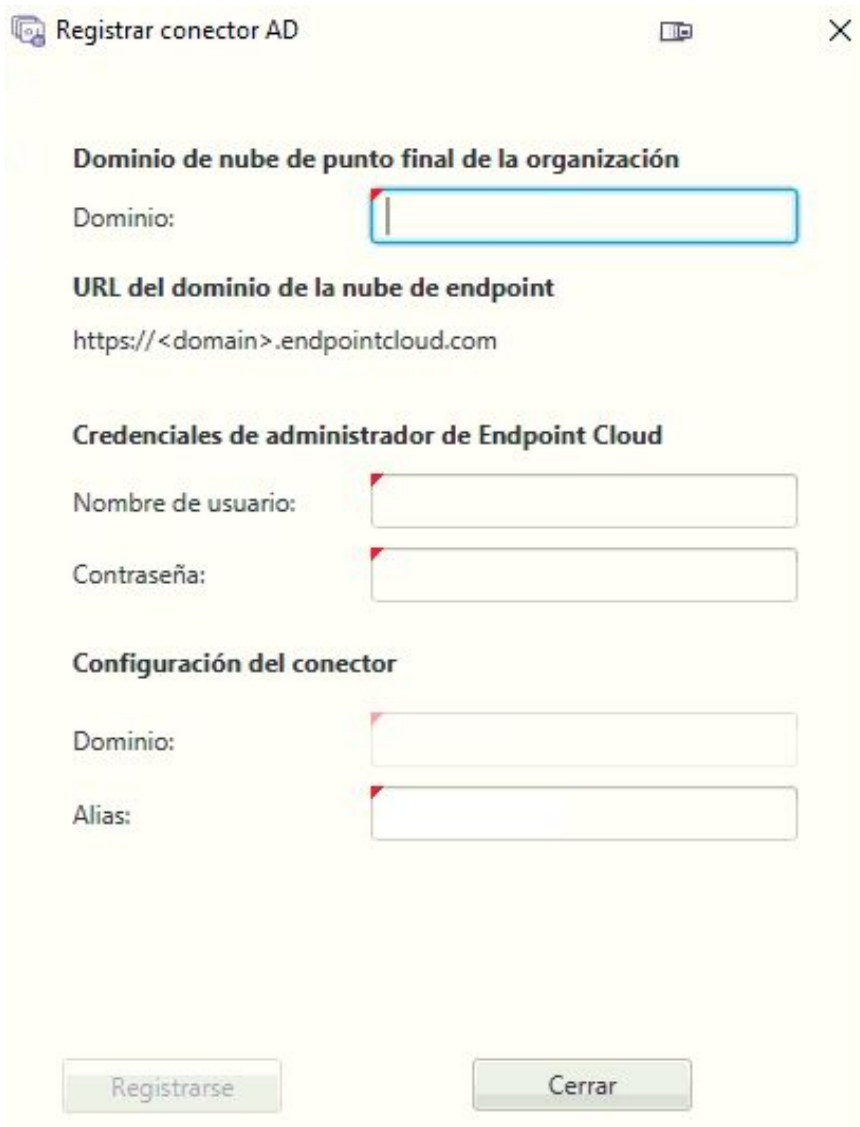
6. Siga las instrucciones en pantalla para instalarlo.



Puede instalarlo en cualquier directorio (la ubicación predeterminada es la unidad C).

Cuando complete los pasos de instalación, los archivos comienzan a extraerse e instalarse. Cuando se instalan los archivos, el asistente de instalación le pregunta si desea registrarse.

7. Asegúrese de que Registrarse ahora esté marcado y luego haga clic en Siguiente.



8. Ingrese los detalles de registro:

Campo	Descripción
Dominio	El nombre de su tenant de Aranda Datasafe. Este suele ser el nombre de su organización y es la primera parte de la dirección de su Aranda Datasafe.
Nombre de usuario	Ingrese la dirección de correo electrónico de una cuenta de Aranda Datasafe que tenga el rol de Oficial de seguridad. Solo las cuentas de usuario de Security Officer tienen permiso para registrar un AD Connector.
Dominio	Ingrese el nombre de dominio de la organización
Contraseña	Ingrese la contraseña para la cuenta de Aranda Datasafe.
Alias	Ingrese el nombre del conector AD como aparecerá en Aranda Datasafe.

9. . Haga clic en **Registrarse** y **finalizar**.

Crear una Política

Una política es un conjunto de reglas que definen:

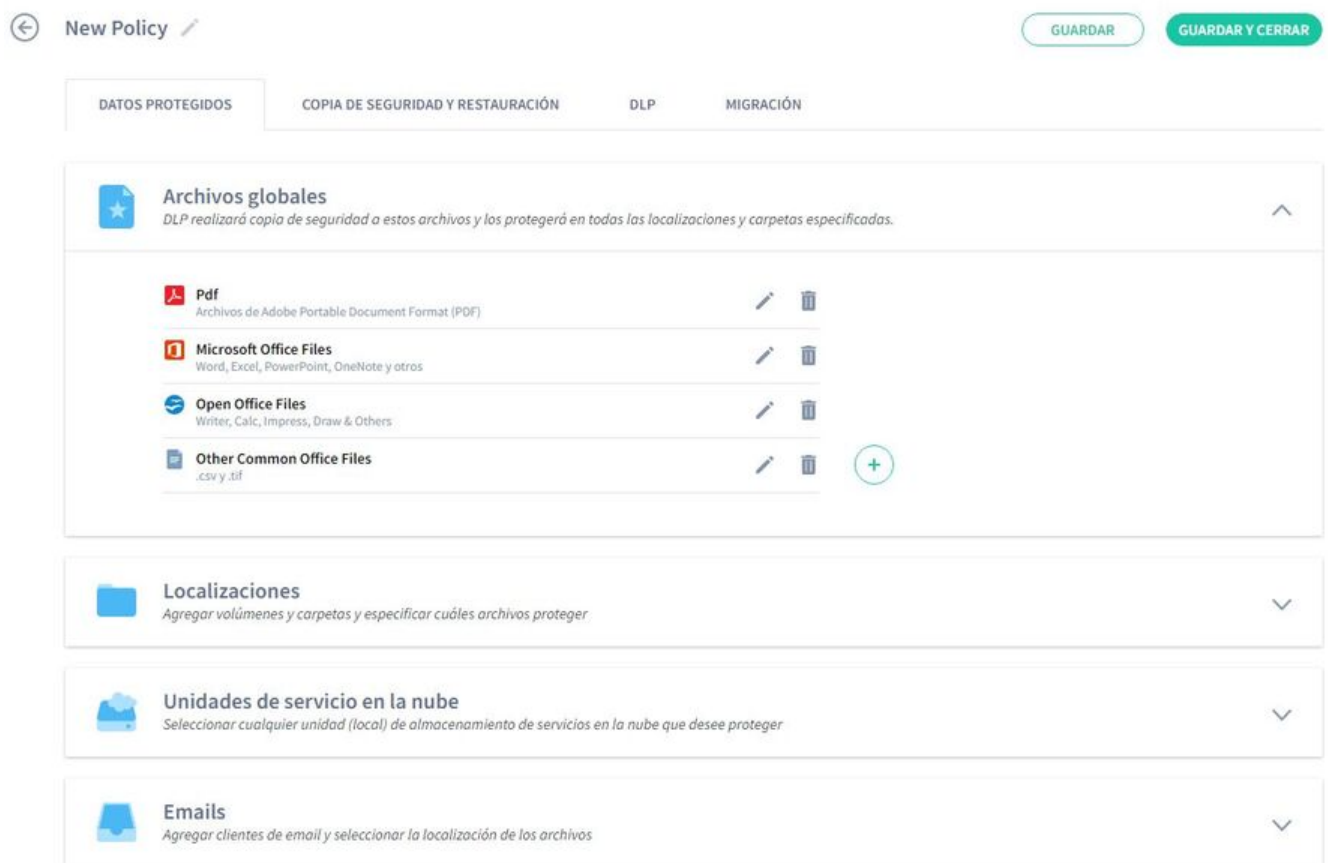
- Qué datos están protegidos y respaldados
- Con qué frecuencia ocurren las copias de seguridad
- Si se utiliza alguna función de prevención de pérdida de datos para proteger sus datos en caso de pérdida o robo de un dispositivo
- Si se realiza una copia de seguridad de la configuración del perfil de usuario de Windows.

Puede crear tantas políticas como necesite. Puede tener una Política para todos o puede tener diferentes Políticas para cada equipo.

Crear una nueva política

1. Haga clic en Políticas.

Si no tiene ninguna política en Aranda Datasafe, haga clic en Agregar una política. Aranda Datasafe crea una nueva Política y la abre, lista para que usted defina su configuración.



2. Ingrese un nombre a la Política. Haga clic en el ícono de edición junto al nombre predeterminado y luego ingrese el nuevo nombre.

Su nueva Política tiene configuraciones predeterminadas, y muchos administradores de Aranda Datasafe encuentran que estas configuraciones son adecuadas para sus necesidades. Si tiene diferentes requisitos, puede cambiar la configuración en las siguientes secciones:

Campo	Descripción
Datos protegidos	Se utiliza para definir qué datos se seleccionan para su protección.
Copia de seguridad y restauración	Se utiliza para elegir la frecuencia con la que se realizan las copias de seguridad.
DLP	Se utiliza para elegir las medidas de prevención de pérdida de datos para la política.
Migración	Se utiliza para elegir si se realiza una copia de seguridad de la configuración relacionada con los perfiles de usuario de Windows.

Visualice las opciones que puede tomar en las seccionesDatos protegidos, Copia de seguridad y restauración , DLP y Migración.

Datos Protegidos

Utilice la configuración de Datos protegidos para elegir qué archivos serán protegidos y respaldados (de acuerdo con las reglas definidas en la política). La configuración de la política define:

- Qué datos se respaldan y protegen
- Si el cifrado se aplica a los archivos del dispositivo local.
- Si el acceso a los datos se puede revocar automáticamente.
- Si se pueden borrar los datos protegidos de un dispositivo de forma remota

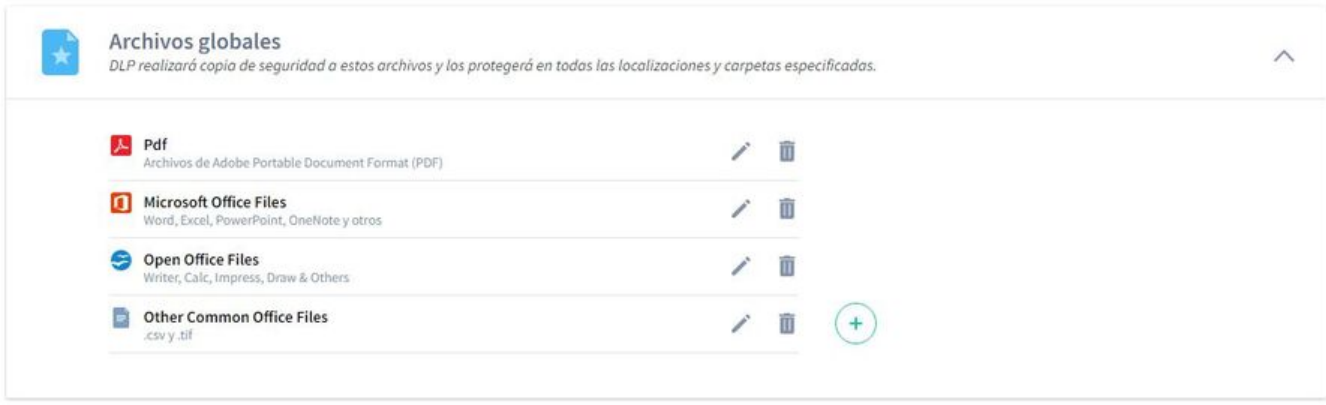
Visualice las diferentes secciones.

Archivos globales

Los archivos globales son colecciones de tipos de archivos. Por ejemplo, hay una colección de archivos de Microsoft Office, para archivos guardados en Word, Excel, PowerPoint, etc. De forma predeterminada, Aranda Datasafe realizará una copia de seguridad de estos archivos 'globales', independientemente de dónde estén almacenados en los dispositivos que usan la política..

Puede utilizar la configuración de Archivos globales para:

- Agregar o eliminar tipos de archivos de las diferentes colecciones
- Cree una nueva colección para diferentes tipos de archivos. Por ejemplo, es posible que desee crear una nueva colección que contenga los tipos de archivo para su software propietario.



Ubicaciones

Puede configurar Aranda Datasafe para realizar copias de seguridad y proteger archivos en ubicaciones específicas en una computadora (solo unidades locales, de forma predeterminada). Algunas ubicaciones comunes se incluyen de forma predeterminada, incluidos Todos los volúmenes, Escritorio y Documentos, y puede agregar otras ubicaciones si es necesario.

Para cada ubicación, puede elegir qué archivos se respaldarán y protegerán: todos los archivos, solo archivos globales o un conjunto de archivos que elija manualmente.

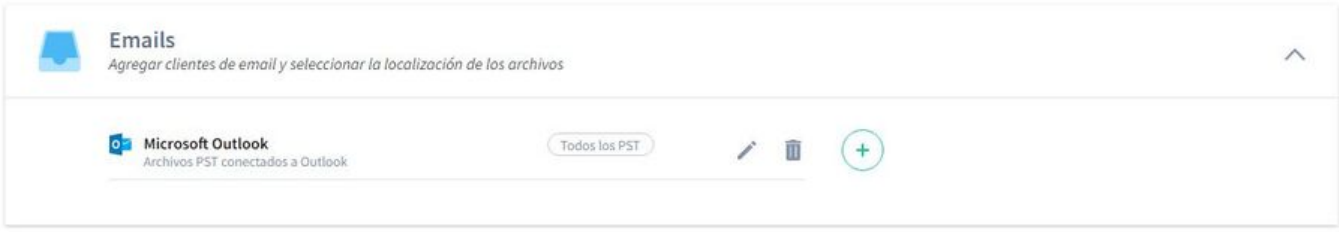
Unidades en la nube

La sección Unidades en la nube funciona de la misma manera que Ubicaciones, excepto que se aplica a las ubicaciones de almacenamiento en la nube, como One Drive.

Elija la unidad en la nube que desea que Aranda Datasafe respalde y proteja, y luego elija incluir todos los archivos, archivos globales y / o una selección de archivos personalizada.

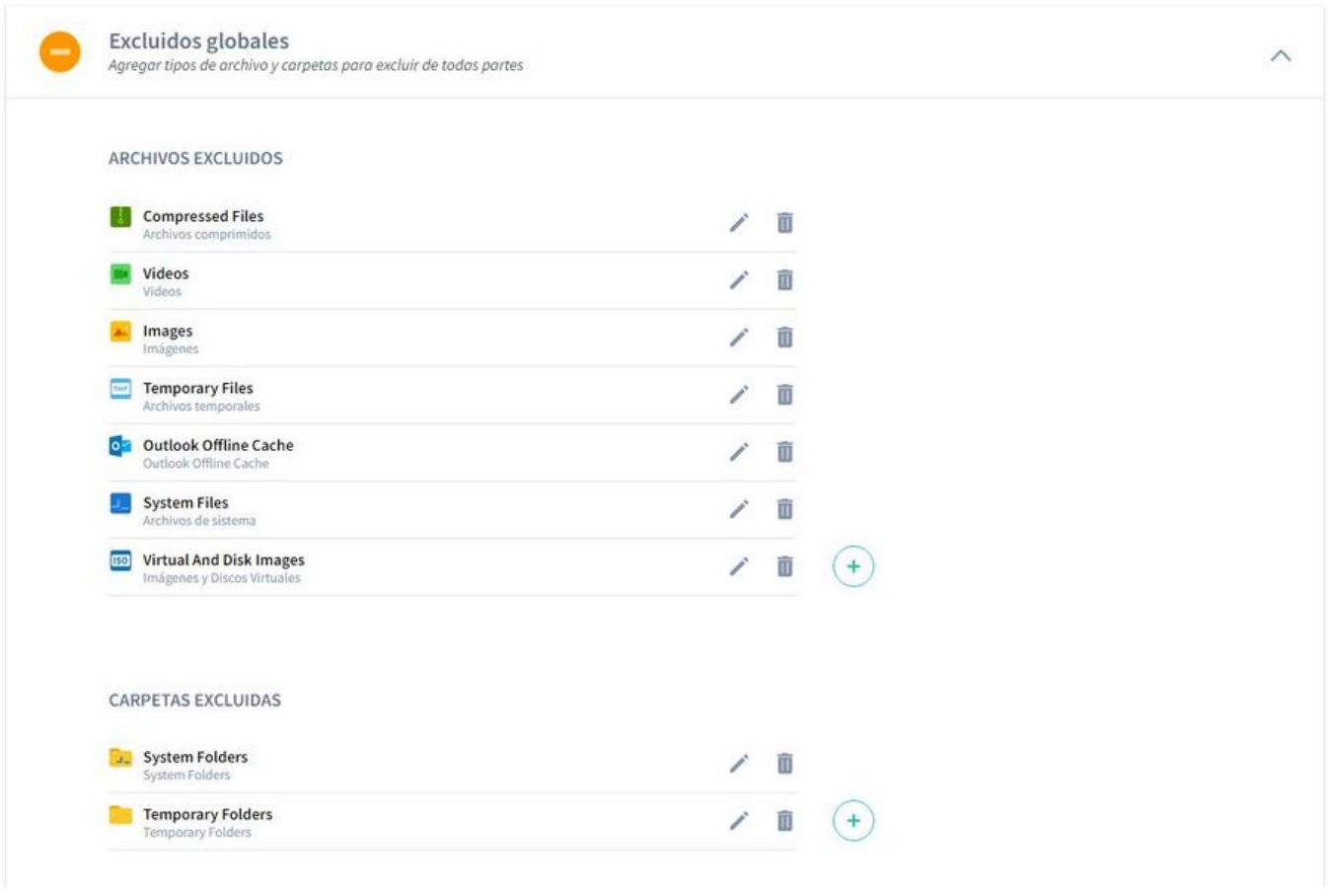
Emails

Utilice la sección Correos electrónicos para configurar Aranda Datasafe para realizar copias de seguridad y proteger los archivos de su cliente de correo electrónico. Por ejemplo, puede agregar Microsoft Outlook como cliente de correo electrónico y luego configurar Aranda Datasafe para hacer una copia de seguridad y proteger todos los archivos PST de Outlook o solo aquellos archivos PST que están activos en el perfil de Outlook.



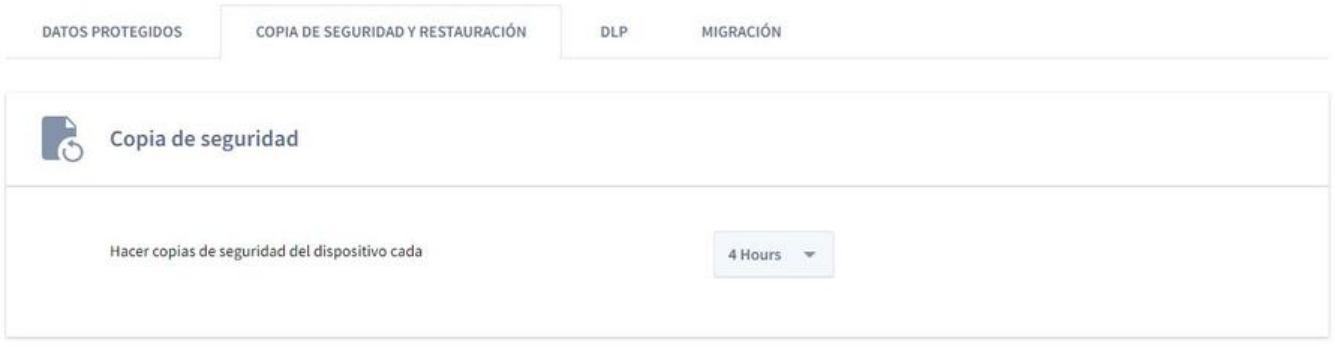
Exclusiones Globales

Utilice la sección Exclusiones globales para especificar qué tipos de archivos y carpetas no deben respaldarse ni protegerse. Tenga en cuenta que, si se incluye una carpeta o un tipo de archivo en Archivos globales y Excluidos globales, no se hará una copia de seguridad ni se protegerá (los archivos excluidos globales tienen prioridad sobre los archivos globales).



Copia de seguridad y restauración

Utilice la pestaña Copia de seguridad y restauración para establecer el cronograma para realizar copias de seguridad de los dispositivos (que utilizan la política) de forma regular.



DLP

La pestaña Prevención de pérdida de datos (DLP) es donde usted controla la configuración para proteger los datos localmente en los dispositivos. Estas configuraciones están diseñadas para proteger sus datos cuando un dispositivo (que usa esta política) se pierde o es robado.

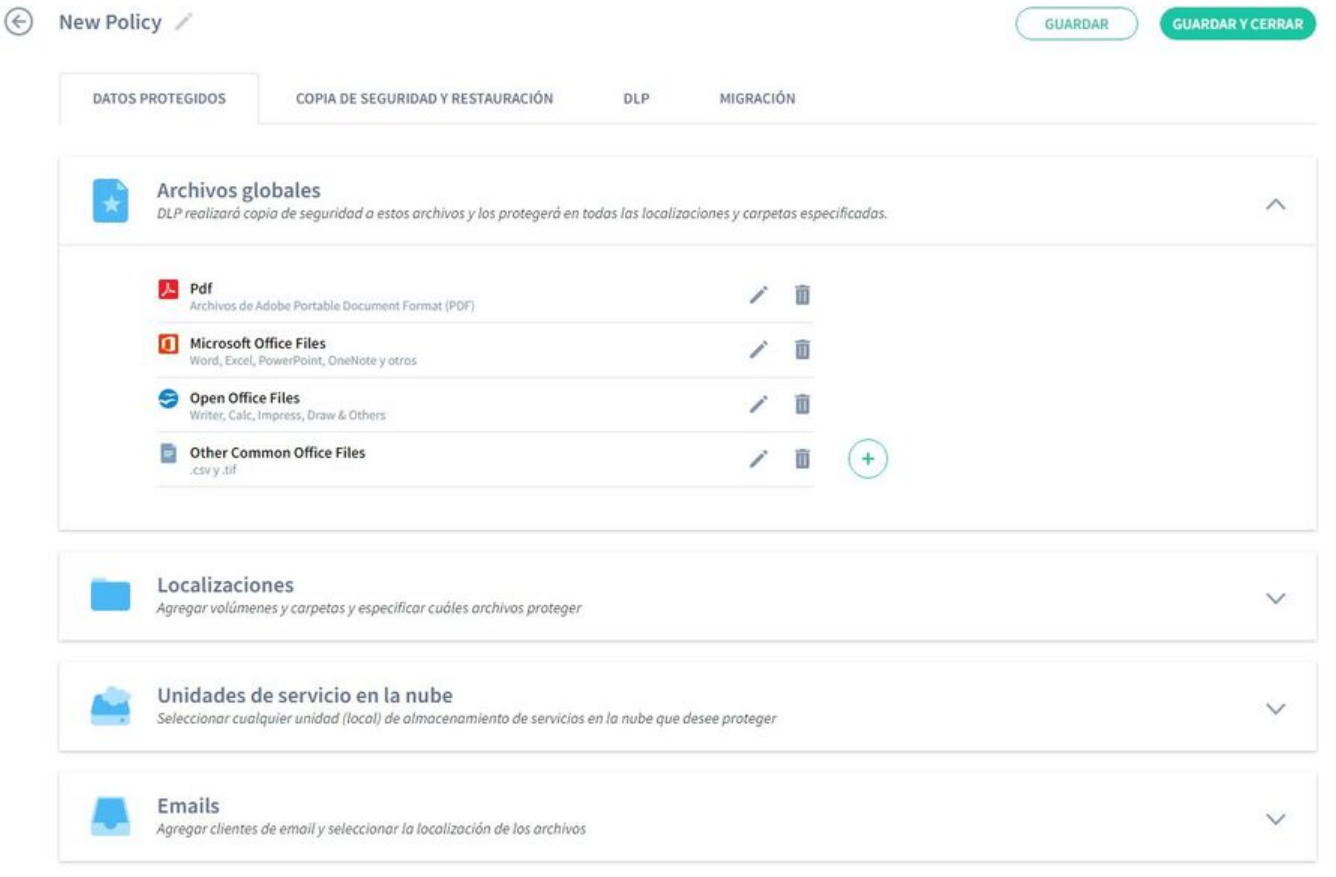
Puede elegir:

1. Habilite el cifrado de archivos locales en la máquina. Esto funciona cargando un certificado de cifrado de usuario en el dispositivo. Solo se puede acceder a los archivos si el certificado está disponible.
2. Evite el acceso a los archivos si el dispositivo no se conecta a Aranda Datasafe dentro de un período de tiempo establecido. El agente revoca automáticamente el certificado de cifrado del usuario, por lo que no se puede acceder a los archivos.
3. Utilice la geolocalización para encontrar la última ubicación conocida del dispositivo.

Migración

Utilice la configuración de Migración para controlar si Aranda Datasafe realiza una copia de seguridad de la configuración del perfil de usuario de Windows. Este tipo de datos incluye configuraciones de accesibilidad, configuraciones de mouse y teclado, favoritos y muchas otras configuraciones específicas del usuario.

Puede habilitar o deshabilitar la migración según sea necesario.



Asignar Políticas y Repositorios a sus Equipos

Puede asignar una política y un repositorio a cada uno de sus equipos. Estos le dicen a Aranda Datasafe qué dispositivos deben respaldarse y protegerse, con qué frecuencia se deben realizar las copias de seguridad y dónde se deben almacenar los datos.

Para asignar una política y un repositorio, debe editar el equipo.

1. Haga clic en **Inventario**.

2. En la barra de**Equipos**, ubique el cursor sobre el equipo al que va a asignar un repositorio y / o Política.

3. Haga clic en el botón de opción del Equipo (...).

4. Haga clic en **Editar**.

5. Elija una política de la lista.

6. Elija un repositorio de la lista.

7. Haga clic en Guardar equipo.

El equipo ahora está asociado con la política y el repositorio que seleccionó. Cada dispositivo asignado a ese equipo será respaldado y protegido de acuerdo con los detalles de la Política seleccionada. Los datos de los dispositivos del equipo se cifrarán y almacenarán en el repositorio seleccionado.

Activar Dispositivos

Cuando haya configurado sus equipos, repositorios y políticas, puede**activar** sus dispositivos.

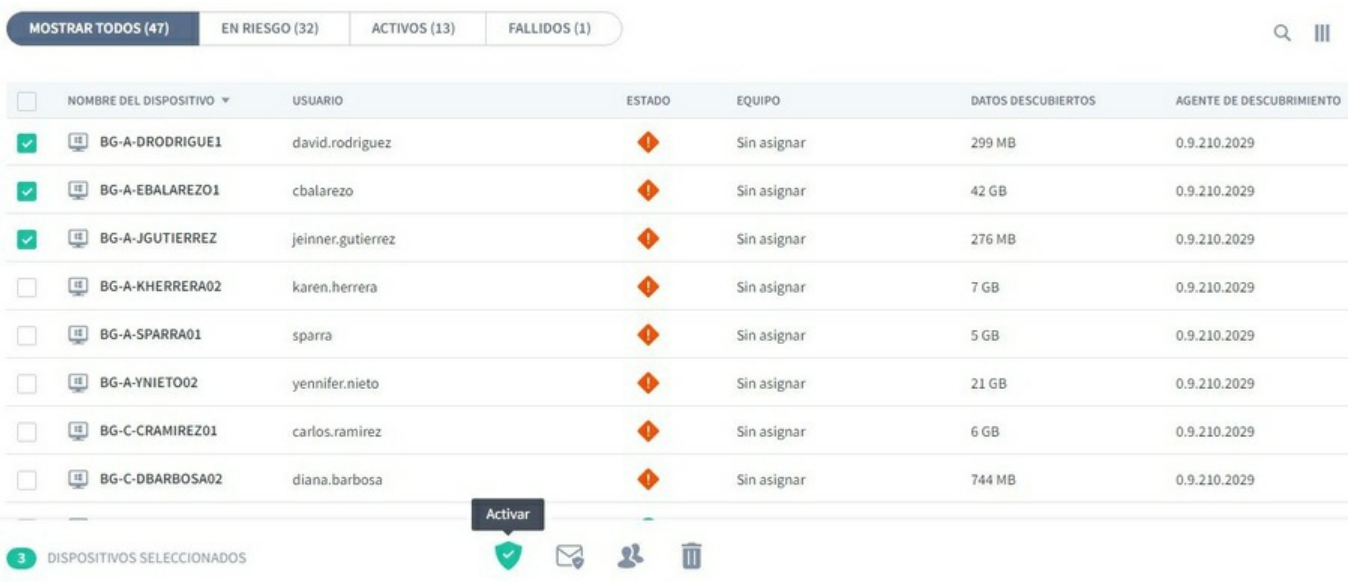
Cuando activa un dispositivo, crea una solicitud para que ese dispositivo sea protegido y respaldado. Si la solicitud de activación tiene éxito, el dispositivo estará protegido **cuando se programe la siguiente copia de seguridad**(como se define en la configuración de la Política).

Para activar un dispositivo:

Haga clic en **Inventario**. Busque el dispositivo que desea activar en la lista de dispositivos.

Para activar un solo dispositivo, puede hacer clic en su botón de opción (...) y luego hacer clic en**Activar**.

Para activar varios dispositivos, seleccione las casillas de verificación de los dispositivos que desea activar. Luego haga clic en el íconoActivar en la barra emergente en la parte inferior.



Cuando activa un dispositivo, su estado cambia de**En riesgo** a **Pendiente**. Después de un breve retraso (alrededor de 10 minutos si es la primera vez que se activa el dispositivo), el dispositivo realizará una copia de seguridad; si tiene éxito, el estado del dispositivo cambia a **Protegido** y se muestra una marca verde.

Si el dispositivo no se puede proteger, se muestra un ícono de escudo rojo. Deberá investigar por qué ha fallado la activación. Puede deberse a que el usuario no inició sesión en el dispositivo o hubo un problema relacionado con la conexión.

Copia de Seguridad

Cuando ha activado dispositivos en Aranda Datasafe, sus datos se respaldan automáticamente:

- Aproximadamente 10 minutos después de la activación inicial o después de que se inicia el agente
- Regularmente, de acuerdo con el cronograma de copias de seguridad (definido en la Política).

Una vez realizada la copia de seguridad automática inicial, también puede realizar una copia de seguridad de un dispositivo manualmente. La copia de seguridad se inicia desde Aranda Datasafe o utilizando el Agente de protección localmente en el dispositivo.

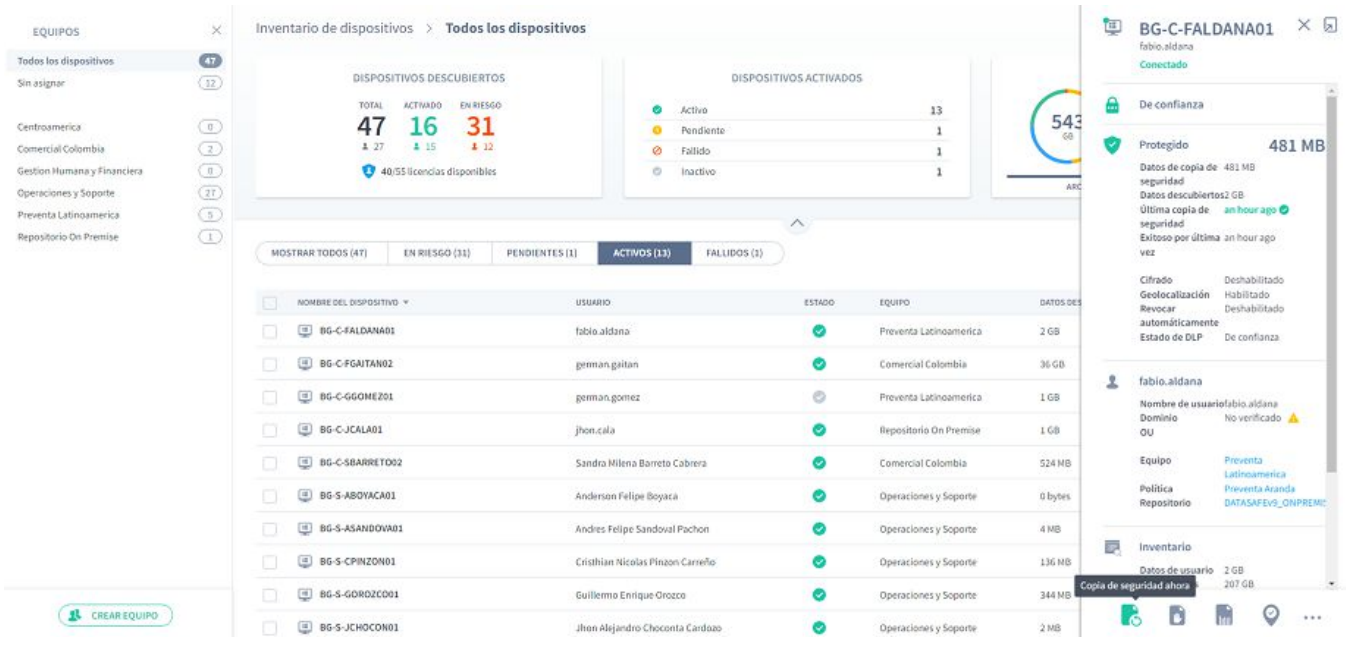
En este paso, aprenderá cómo iniciar una copia de seguridad desde Aranda Datasafe y luego verá información detallada sobre la copia de seguridad.

1. Haga clic en Inventario.

2. En la lista de dispositivos, haga clic en el dispositivo que desea respaldar. Sus detalles aparecen en un panel deslizable.

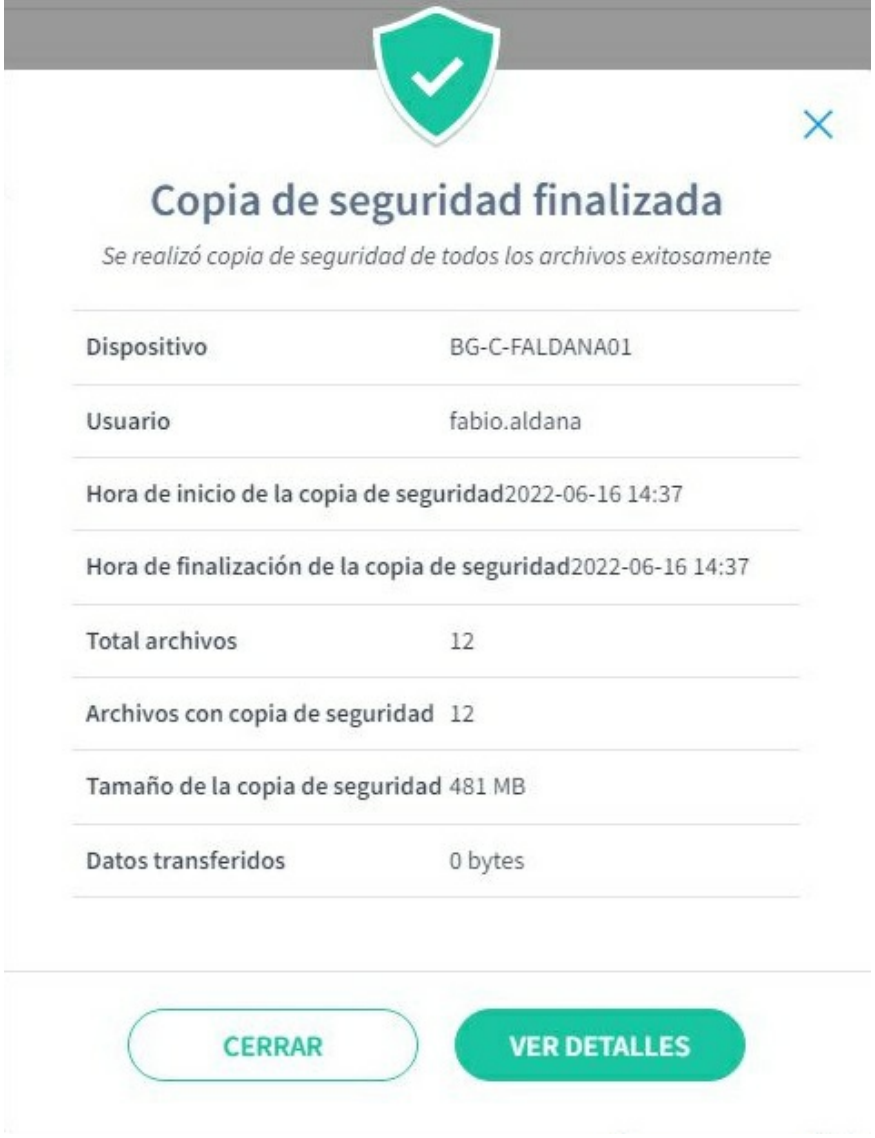
3. Haga clic en el ícono Hacer copia de seguridad ahora en la parte inferior del panel deslizante.

Aparece un mensaje de confirmación en la parte inferior de la pantalla para informarle que la solicitud de copia de seguridad se realizó correctamente.



El software Protection Agent (en el dispositivo del usuario) utiliza la deduplicación para asegurarse de que solo se realicen copias de seguridad de datos únicos en el repositorio. La cantidad de tiempo que se tarda en realizar una copia de seguridad de un dispositivo variará, dependiendo de la cantidad de datos que se deben indexar y realizar una copia de seguridad.

4. En el panel deslizante, haga clic en el enlace junto a la entrada Última copia de seguridad para mostrar un resumen de la copia de seguridad.



5. Para obtener información más detallada sobre la copia de seguridad, haga clic en Ver detalles. A continuación, puede ver los detalles de la copia de seguridad, el dispositivo, los archivos de los que no se pudo hacer una copia de seguridad y los registros de errores.

Restaurar en Dispositivo

Aranda Datasafe almacena copias de seguridad de los datos protegidos en sus dispositivos activados. Si los datos se eliminan accidentalmente en el dispositivo, puede restaurarlos descargándolos de Aranda Datasafe. También puede restaurar copias de seguridad de un dispositivo antiguo a un dispositivo nuevo.

Para **restaurar** archivos en un dispositivo:

1. Inicie sesión en el dispositivo que recibirá la copia de seguridad de los datos de Aranda Datasafe.

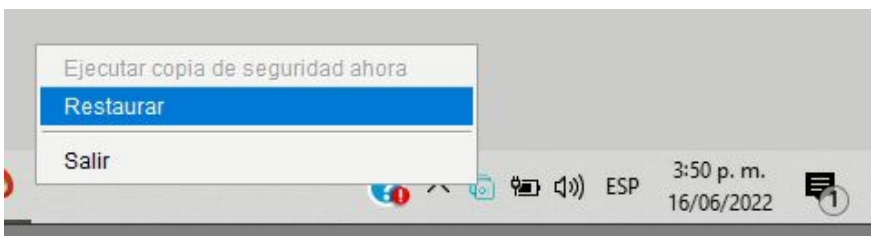
2. Si el dispositivo ya tiene instalado Discovery Agent, ignore los pasos 2 y 3 y continúe desde el paso 4.

3. Si necesita restaurar datos a un nuevo dispositivo o un dispositivo que no ha sido protegido por Aranda Datasafe antes, necesita instalar Discovery Agent. Continúe desde el paso 2.

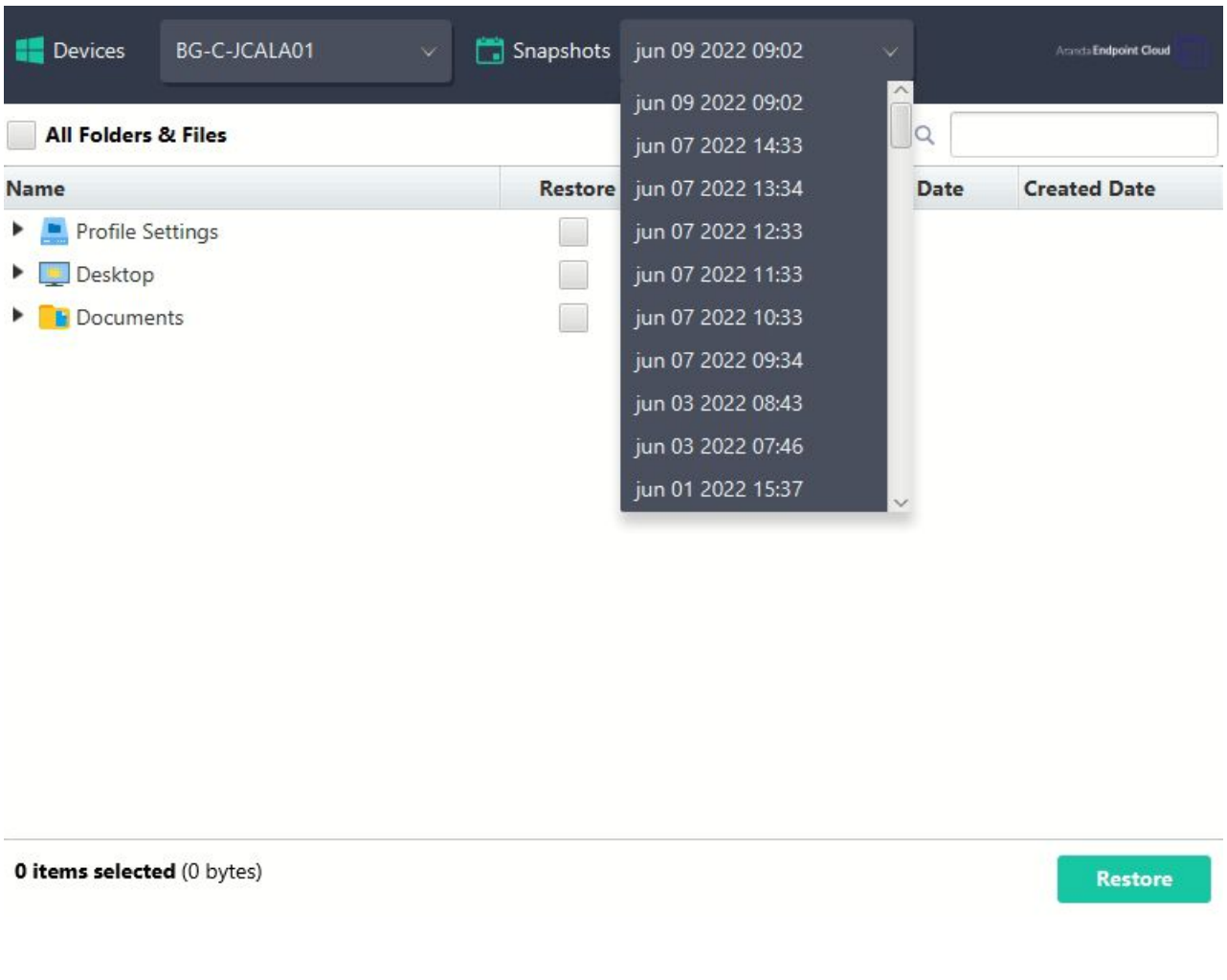
4. Instale Discovery Agent en el dispositivo, para que Aranda Datasafe pueda detectarlo.

5. En Aranda Datasafe, active el nuevo dispositivo.

6. En la barra de tareas de Windows, haga clic con el botón derecho en el ícono del Agente de protección y seleccione Restaurar.



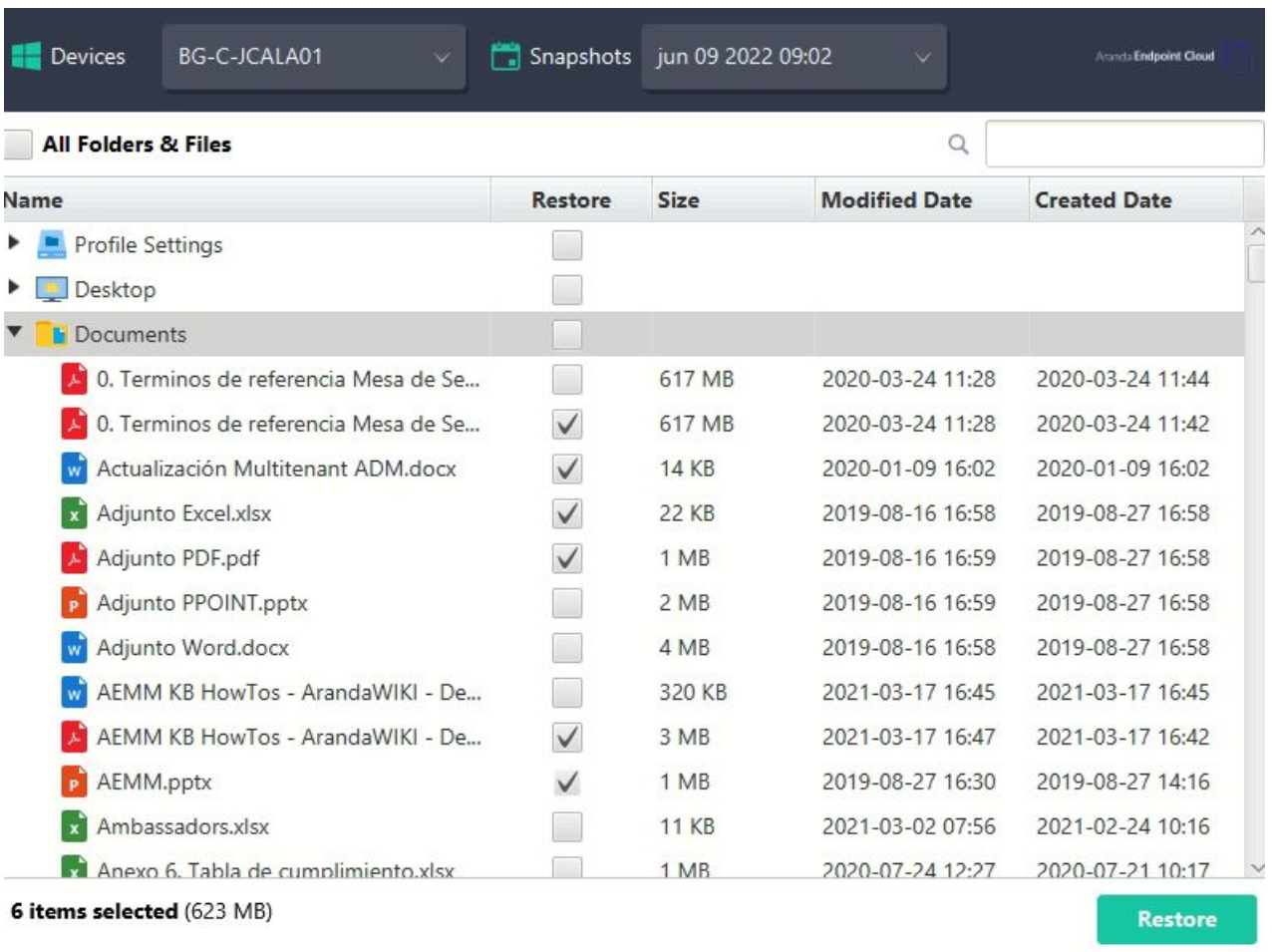
7. En la parte superior del Agente de Aranda Datasafe, elija el dispositivo que contenía los datos que desea restaurar. Luego, elija la instantánea adecuada. Una instantánea es un registro de los datos de un dispositivo en un momento específico y puede elegir entre cualquiera de los momentos que se muestran en la lista.



8. Elija qué archivos desea restaurar. Seleccione los archivos de las ubicaciones disponibles (Escritorio, C: \, etc.).

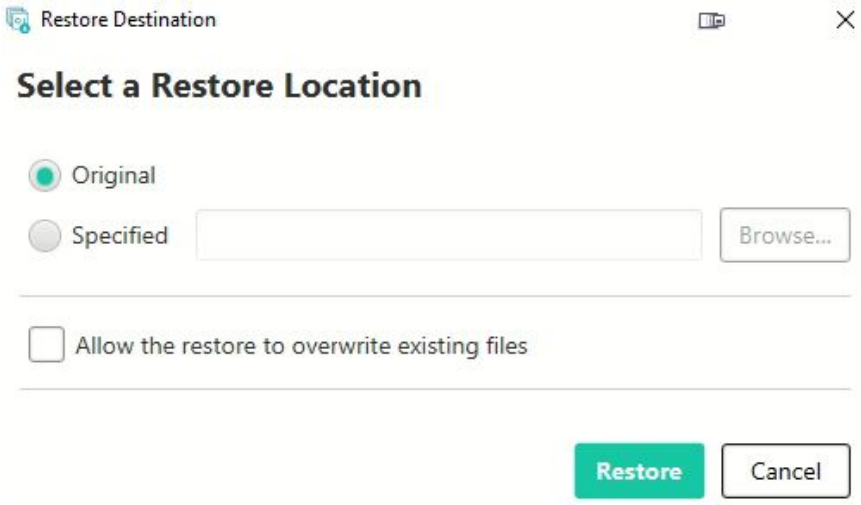
Si la política tiene habilitada la migración y la opción Perfiles de usuario de Microsoft Windows está seleccionada, también puede restaurar los datos del perfil de usuario. Seleccione la opción **Configuración de perfil** para restaurar esta configuración.

Si la función de migración está desactivada o los perfiles de usuario de Microsoft Windows no están seleccionados, solo puede optar por restaurar los datos de copia de seguridad.



9. Seleccione **Restaurar**.

10. . Elija la ubicación para los archivos de restauración. Aquí es donde se restaurarán en su nuevo dispositivo. Si elige **Original**, los archivos se recuperarán en la misma ubicación que tenían en el dispositivo anterior. O puede elegir una ubicación **especificada** diferente si lo prefiere.



Seleccione **Restaurar**.

Los datos seleccionados se restauran desde el repositorio a su dispositivo. Si ha elegido archivos de escritorio, los verá aparecer en el escritorio.

Si está restaurando los datos de respaldo y la configuración del perfil de usuario, la restauración se completará en dos fases separadas.

Prevención Pérdida de Datos

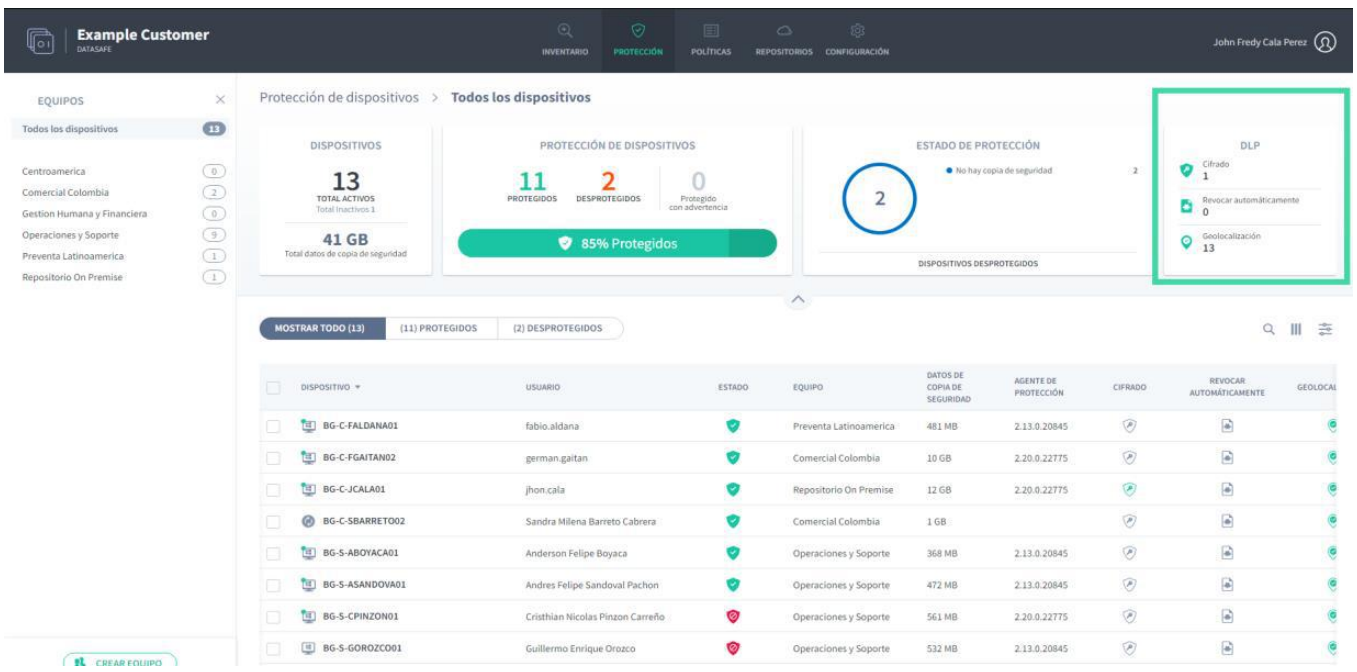
Aranda Datasafe tiene funciones de prevención de pérdida de datos (DLP) que mitigan su riesgo en caso de pérdida o robo de un dispositivo protegido. Las funciones están habilitadas en la Política [ver Crear una Política](#) y pueden proteger sus datos con:

- Cifrado de datos locales en sus dispositivos
- Prevención automática del acceso a datos protegidos si un dispositivo no se conecta dentro de un número específico de días (revocación automática)
- Proporcionarle la última ubicación conocida del dispositivo (geolocalización)
- Permitirle borrar de forma remota los datos respaldados en un dispositivo

Veamos cómo puede ver y usar las funciones de DLP.

Ver el estado de DLP

Puede ver el estado de DLP en la página Protección. Muestra la cantidad de dispositivos que tienen habilitadas las funciones de cifrado local, revocación automática y geolocalización (en la política).



El estado de DLP también se muestra en la lista de dispositivos en la parte inferior de la sección Protección.

Revocar un dispositivo

Si una política tiene habilitada el cifrado local, cada dispositivo recibe un certificado de cifrado que se almacena localmente en cada máquina. Los datos cifrados solo pueden ser accedidos por el usuario registrado si el certificado está en su lugar.

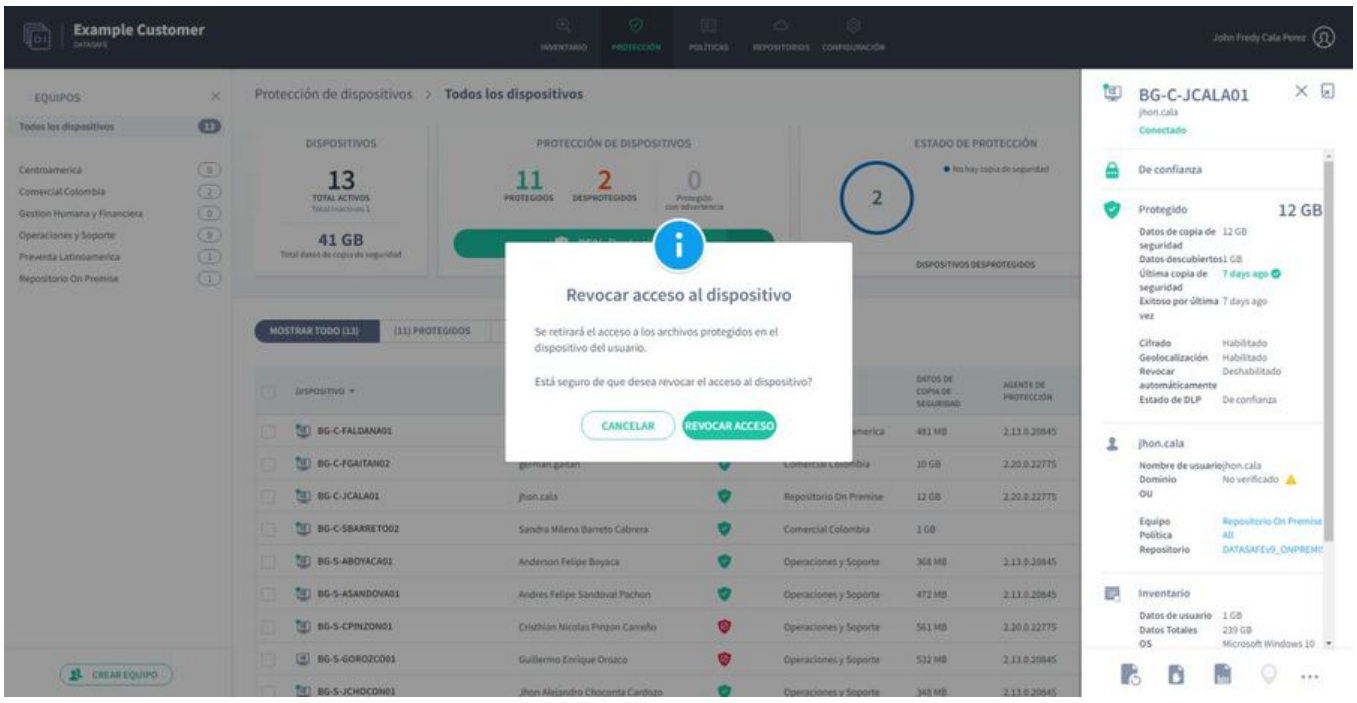
Al revocar un dispositivo, elimina el certificado para que no se pueda acceder a los datos cifrados.

1. Haga clic en **Protección**.

2. Haga clic en el dispositivo que desea revocar.

3. Haga clic en el ícono **Revocar dispositivo**.

4. Haga clic en **Revocar** para confirmar.



⚐ **Nota:** Si la revocación automática está habilitada en una política, Aranda Datasafe revocará automáticamente el certificado de cualquier dispositivo protegido que no se conecte a Aranda Datasafe dentro de un número específico de días. (Puede cambiar el período de tiempo de revocación automática en la configuración de la política).

Borrar un dispositivo

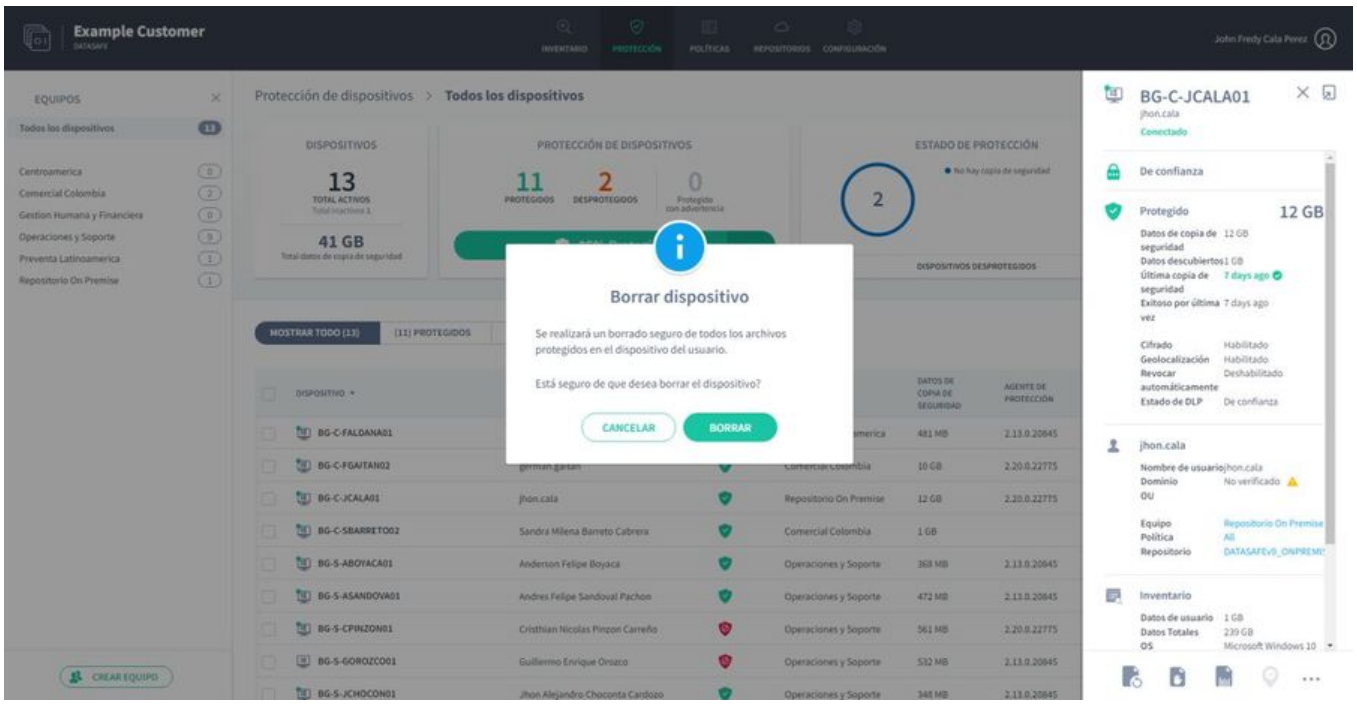
Puede borrar de forma remota los archivos protegidos en sus dispositivos. Con un borrado, los archivos protegidos se eliminan y Aranda Datasafe también realiza un "borrado forense" para eliminar cualquier rastro de los archivos en el dispositivo.

1. Haga clic en **Protección**.

2. Haga clic en el dispositivo que desea borrar.

3. Haga clic en el ícono **borrar**.

4. . Haga clic en Borrar para confirmar.



Localizar un dispositivo

Si una política tiene la geolocalización habilitada, puede ver la última ubicación conocida de un dispositivo protegido (el dispositivo debe tener Wi-Fi habilitado).

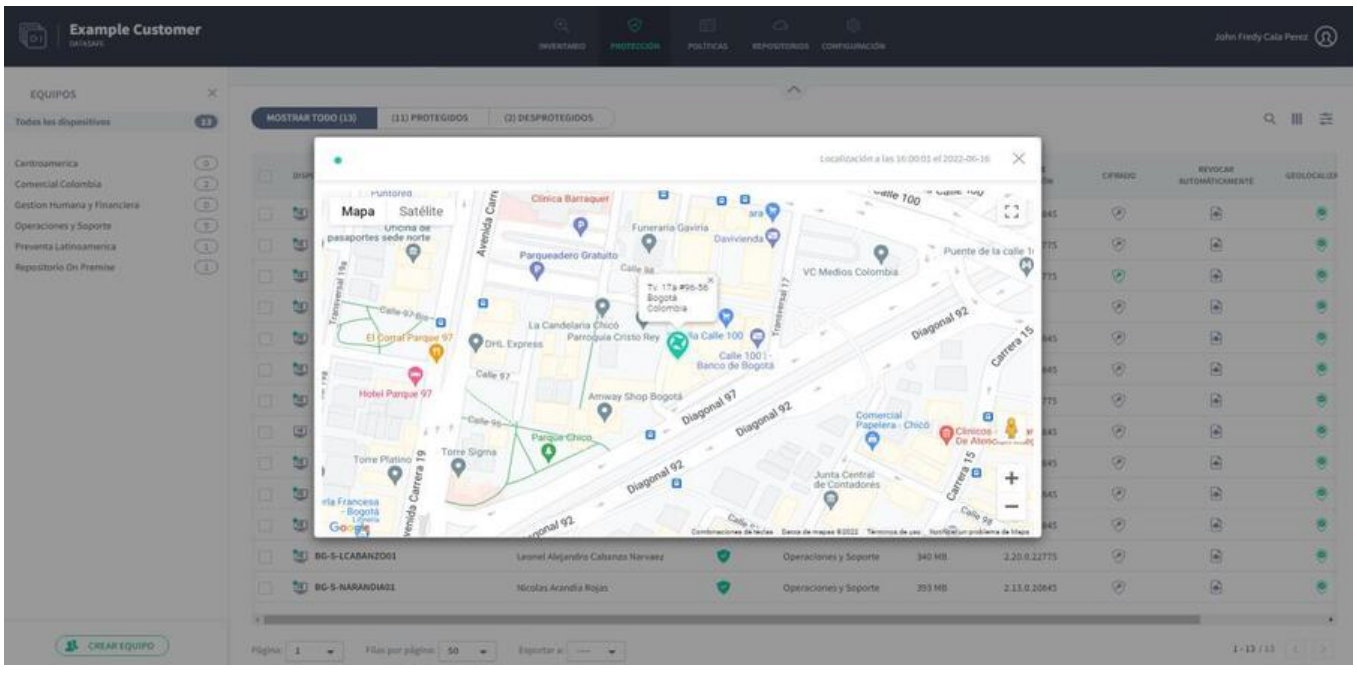
Para usar la geolocalización para encontrar un dispositivo:

1. Haga clic en **Protección**.

2. Haga clic en el dispositivo que desea ubicar.

3. Haga clic en el ícono Geolocalizar.

La última ubicación conocida se muestra en un mapa de Google. Puede acercar, alejar y mostrar la vista de satélite.



Migración de Configuración

En algún momento, lo más probable es que deba reemplazar uno de sus dispositivos protegidos. Por ejemplo, es posible que sea necesario actualizar un dispositivo antiguo a un modelo más nuevo o se puede perder o robar un dispositivo protegido. Para facilitar y agilizar la configuración de un nuevo dispositivo, Aranda Datasafe tiene una función de migración.

Con la función de migración, puede configurar Aranda Datasafe para realizar copias de seguridad mensuales de la configuración del perfil de usuario de Windows en dispositivos protegidos. Luego, cuando necesite reemplazar un dispositivo protegido, puede migrar su configuración de Aranda Datasafe al nuevo dispositivo de reemplazo.

Para utilizar la función de migración, debe habilitarla en las políticas relevantes.

Habilitar la migración de perfiles de usuario

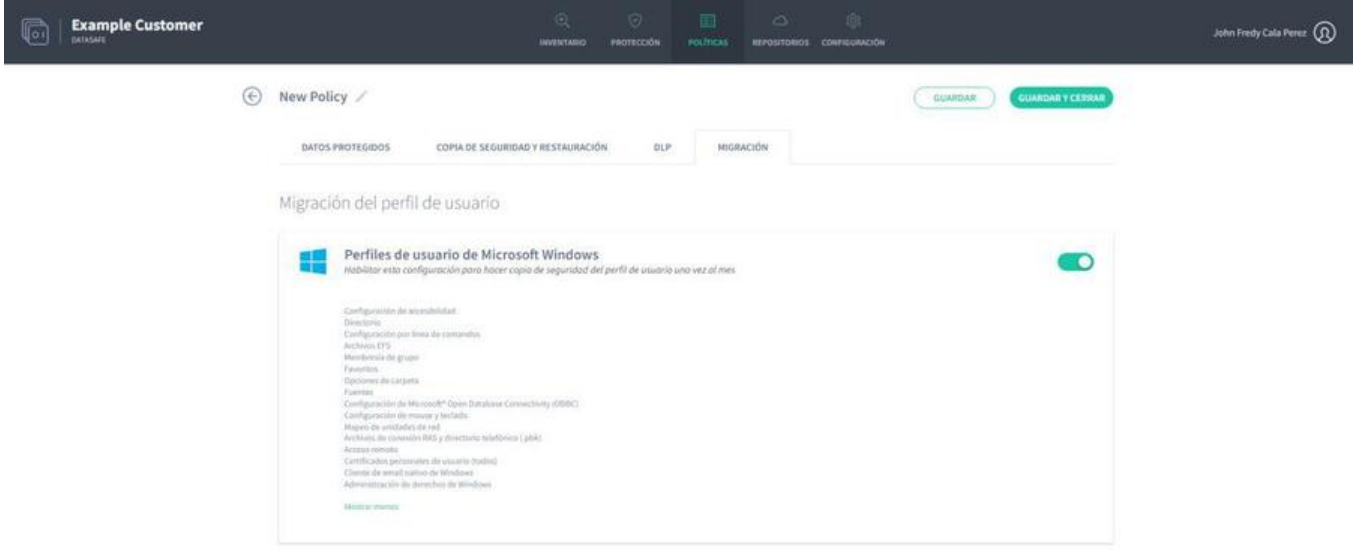
Para habilitar la función de migración de la configuración del perfil de usuario:

1. En Aranda Datasafe, haga clic en **Políticas**.

2. Edite la Política asociada con el equipo del dispositivo.

3. Haga clic en **Migración**.

4. Habilite la migración de perfiles para los**perfiles de usuario de Microsoft Windows**.



5. Haga clic en el enlace **Mostrar más** para ver una lista completa de la información del perfil de usuario de Windows que se respaldará. Incluye el diseño de la barra de tareas, unidades de red asignadas, opciones de carpeta, cuentas de correo electrónico, archivos pst adjuntos anteriormente y firmas de correo electrónico.

6. Haga clic en **Guardar y cerrar**.

Se hará una copia de seguridad de los datos y perfiles del usuario en los dispositivos protegidos cuando se realice la próxima copia de seguridad de los datos (según lo programado en la política).

Cuando se ha realizado una copia de seguridad, puede migrar la configuración a un nuevo dispositivo.

Migrar la configuración a un nuevo dispositivo

Si ha habilitado la migración en una política, puede usar Restaurar para transferir los datos del perfil de usuario de Windows (y los datos de respaldo) desde un dispositivo antiguo a un dispositivo nuevo (a través de Aranda Datasafe).

Para restaurar archivos en un dispositivo:

1. Inicie sesión en el nuevo dispositivo.

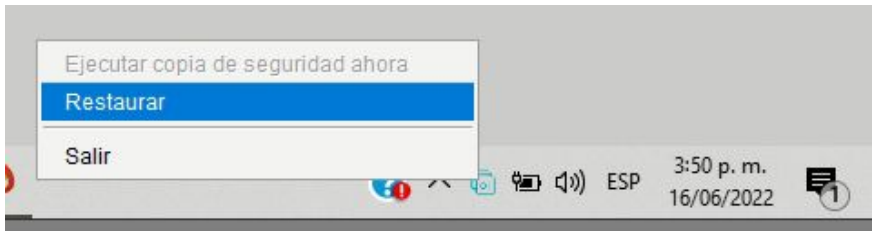
Si el dispositivo ya tiene instalado Discovery Agent, ignore los pasos 2 y 3 y continúe desde el paso 4.

Si necesita restaurar datos a un nuevo dispositivo o un dispositivo que no ha sido protegido por Aranda Datasafe antes, necesita instalar Discovery Agent. Continúe desde el paso 2.

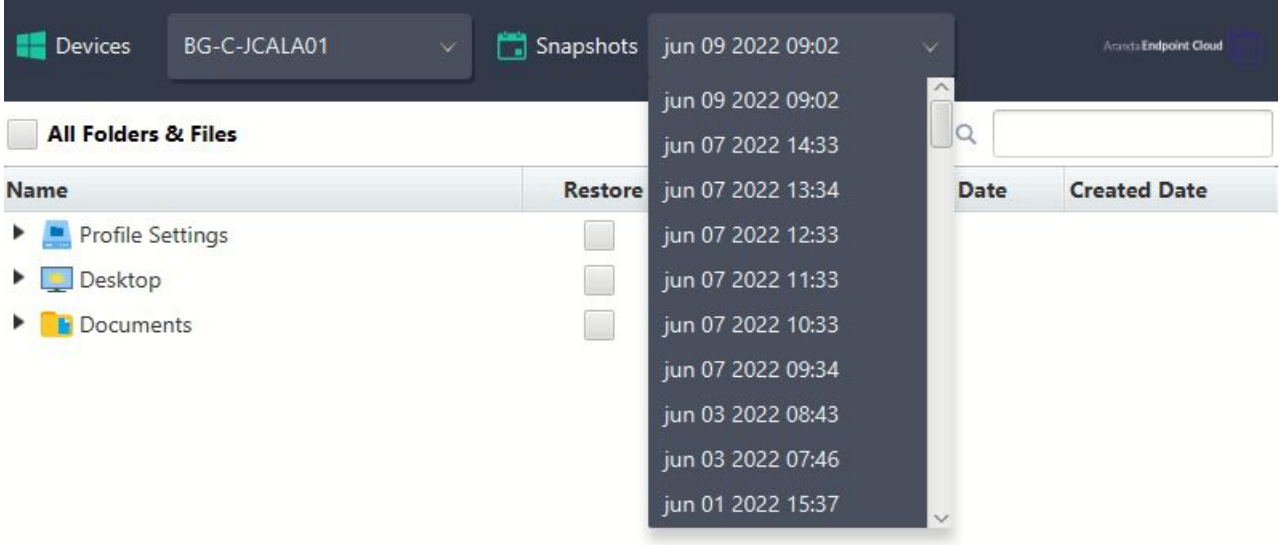
2. Instale Discovery Agent en el dispositivo, para que Aranda Datasafe pueda detectarlo.

3. En Aranda Datasafe, active el nuevo dispositivo.

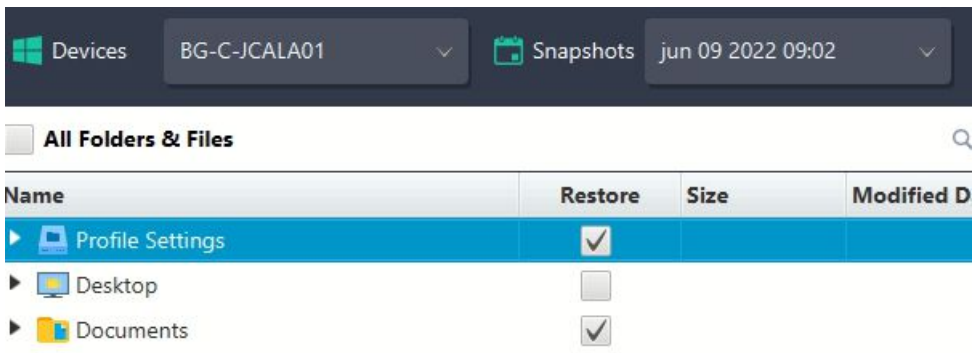
4. En la bandeja del sistema de Windows, haga clic con el botón derecho en el ícono del Agente de protección y seleccione **Restaurar**.



5. En la parte superior del Agente Aranda Datasafe, elija el dispositivo y luego la instantánea que desea migrar al nuevo dispositivo. La instantánea es un registro de los datos de un dispositivo en un momento específico y puede elegir entre cualquiera de los momentos que se muestran en la lista.

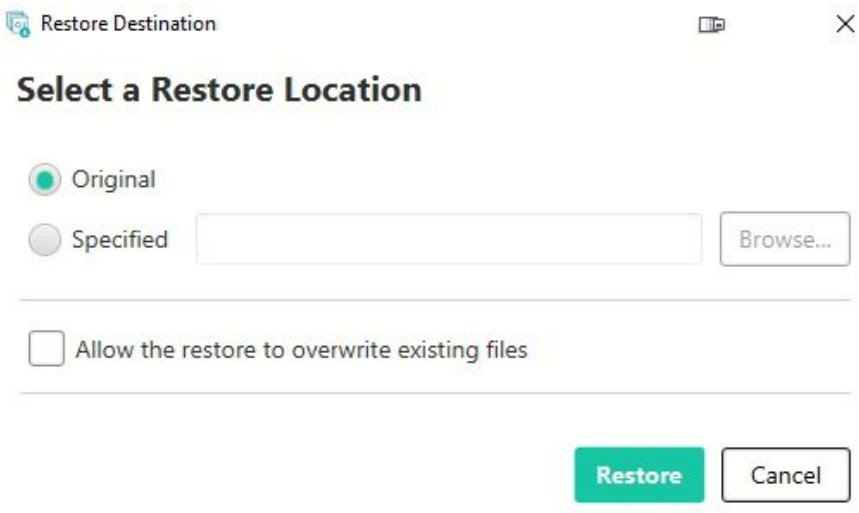


6. Elija qué archivos desea restaurar. Puede elegir **Todas las carpetas y archivos**, todos los archivos del escritorio, todos los documentos o todos los archivos de los volúmenes (unidades). Alternativamente, puede seleccionar archivos individuales.



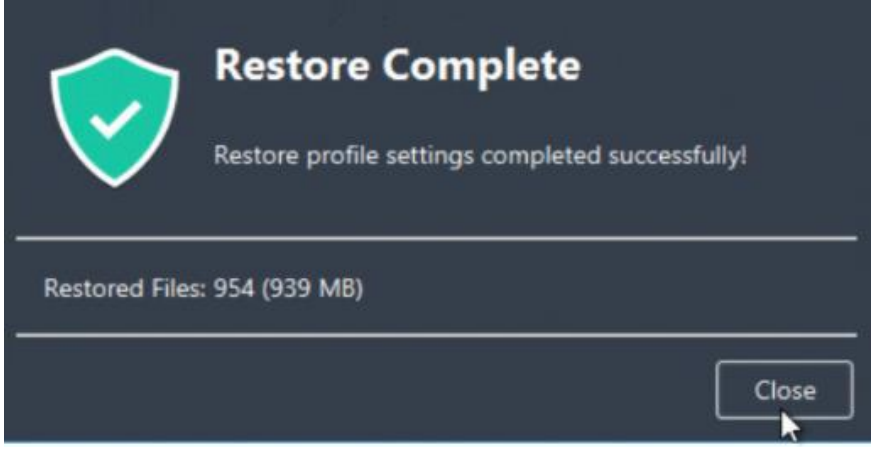
7. Seleccione **Restaurar**.

8. Elija la ubicación de los archivos migrados. Si elige **Original**, los archivos se cargarán en la misma ubicación que tenían en el dispositivo anterior. O puede elegir una ubicación **especifica** diferente si lo prefiere.



9. Seleccione **Restaurar**.

Los datos de usuario seleccionados y la información del perfil se descargan de Aranda Datasafe a su nuevo dispositivo. Si ha elegido archivos de escritorio, los verá aparecer en el escritorio.



Descubrimiento e Inventario

Descubrimiento e Inventario

Aranda Datasafe puede brindarle una descripción general de sus dispositivos y datos a escala global. Puede usar esta información para determinar qué tipos de datos tiene su organización, qué datos están en riesgo y cuánto espacio de almacenamiento se requiere para respaldarlos en Aranda Datasafe.

Para obtener una descripción general, instale la aplicación Discovery Agent en cada uno de sus dispositivos comerciales (pero no la instale en su servidor).

Discovery Agent permite que Aranda Datasafe detecte los dispositivos de sus usuarios automáticamente.

¿Qué es Discovery Agent?

El agente de descubrimiento es una aplicación liviana y gratuita que puede implementar en un número ilimitado de dispositivos en su organización. Le brinda una vista instantánea de sus dispositivos terminales y datos, para que pueda planificar su almacenamiento y comenzar a proteger sus dispositivos, todo desde Aranda Datasafe.

Cuando ejecuta Discovery Agent, analiza sus dispositivos y datos y crea un inventario. Aranda Datasafe utiliza el inventario para brindarle una gran cantidad de información sobre sus dispositivos y datos, incluidos detalles de:

- Los componentes de hardware que componen el dispositivo
- Las aplicaciones, controladores, servicios y actualizaciones instalados
- Los datos de los dispositivos, clasificados automáticamente en datos comerciales y no comerciales
- Estado de activación. Puede ver qué dispositivos están en riesgo y cuáles están activados para protección.

Puede acceder a toda esta información desde la página de Inventario de Aranda Datasafe.

Instalación y despliegue de Discovery Agent

Puede utilizar Discovery Agent de Aranda Datasafe para identificar:

- La cantidad de datos de su empresa que están en riesgo.
- Cuánto espacio de almacenamiento necesitará para realizar copias de seguridad y proteger sus dispositivos.

Discovery Agent es gratuito y le brinda una descripción general de sus dispositivos y datos. Debe instalarlo en todos los dispositivos que le gustaría respaldar y proteger con Aranda Datasafe.

Descargar Discovery Agent

Puede descargar e instalar Discovery Agent en todos los dispositivos que desee que se incluyan en el inventario de Aranda Datasafe**No instale Discovery Agent en sus servidores locales o servidores en la nube**.

En un dispositivo que desea que lo descubran:

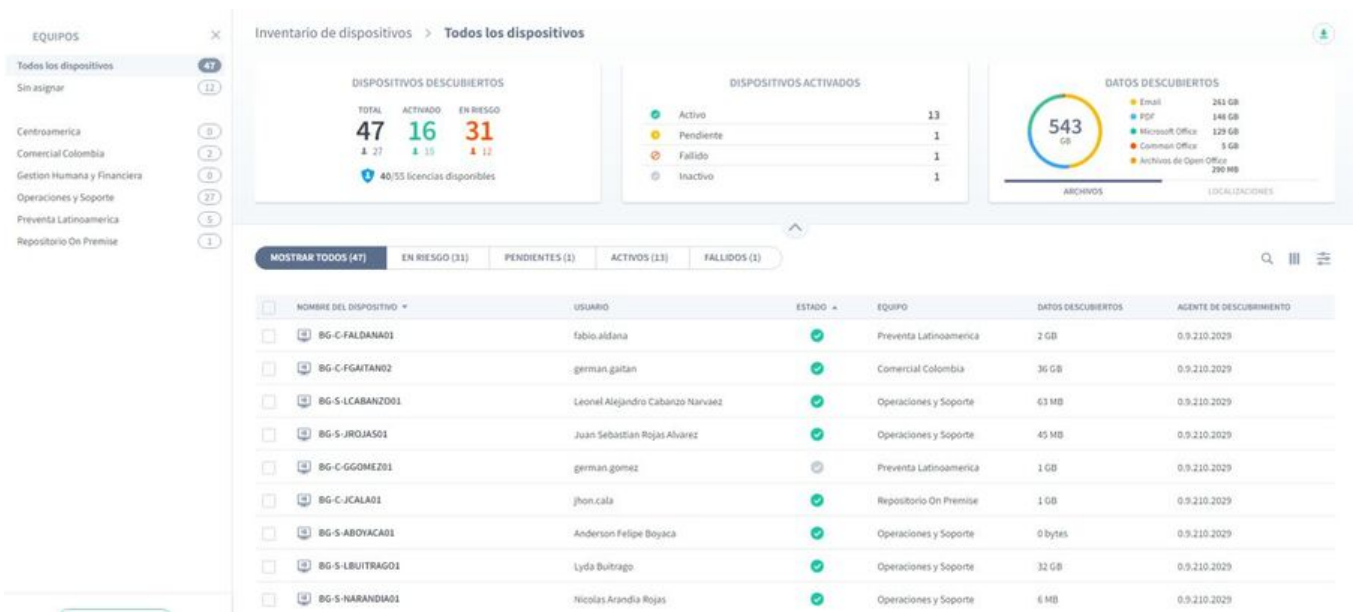
1. Inicie sesión en Aranda Datasafe como administrador.

Si Aranda Datasafe aún no ha descubierto ningún dispositivo, la página de Inventario no contiene información sobre el dispositivo y le aconseja que descargue el agente de descubrimiento.

Si Aranda Datasafe ha descubierto dispositivos, la página de Inventario muestra información sobre esos dispositivos.

2. Si Aranda Datasafe no ha descubierto ningún dispositivo, haga clic en Descargar Discovery Agent para comenzar a descargar un Discovery Agent que sea específico para su Tenant de Aranda Datasafe. (El paquete Discovery Agent MSI se descarga en su navegador).

Si Aranda Datasafe ha descubierto dispositivos anteriormente, haga clic en el ícono de descarga en la parte superior derecha, arriba del pane**Datos descubiertos##**. Discovery Agent comenzará a descargarse en su navegador.



Instale Discovery Agent en sus dispositivos de usuario final

Instale el paquete Discovery Agent MSI en cada dispositivo de usuario (computadora de escritorio, computadora portátil, etc.). El agente de descubrimiento realizará un inventario de dispositivos y datos, y luego cargará de forma segura la información en Aranda Datasafe.

Prerrequisitos

- Los dispositivos del usuario deben tener**acceso a Internet** ya que Discovery Agent necesita conectarse a Aranda Datasafe.
- Los dispositivos del usuario deben utilizar un**sistema operativo Windows**, Windows 7 o posterior. Pronto habrá una versión para Mac.
- **Los firewalls y los servidores proxy deben permitir las conexiones**. Es posible que deba incluir en la lista blanca endpointcloud.com y la ruta completa a la URL de tenant de Aranda Datasafe. Ejemplo: https://arandasoftware.endpointcloud.com donde **"arandasoftware"** se reemplaza por el nombre de su organización.

Puede instalar Discovery Agent de forma manual o remota en cada dispositivo.

Instalación manual del agente

Discovery Agent se puede instalar ejecutando el paquete MSI en cada dispositivo de usuario.

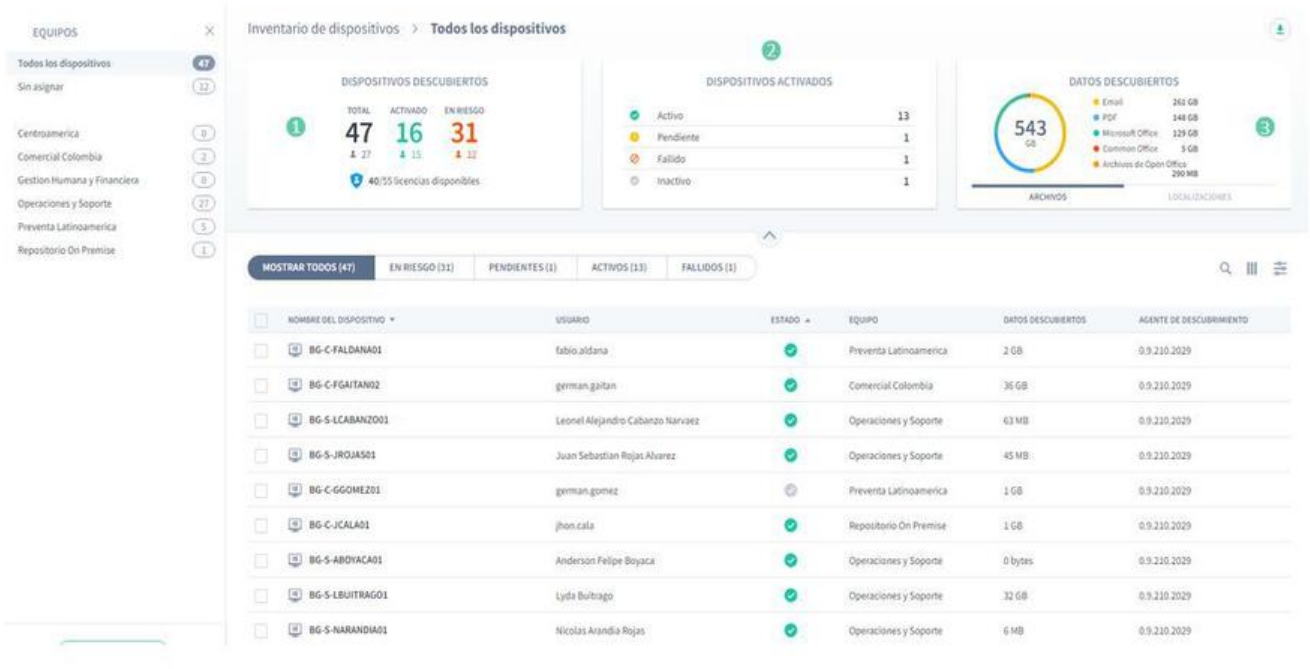
Es posible que desee mover el paquete MSI a una carpeta compartida a la que puedan acceder todos los dispositivos. Alternativamente, puede colocar el paquete MSI en una tarjeta de memoria y transferirlo entre dispositivos de esa manera.

Instalación remota del agente

Puede instalar el paquete MSI en los dispositivos de forma remota, utilizando la función de directiva de grupo de Active Directory o una aplicación de terceros. Para obtener más detalles, comuníquese con el soporte de Aranda (reportedecasos@arandasoft.com).

Inventario de Dispositivos

La página de Inventario muestra información sobre los dispositivos que Aranda Datasafe ha descubierto. Esta información incluye detalles sobre cada dispositivo, la cantidad de datos descubiertos y el estado de protección de cada dispositivo.



Dispositivos descubiertos

El panel Dispositivos descubiertos proporciona un resumen de los dispositivos que se han descubierto.

Campo	Descripción
Total	El número total de dispositivos que se han descubierto (dispositivos activados + dispositivos en riesgo). Debajo del número total está el número de usuarios. En la imagen de arriba, Aranda Datasafe ha descubierto 47 dispositivos y 27 usuarios.
Activos	La cantidad de dispositivos descubiertos que se han activado. Los dispositivos que están activados están siendo respaldados y protegidos o están esperando ser respaldados y protegidos. Cuando activa un dispositivo por primera vez, su estado se establece en activado, pero la activación no comienza hasta que se realiza la siguiente copia de seguridad. Debajo del número activado está el número de usuarios que han activado sus dispositivos.
En Riesgo	La cantidad de dispositivos descubiertos que no se han activado y, por lo tanto, no están protegidos o respaldados por Aranda Datasafe.
Licencias Disponibles	La cantidad de licencias que se utilizan actualmente y la cantidad total de licencias que tiene disponibles.

Dispositivos activados

El panel Dispositivos activados proporciona información sobre los dispositivos que se han activado (configurados para ser respaldados y protegidos).

Campo	Descripción
Activos	La cantidad total de dispositivos que se han activado y actualmente están respaldados y protegidos por Aranda Datasafe.
Pendiente	La cantidad de dispositivos descubiertos que han sido activados pero que aún no están respaldados y protegidos por Aranda Datasafe. Se activarán cuando el agente de protección se autentique correctamente.
Fallido	La cantidad de dispositivos descubiertos que no se pudieron activar. Una activación puede fallar si Protection Agent no se descargó e instaló o si el usuario no está autenticado con Active Directory.
Inactivo	La cantidad de dispositivos descubiertos que no se han conectado a Aranda Datasafe en los últimos 30 días.

Datos descubiertos

El panel de Datos descubiertos proporciona un resumen de los tipos de datos comerciales que Aranda Datasafe ha encontrado en sus dispositivos. De forma predeterminada, muestra los archivos con un resumen de los tipos de archivos y la cantidad de espacio de almacenamiento necesario para realizar una copia de seguridad.

Si hace clic en Ubicaciones, el panel proporciona un resumen de los distintos lugares donde se encuentran los datos en sus dispositivos. También proporciona detalles del espacio de almacenamiento necesario para realizar una copia de seguridad de cada ubicación.

Barra lateral de equipos

En el lado izquierdo de la página de Inventario está la barra lateral de Equipos. Esto muestra una lista de los equipos que están configurados en Aranda Datasafe (más Todos los dispositivos y Sin asignar, que están integrados).

Si hace clic en un equipo, los paneles de inventario y la lista se actualizan para que solo muestre información de los dispositivos del equipo seleccionado. Puede hacer clic en Todos los dispositivos para configurar el Inventario para que muestre los datos de cada dispositivo.

Lista de dispositivos

La sección inferior del Inventario muestra la lista de dispositivos, que contiene un resumen de los dispositivos que Aranda Datasafe ha descubierto.

NOMBRE DEL DISPOSITIVO	USUARIO	ESTADO	EQUIPO	DATOS DESCUBIERTOS	AGENTE DE DESCUBRIMIENTO
BG-C-FALDANA01	fabio.aldana		Preventa Latinoamerica	2 GB	0.9.210.2029
BG-C-FGAITAN02	german.gaitan		Comercial Colombia	36 GB	0.9.210.2029
BG-S-LCABANZO01	Leonel Alejandro Cabanzo Narvaez		Operaciones y Soporte	63 MB	0.9.210.2029
BG-S-JROJAS01	Juan Sebastian Rojas Alvarez		Operaciones y Soporte	45 MB	0.9.210.2029
BG-C-GGOMEZ01	german.gomez		Preventa Latinoamerica	1 GB	0.9.210.2029
BG-C-JCALA01	jhon.cala		Repositorio On Premise	1 GB	0.9.210.2029

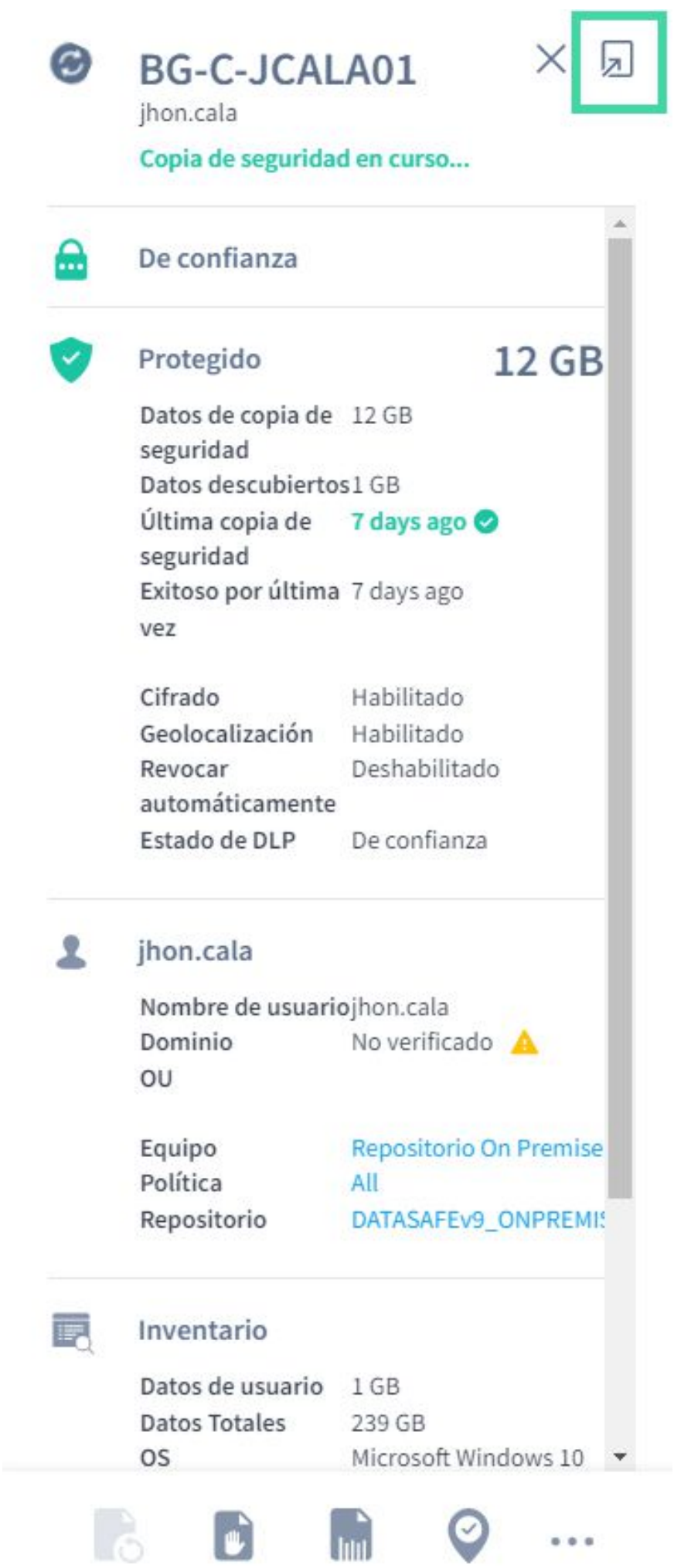
Campo	Descripción
Nombre	El nombre del dispositivo Dispositivo
Usuario	El nombre del usuario asociado al dispositivo
Estado	Muestra el estado del dispositivo: - Activo (Ícono verde de verificacion) - Activación Pendiente (ícono Amarillo de reloj) - En riesgo (Ícono rojo de advertencia) - Fallido (ícono rojo de fallido)
Equipo	El equipo al que el dispositivo este asignado
Datos descubiertos	La cantidad de data de negocio descubierta
Agente de descubrimiento	El número de versión del software Discovery Agent que se utilizó para descubrimiento encontrar el dispositivo.

Si resalta un dispositivo en la lista, aparece un botón de opción (...) a la derecha del nombre del dispositivo. Haga clic en el botón de opción para mostrar un menú contextual con estas opciones:

Campo	Descripción
Ver	Muestra la página Dispositivo, que contiene detalles sobre el dispositivo, incluido su hardware y software.
Activar	Úselo para activar el dispositivo para que Aranda Datasafe comience a respaldarlo y protegerlo. Solo puede activar un dispositivo si está asignado a un equipo y el equipo está asignado a un repositorio y una política.
Asignar Equipo	Úselo para asignar el dispositivo a un equipo. Aranda Datasafe solo puede respaldar y proteger los dispositivos que están asignados a los equipos, ya que los equipos deben estar asociados con un repositorio y una política.
Borrar	Úselo para eliminar un dispositivo.

Barra lateral del dispositivo

Si hace clic en un dispositivo de la lista de dispositivos, aparece la barra lateral del dispositivo. Muestra información adicional sobre el dispositivo seleccionado. Si hace clic en el ícono Ver en la esquina superior, Aranda Datasafe muestra la página del Dispositivo, que contiene una vista más detallada del dispositivo, incluido su hardware y software.

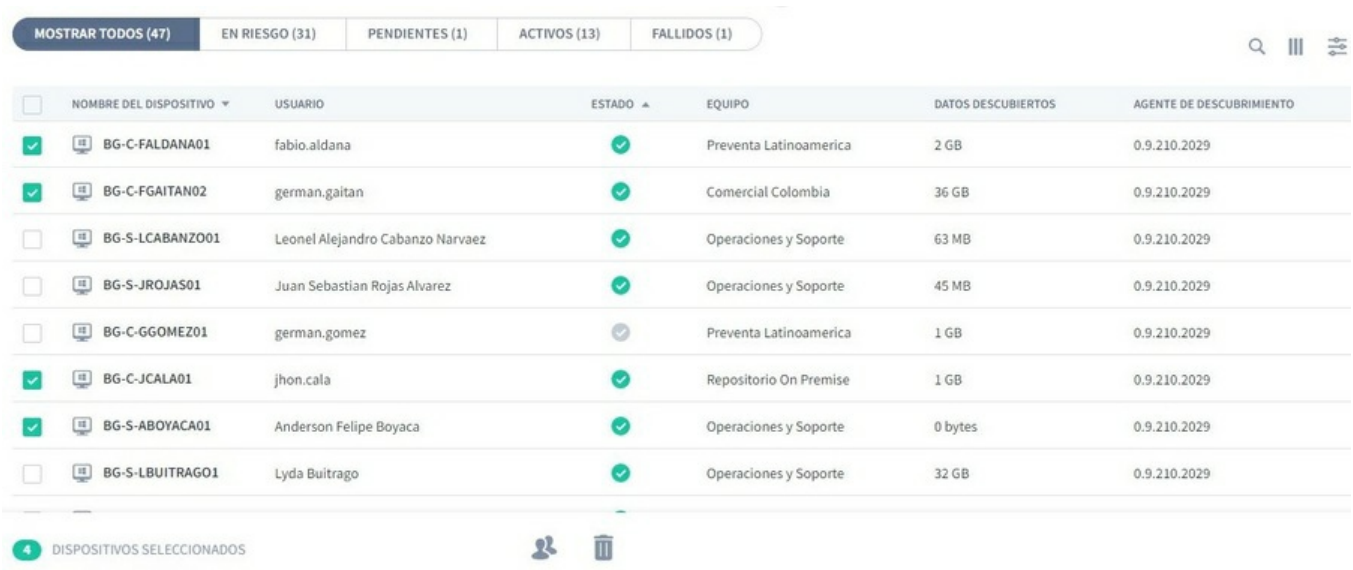


En la parte inferior de la barra lateral del dispositivo, hay íconos para realizar una copia de seguridad manual del dispositivo, revocarlo, borrarlo y utilizar la geolocalización para descubrirlo.

Acciones multidispositivo

Puede utilizar la lista de dispositivos para aplicar una sola acción a varios dispositivos. Por ejemplo, puede asignar varios dispositivos al mismo equipo.

Utilice la casilla de verificación a la izquierda de cada fila de dispositivos para seleccionar un dispositivo. Cuando selecciona las casillas de verificación, las opciones de acción aparecen al final de la lista. Estos funcionan de la misma manera que para dispositivos individuales, excepto que la acción se aplicará a todos los dispositivos que seleccionó.



Dispositivos

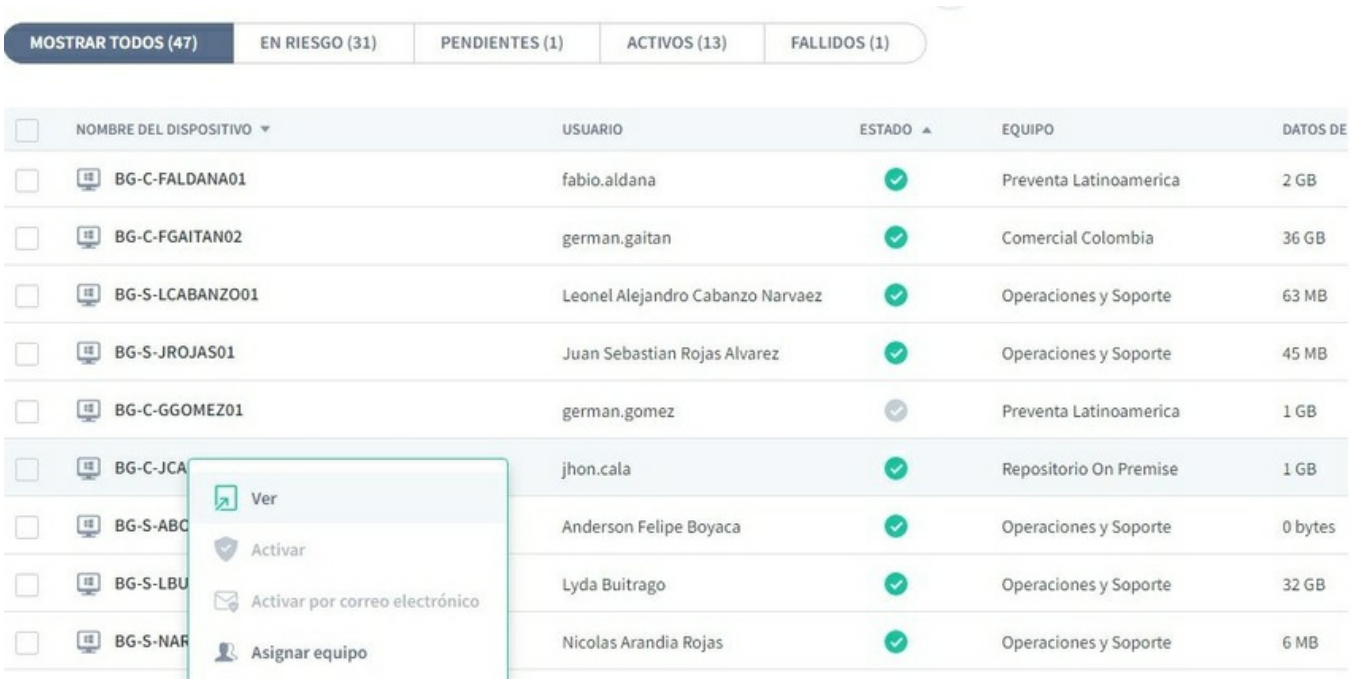
Aranda Datasafe proporciona una página de dispositivo para cada dispositivo que descubre. La página Dispositivo proporciona información detallada sobre el estado, los datos, el hardware y el software del dispositivo.

Para acceder a la página **Dispositivo** de un dispositivo:

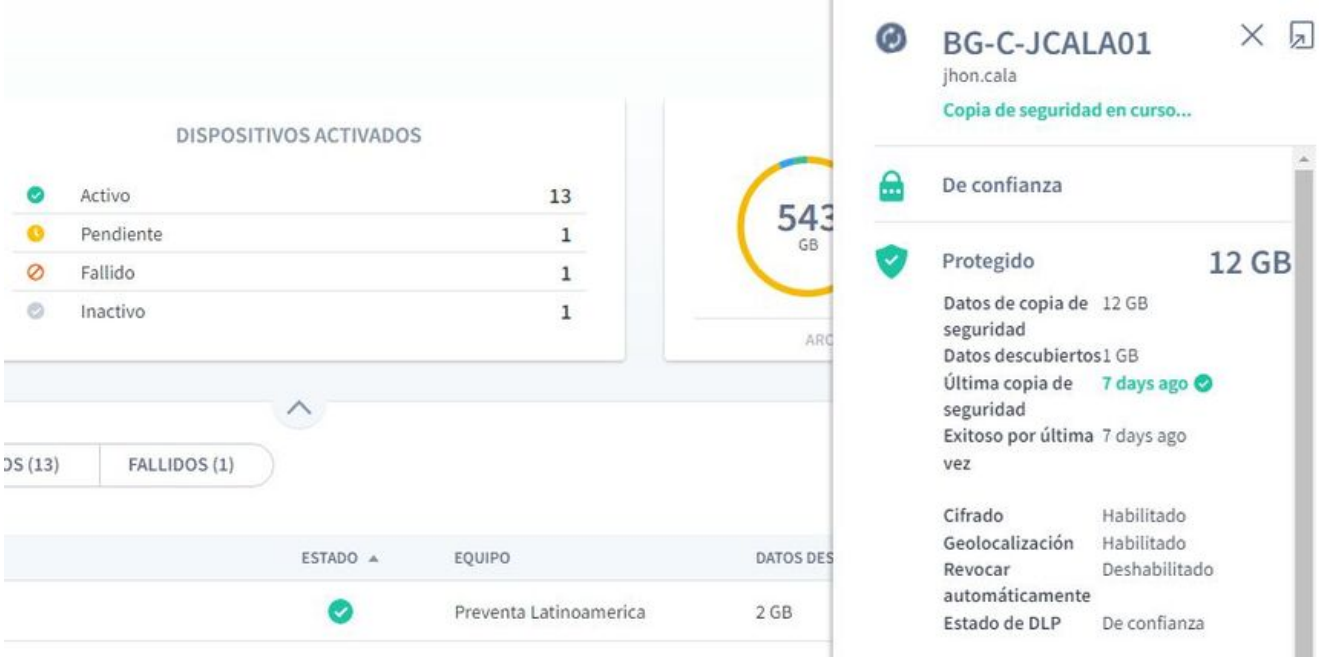
1. Haga clic en **Inventario** o **Protección**.

2. Haga clic en el botón de opciones (...) del dispositivo en la lista de dispositivos.

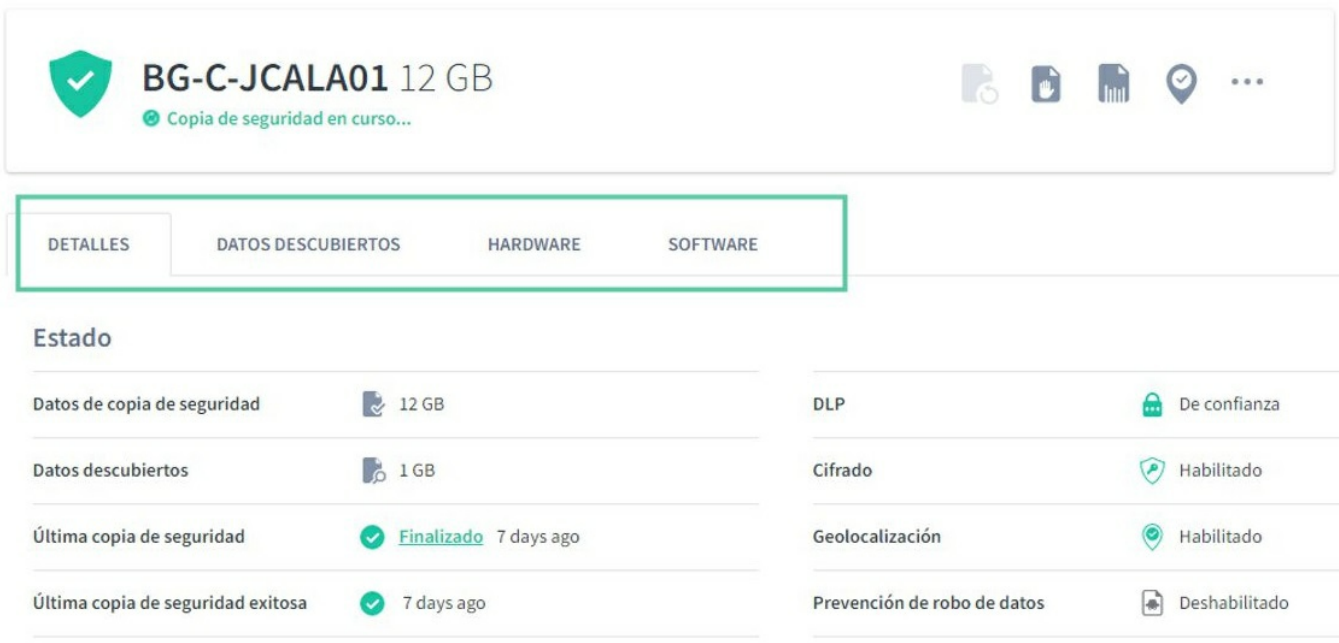
3. Haga clic en **Ver**.



De forma alternativa, puede hacer clic en el dispositivo en la lista de dispositivos y luego seleccionar el ícono **Ver** en la parte superior del panel deslizante.

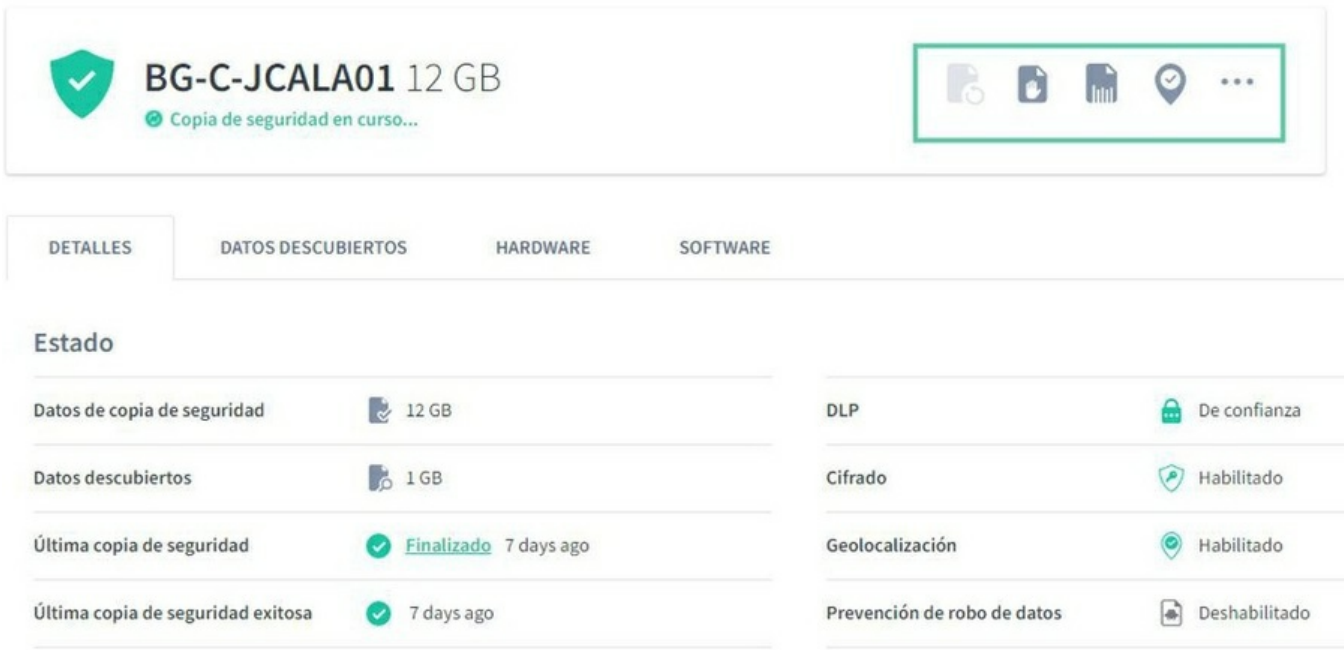


La página Dispositivo tiene un panel de acciones en la parte superior y pestañas de información debajo. La pestaña **Detalles** se muestra de forma predeterminada y puede seleccionar **Datos descubiertos**, **Hardware** y **Software**.



Acciones

El banner de nombre y estado en la parte superior de la página Dispositivo contiene varios íconos de acción. La disponibilidad de los íconos varía según las funciones que estén habilitadas en la Política y si se ha activado el Agente de protección.



Puede utilizar los íconos de acción solo una vez que se haya activado el Agente de protección:

- Hacer una copia de seguridad de un dispositivo manualmente
- Revocar un dispositivo.
- Limpiar un dispositivo.
- Localizar un dispositivo.

Detalles

La pestaña Detalles se muestra de forma predeterminada y proporciona información sobre la vista del dispositivo de Aranda Datasafe.

La sección Estado incluye el tamaño de los datos de la copia de seguridad, la cantidad de datos descubiertos, la hora y el estado de la copia de seguridad más reciente y si las funciones de DLP están habilitadas.

La sección Perfil muestra las credenciales del perfil de usuario y el equipo, la política y el repositorio con los que está asociado el dispositivo.

La sección Dispositivo muestra información sobre el sistema operativo y los agentes que se ejecutan en el dispositivo. También muestra los detalles de la conexión de red.

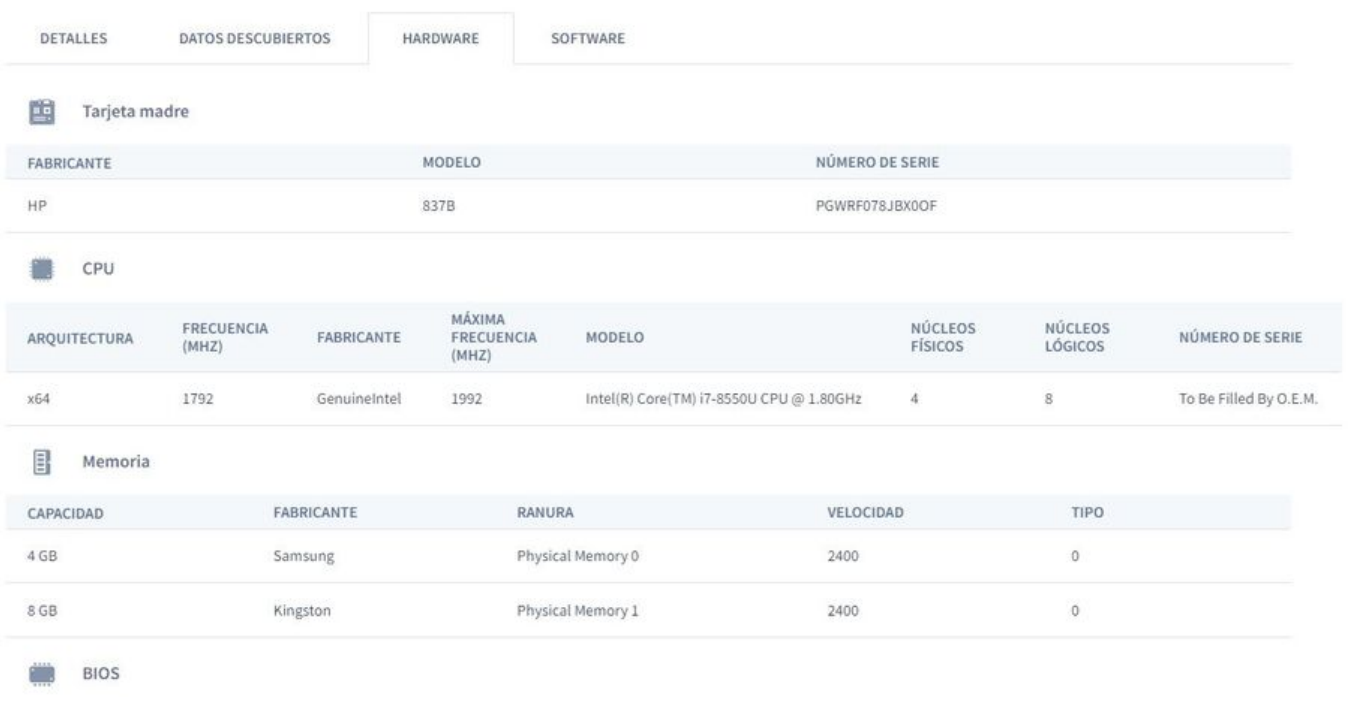
Datos descubiertos

La pestaña Datos descubiertos proporciona información sobre los datos que Aranda Datasafe ha descubierto en el dispositivo.

Hay información sobre los tipos de archivo que Aranda Datasafe ha descubierto y también las ubicaciones donde se encontraron los datos.

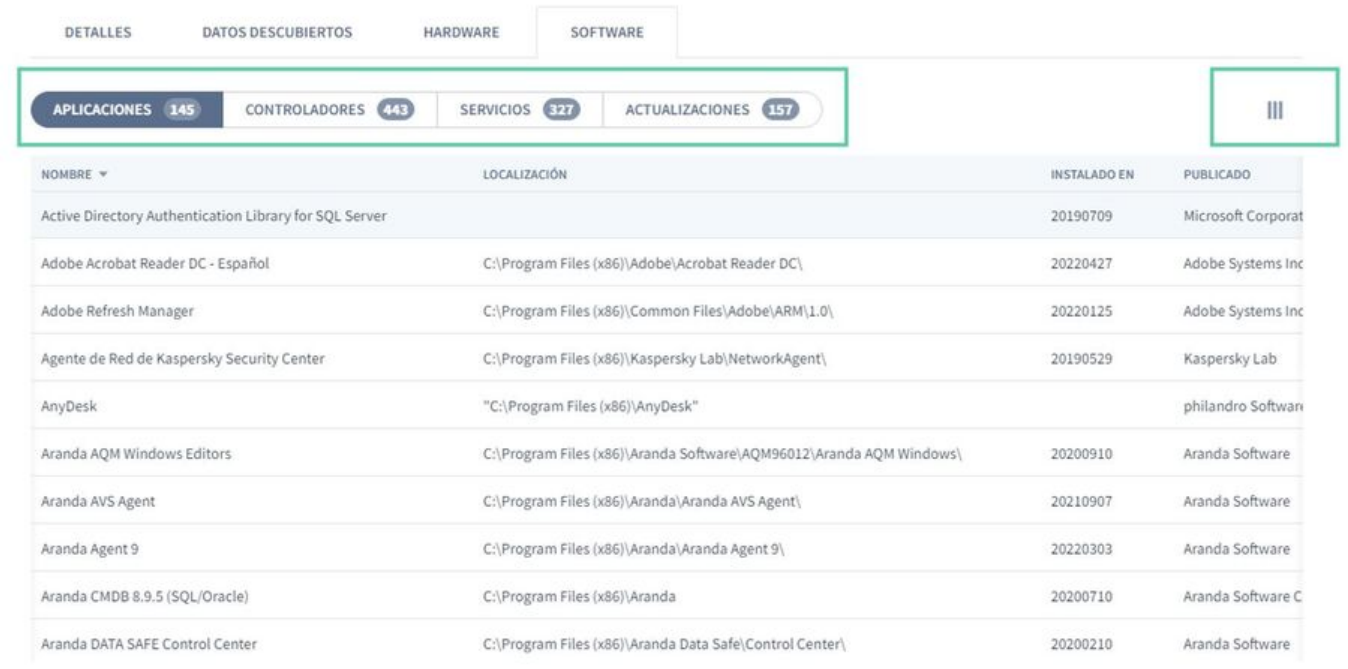
Hardware

La pestaña Hardware proporciona información sobre el dispositivo y sus componentes, incluido el tipo de placa base y procesador, y la cantidad de memoria.



Software

La pestaña de software contiene una lista de las aplicaciones de software, controladores, servicios y actualizaciones que están instalados en el dispositivo.



De forma predeterminada, la lista muestra las **aplicaciones**. Puede hacer clic en los botones sobre la lista para configurarla para que muestre **Controladores, Servicios o Actualizaciones**.

Puede usar la función de **búsqueda** para configurar la lista de software para que solo muestre información sobre aplicaciones, controladores, servicios o actualizaciones que tengan un nombre en particular (o parte de un nombre).

También puede optar por ocultar columnas en la lista de software. Por ejemplo, es posible que no le interese la **fecha de instalación** o el **publicador** en la vista Aplicaciones, por lo que puede ocultar esas columnas.

Para mostrar / ocultar columnas, haga clic en el ícono Columnas y luego elija qué columnas incluir o excluir.

Activando sus Dispositivos

Aranda Datasafe solo respaldará y protegerá los dispositivos que hayan sido activados. Los datos de cualquier dispositivo que no esté activado están potencialmente en riesgo.

Cuando activa un dispositivo, crea una solicitud para que ese dispositivo sea protegido y respaldado. Si la solicitud de activación tiene éxito, el dispositivo estará protegido cuando se programe la siguiente copia de seguridad (como se define en la configuración de la Política).

Prerrequisitos

En este artículo, explicamos cómo activar sus dispositivos. Antes de poder activar un dispositivo, debe tener lo siguiente en su lugar:

- Una política que define qué datos se respaldarán, con qué frecuencia se respaldarán y qué configuraciones de protección se utilizarán consulte Políticas.
- Una repositorio que define el área de almacenamiento que se utilizará para almacenar los datos de respaldo del dispositivo. Para obtener más información sobre los repositorio, consulte repositorios.
- Un equipo. La política y el repositorio deben asignarse al equipo. El dispositivo que vas a activar también debe estar asignado al Equipo. Para obtener más información, consulte Equipos.

Cuando estas configuraciones están en su lugar, puede activar sus dispositivos **"en riesgo"**.

Activar un dispositivo

Para activar un dispositivo "en riesgo":

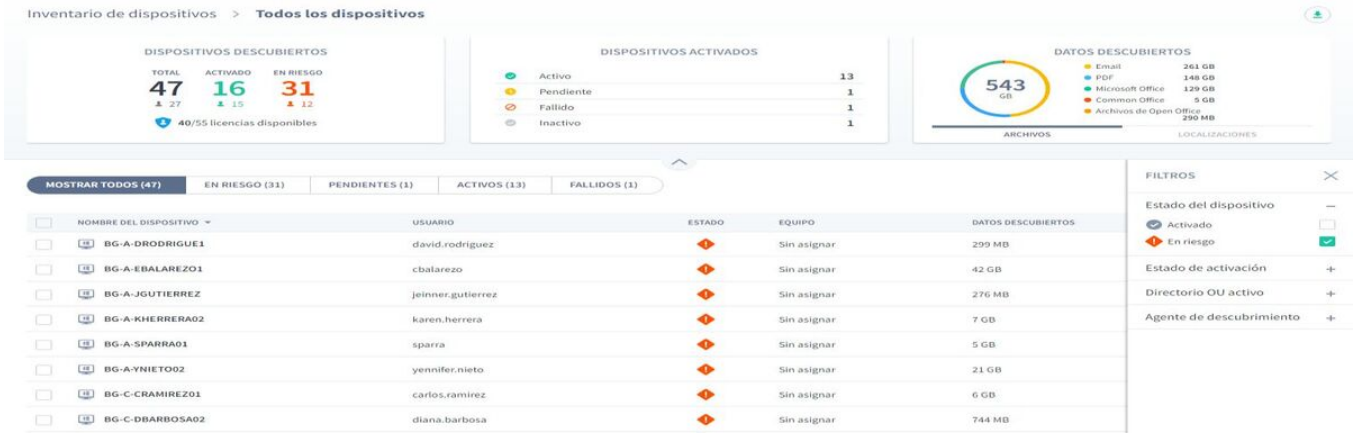
1. Haga clic en **Inventario**.

2. Haga clic en el ícono de filtro que se encuentra sobre la lista de dispositivos.

3. Elija **Estado del dispositivo** y seleccione **En riesgo**.

4. Haga clic en **Aplicar**.

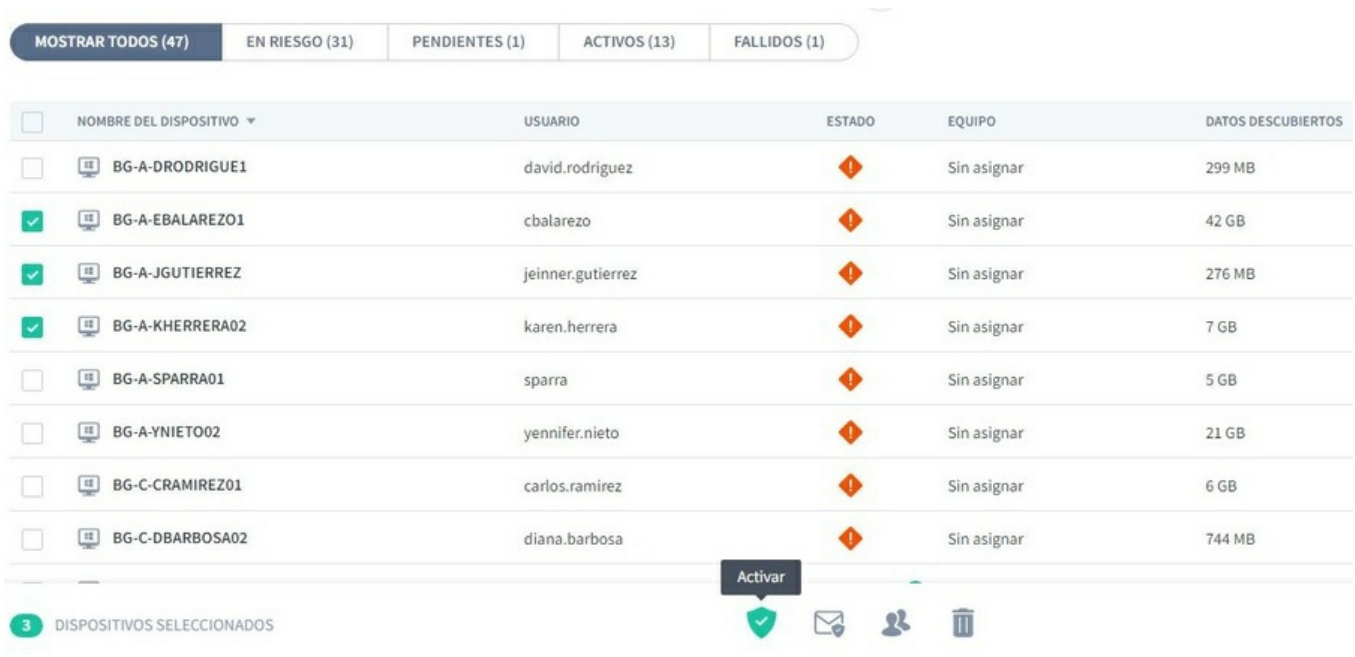
La lista de dispositivos ahora está filtrada para que solo muestre aquellos dispositivos que están "en riesgo".



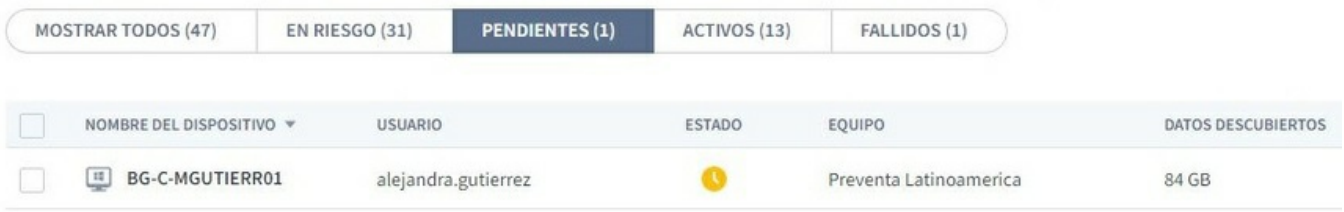
5. Hay varias formas de activar dispositivos.

Para activar un solo dispositivo, puede hacer clic en su botón de opción y luego hacer clic en **Activar**. O puede seleccionar su casilla de verificación y hacer clic en el ícono **Activar** en la barra emergente en la parte inferior.

Para activar varios dispositivos, seleccione las casillas de verificación de los dispositivos que desea activar. Luego haga clic en el ícono Activar en la barra emergente en la parte inferior.



Cuando activa un dispositivo, su estado cambia de En riesgo a Pendiente. Después de un breve retraso, el estado del dispositivo cambia a Activo y se muestra un ícono de verificación verde.



Si el dispositivo no se puede activar, se muestra un ícono de error rojo. Deberá investigar por qué ha fallado la activación. Puede deberse a que el usuario no inició sesión en el dispositivo o hubo un problema de conexión.

6. Para saber qué dispositivos están protegidos por Aranda Datasafe, haga clic en Protección.La página de Protección muestra detalles de los dispositivos que actualmente tienen datos cifrados y respaldados por Aranda Datasafe.

Filtrado Página de Inventario

De forma predeterminada, la página Inventario muestra información para todos los equipos y dispositivos. Pero, si es necesario, puede filtrar la página Inventario para que solo muestre información que cumpla con ciertos criterios. Por ejemplo, puede filtrar la página Inventario para que solo muestre información de los dispositivos de un equipo en particular.

Hay varias formas de filtrar la página de Inventario (o partes de la página de Inventario):

Filtrar por equipo

Utilice una búsqueda para filtrar la lista de dispositivos

Filtrar la lista de dispositivos por criterios seleccionados

Mostrar u ocultar columnas en la lista de dispositivos.

Filtrar por Equipo

Puede usar la barra lateral de Equipos para filtrar la página de Inventario de modo que solo muestre información sobre los dispositivos en ciertos Equipos. Por ejemplo, puede configurar la página Inventario para que solo muestre información para un equipo de "Finanzas" y un equipo de "RRHH".

Nota

Si usa la barra lateral de Equipos para filtrar la página de Inventario, se filtran todos los paneles de información y la lista de dispositivos.

1. Haga clic en **Inventario**.

2. En la sección **Equipos**, haga clic en:

- **Todos los dispositivos** para mostrar información sobre todos los dispositivos en todos los equipos (esto es el equivalente a eliminar el filtro de equipo)
- **Sin asignar** para mostrar información solo para aquellos dispositivos que aún no están asignados a un equipo
- **** para mostrar información sobre los dispositivos de un equipo específico.

Cuando selecciona un Equipo o Equipos, la página de**Inventario** se actualiza y se filtran las pantallas de información y la lista de dispositivos. Solo muestran información sobre los dispositivos de los equipos seleccionados.

Haga clic en **Todos los dispositivos** en la barra lateral de**Equipos** para eliminar el filtro.

Utilice una búsqueda para filtrar la lista de dispositivos

Puede usar la función de búsqueda para filtrar la lista de dispositivos de modo que solo incluya dispositivos que tengan ciertos valores. Por ejemplo, puede usar la búsqueda para filtrar la lista de modo que solo muestre dispositivos con un nombre en particular (o prefijo a un nombre). Esto es útil si tiene un esquema de nomenclatura de dispositivos consistente y solo desea ver dispositivos en particular. Por ejemplo, puede tener dispositivos que comienzan con nombres que comienzan con ERL, por lo que puede buscar ERL.

Puede utilizar la búsqueda para filtrar la lista de dispositivos por cualquier valor de texto, incluido el nombre del dispositivo, el nombre de usuario y el nombre del equipo.

Para aplicar un filtro de búsqueda:

1. Haga clic en el ícono de búsqueda que se encuentra sobre la lista de dispositivos.

2. Ingrese los primeros caracteres del valor de texto que desea usar como filtro. Aranda Datasafe aplica el filtro a medida que escribe, por lo que puede hacer coincidencias parciales O puede ingresar el valor de texto completo para ser más específico.

Filtrar la lista de dispositivos por criterios seleccionados

Puede filtrar la lista de dispositivos para que solo muestre los dispositivos que coincidan con los criterios elegidos.

Para filtrar la lista de dispositivos:

1. Haga clic en el ícono de filtro

para mostrar las opciones de Filtros deslizantes.

2. Expanda Categorías de **filtros** y seleccione los criterios de filtros que desea aplicar. La lista de dispositivos solo mostrará los dispositivos que coincidan con todos los criterios que seleccione.

3. Haga clic en **Aplicar**.

Puede elegir cualquiera de estas opciones de filtro:

Filtro	Descripción	Opciones
Estado Dispositivo	Filtrar dispositivos según su estado de activación.	Activado (seleccionado para activación) En riesgo (aún no seleccionado para activación)
Estado Activación	Filtre la lista para que solo muestre dispositivos con un estado de activación particular.	Pendiente El proceso de activación está programado para comenzar. - Activo. El dispositivo se ha activado con éxito Fallido - El proceso de activación no tuvo éxito.
Active Directory OU	Filtrar por una unidad organizacional de Active Directory de dispositivos. Estos datos de OU provienen del agente de descubrimiento en el dispositivo del usuario.	Lista de unidades organizativas disponibles
Agente de Descubrimiento	Filtre la lista para que solo muestre los dispositivos que utilizan una versión particular del software Discovery Agent.	Lista de agentes de descubrimiento disponibles

Para eliminar los filtros, haga clic en el ícono de Filtro y haga clic en**Restablecer** (o desmarque cada una de las casillas de filtro).

Mostrar u ocultar columnas en la lista de dispositivos

Puede optar por mostrar u ocultar columnas en la lista de dispositivos. Por ejemplo, es posible que no le interese qué versión de Discovery Agent se utilizó para descubrir un dispositivo, por lo que puede ocultarlo de la vista.

Para mostrar / ocultar columnas, haga clic en el ícono Columnas y luego elija qué columnas incluir. Para obtener una descripción de cada columna, consulte la[Página de inventario](#).

Protección

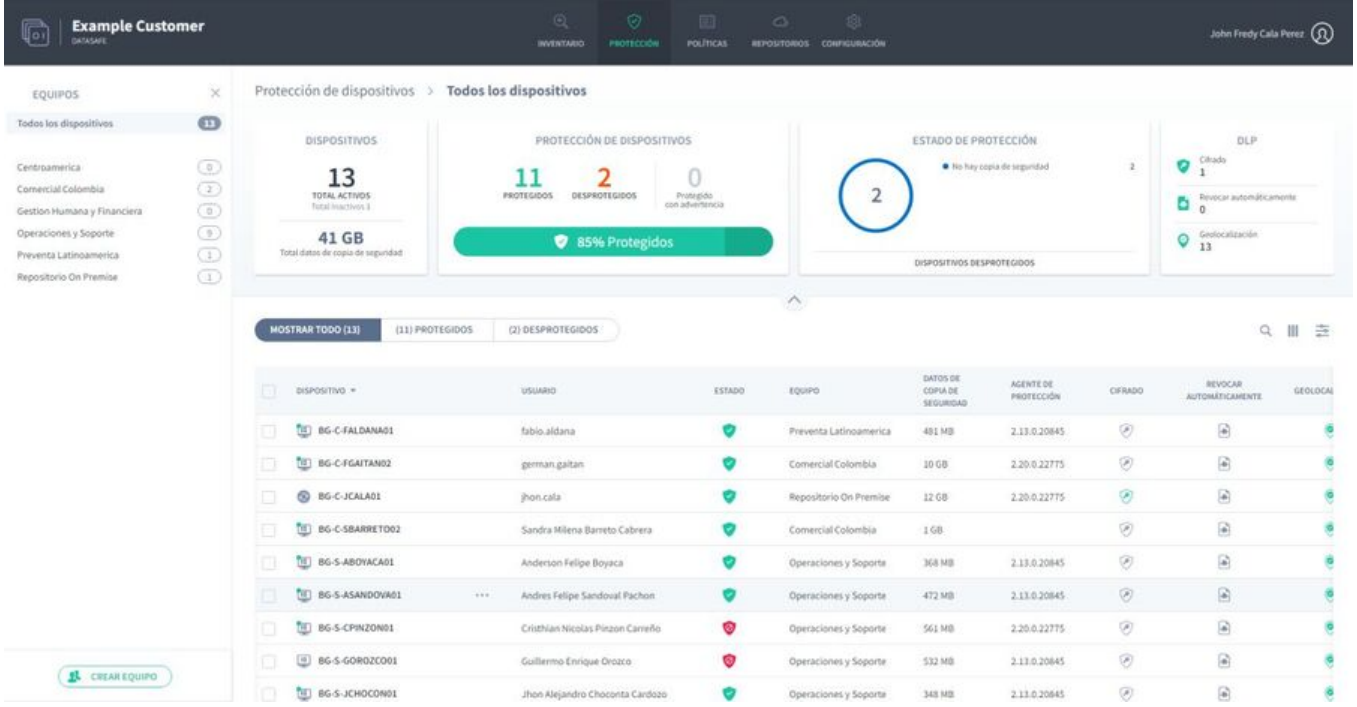
Protección

Aranda Datasafe protege los datos de su empresa al realizar automáticamente copias de seguridad cifradas de los datos de su empresa. También tiene funciones de prevención de pérdida de datos (DLP) que puede activar o desactivar, según sus requisitos.

Puede utilizar la página Protección para ver el estado de protección de todos sus dispositivos activados. Tenga en cuenta que la[página Protección](#) no muestra datos para dispositivos que aún no se han activado.

Protección dispositivo

La página**Protección** proporciona información sobre los dispositivos activados y su estado de protección actual. Puede usarlo para averiguar qué dispositivos están actualmente protegidos, desprotegidos o protegidos con advertencia.



Estado de Protección	Descripción
Protegido	El dispositivo ha sido activado, tiene el software Protection Agent instalado y sus datos están respaldados por Aranda Datasafe.
Sin protección	El dispositivo se ha activado, tiene el software Protection Agent instalado, pero no se ha realizado una copia de seguridad con éxito en los últimos 5 días. (5 días es el rango de protección predeterminado) Hasta que se realice una copia de seguridad exitosa, los datos de un dispositivo desprotegido están en riesgo. La primera copia de seguridad del dispositivo generalmente ocurre alrededor de 10 minutos después de que se activa el dispositivo. Pero puede llevar más tiempo, según el tiempo que tarde el software Protection Agent en indexar los archivos.
Protegido con Advertencia	El dispositivo se ha activado y tiene instalado el software Protection Agent. El dispositivo realizó una copia de seguridad exitosa en los últimos 5 días, pero Advertencia falló el último intento de copia de seguridad.

La página Protección solo muestra los dispositivos que se detectan y activan correctamente. Si la página de Protección está vacía, sus dispositivos no han sido descubiertos o han sido descubiertos, pero no activados.

> ⚐ **Nota:** En la página Inventario , usamos el término "En riesgo" para describir un dispositivo que se ha descubierto, pero no se ha activado. Los dispositivos "Desprotegidos" en la página de Protección se han activado, pero no se ha realizado una copia de seguridad en el rango de protección. Tanto los dispositivos "en riesgo" como los "desprotegidos" contienen datos que son vulnerables.

Dispositivos

El panel Dispositivos proporciona un resumen de:

- Número de dispositivos activos e inactivos
- Cantidad de datos de respaldo en todos los dispositivos.

Los datos de respaldo muestran la suma de todos los datos incluidos en la Política en todos los dispositivos en un momento específico. Este número no es la información almacenada en el repositorio.

Un dispositivo activo es un dispositivo que se ha activado y se ha conectado a Aranda Datasafe en los últimos 30 días.

Campo	Descripcion
Total Activos	La cantidad total de dispositivos que están activos. Estos dispositivos se han activado y están**protegidos, protegidos con advertencia o desprotegidos** (consulte Protección de dispositivos). Los dispositivos activos no están necesariamente protegidos ni respaldados.
Total Inactivos	La cantidad total de dispositivos que se han activado pero que no se han conectado a Aranda Datasafe en los últimos 30 días (y, por lo tanto, no están respaldados por ese período de tiempo).
Total Data Respaldada	La cantidad de datos en todos los dispositivos que se incluyen en las políticas de respaldo en un momento específico. Puede usar esto como una indicación de cuánto espacio de almacenamiento se necesita. Pero tenga en cuenta que la cifra de datos de respaldo cambiará cada vez que cambie la Política o cuando los usuarios agreguen / eliminen datos de respaldo en sus dispositivos.

Protección del dispositivo

El panel Protección de dispositivos proporciona información sobre la cantidad de dispositivos que se han respaldado y protegido en los últimos 5 días. Muestra:

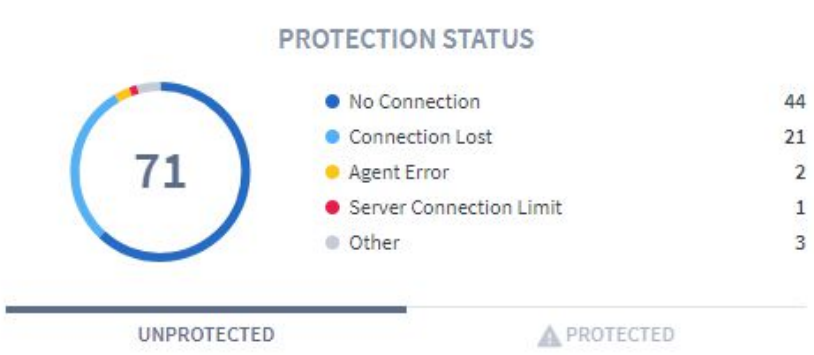
Campo	Descripción
Protegido	La cantidad total de dispositivos de los que se ha realizado una copia de seguridad con éxito en los últimos 5 días.
Sin Protección	La cantidad total de dispositivos que no se han respaldado correctamente en los últimos 5 días.
Protegido con Advertencia	La cantidad total de dispositivos de los que se ha realizado una copia de seguridad con éxito en los últimos 5 días, pero que falló la copia de seguridad más reciente.

Estatus de Protección

El panel Estado de protección proporciona un resumen de la cantidad de dispositivos que están actualmente protegidos, protegidos con advertencias o desprotegidos.

Si algunos de sus dispositivos tienen el estado desprotegido o desprotegido con advertencia, el panel Estado de protección tiene dos pestañas**Desprotegido** y **Protegido** con advertencia (que se muestra en la parte inferior del panel).

La pestaña **Desprotegido** muestra:



Campo	Descripción
Sin Respaldo	La cantidad de dispositivos que están desprotegidos y no tienen datos de respaldo en Aranda Datasafe.
Sin Conexión	La cantidad de dispositivos que están desprotegidos y no tienen conexión a Aranda Datasafe.
Conexión Perdida	La cantidad de dispositivos que están desprotegidos y han perdido su conexión a Aranda Datasafe
Error de Agente	La cantidad de dispositivos que tienen un error de agente que el servidor no puede reconocer. Si tiene mensajes de error del agente, comuníquese con nuestro equipo de soporte técnico para obtener ayuda.
Limite de Conexión al Servidor	La cantidad de dispositivos que intentan conectarse a Aranda Datasafe cuando ya se alcanzó el límite de conexión del servidor. Aranda Datasafe permite una cierta cantidad de conexiones simultáneas (60 por defecto) y una vez que se alcanza este límite, no se pueden realizar conexiones adicionales. Los dispositivos volverán a intentarlo en unos minutos para comprobar si hay una conexión disponible y realizar una copia de seguridad.
Otro	El número de errores que no están categorizados. Si tiene otros errores, comuníquese con nuestro equipo de soporte técnico para obtener ayuda. (reportedecasos@arandasoft.com)

La pestaña **Protegido con advertencia** muestra la cantidad de dispositivos que están protegidos con una advertencia. Si hay advertencias, se proporcionan estadísticas de las advertencias (como se muestra a continuación):

Campo	Descripción
Error de Agente	La cantidad de dispositivos que están protegidos, pero tienen un error de agente que el servidor no puede reconocer. Si tiene mensajes de error del agente, comuníquese con nuestro equipo de soporte técnico para obtener ayuda.
Archivos Bloqueados	La cantidad de dispositivos que están protegidos, pero tienen archivos bloqueados (archivos que estaban abiertos en el dispositivo cuando se realizó la copia de seguridad). Aranda Datasafe puede realizar copias de seguridad de archivos bloqueados, pero el éxito de la copia de seguridad depende de que el servicio VSS de Windows funcione correctamente. Si tiene advertencias de archivo bloqueadas, le recomendamos que filtre la Lista de dispositivos en la página Protegido para mostrar solo los dispositivos con el estado "protegido con advertencia". Luego, muestre el registro de respaldo del dispositivo para determinar qué archivos estaban bloqueados. A continuación, puede decidir si desea cerrar los archivos de los dispositivos y hacer una copia de seguridad de los dispositivos manualmente o dejarlos hasta la próxima copia de seguridad programada.

DLP

El panel DLP muestra un resumen de la cantidad de dispositivos que utilizan las funciones de Prevención de pérdida de datos (cifrado, revocación automática y geolocalización). Las funciones de DLP están habilitadas y deshabilitadas en la configuración de la política.

Barra lateral de equipos

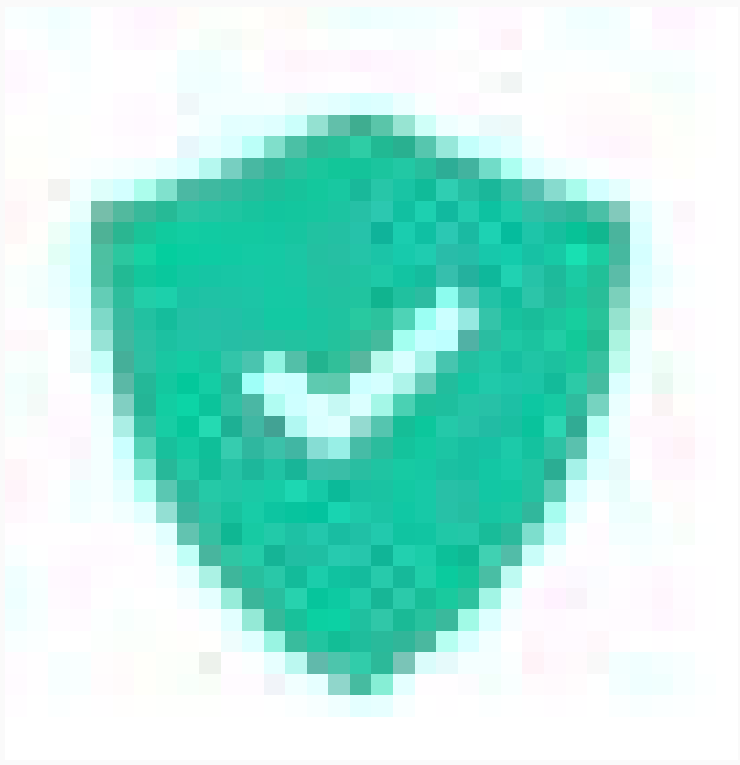
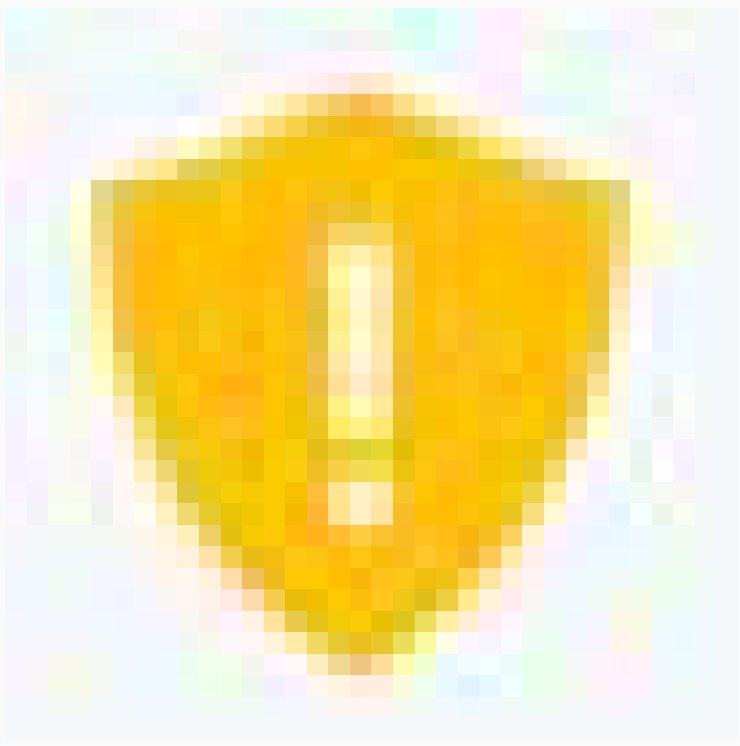
En el lado izquierdo de la página de Protección está la barra lateral de Equipos. Esto muestra una lista de los equipos que están configurados en su Aranda Datasafe (más Todos los dispositivos y Sin asignar, que están integrados).

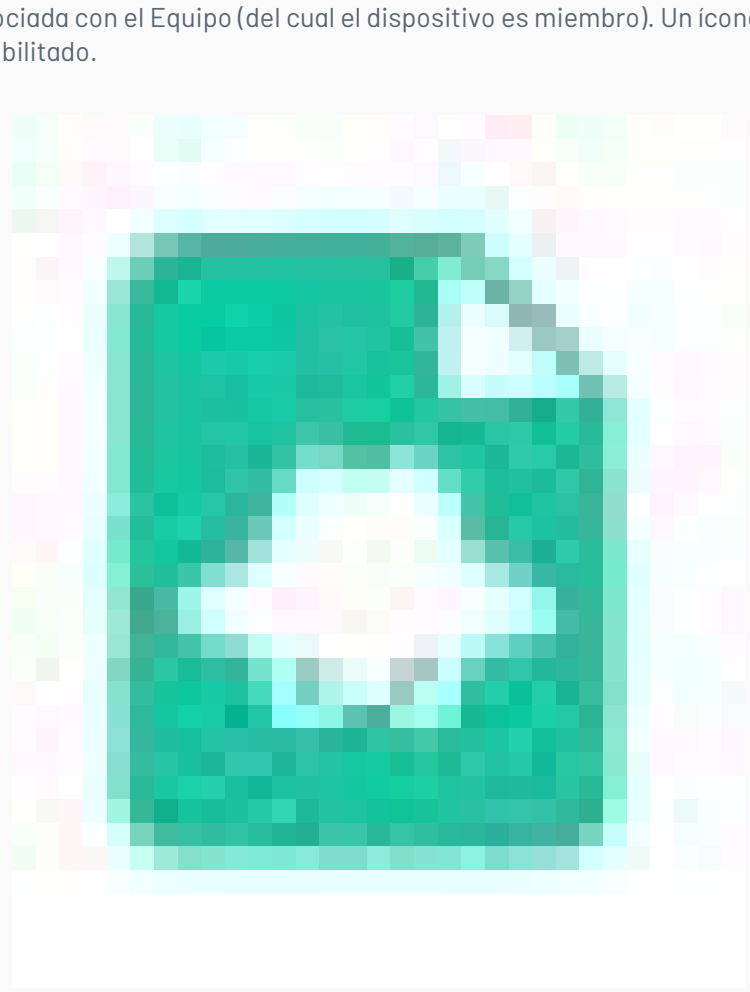
Si hace clic en un equipo, los paneles de protección y la lista de dispositivos se actualizan para que solo muestre información de los dispositivos del equipo seleccionado. Puede hacer clic **en Todos los dispositivos** para configurar el Inventario para que muestre los datos de cada dispositivo.

Los usuarios administradores pueden utilizar un método abreviado de teclado para seleccionar equipos sobre los que informar. Presione la tecla CTRL y luego seleccione los equipos que desea incluir.

Lista de protección de dispositivos

La sección inferior de Protección muestra la lista de protección de dispositivos, que contiene un resumen de los dispositivos que Aranda Datasafe ha descubierto y su estado de protección.

Campo	Descripción
Dispositivo	El nombre del dispositivo.
Usuario	El nombre del usuario asociado con el dispositivo.
Estado	Muestra el estado de la protección: Protegido  Protegido con Advertencia  Sin Protección 

Campo	Descripción
Equipo	El equipo al que está asignado el dispositivo.
Data Respaldada	Aranda Datasafe realiza una copia de seguridad de una cantidad de datos en el dispositivo (de acuerdo con una Política). La cantidad se muestra en la columna Datos de respaldo.
Agente de protección	La versión del software Protection Agent que está instalada actualmente en el dispositivo.
Cifrado	Muestra si la función de cifrado local está habilitada para el dispositivo. Puede habilitar y deshabilitar el cifrado local en la Política que está asociada con el Equipo (del cual el dispositivo es miembro). Un ícono verde significa que está habilitado, un ícono gris significa que está deshabilitado. 
Revocación Automática	<p>Muestra si la función de revocación automática está habilitada para el dispositivo. Puede habilitar y deshabilitar la revocación automática en la Política que está asociada con el Equipo (del cual el dispositivo es miembro). Un ícono verde significa que está habilitado, un ícono gris significa que está deshabilitado.
	Muestra si la función de geolocalización está habilitada para el dispositivo. Puede habilitar y deshabilitar la geolocalización en la Política que está asociada con el Equipo (del cual el dispositivo es miembro). Un ícono verde significa que está habilitado, un ícono gris significa que está deshabilitado.

Campo	Descripción
Geolocalizar	
Estado DLP	Muestra el estado de prevención de pérdida de datos. Esto puede ser: **Confiable**: El dispositivo ha sido autenticado y puede conectarse a Aranda Datasafe. **Revocado**: El dispositivo ha sido revocado, por lo que los usuarios no autorizados no pueden acceder a los datos cifrados en el dispositivo. No es de confianza y no se realizarán más copias de seguridad o restauraciones. **Borrado**: El dispositivo ha sido borrado. No es de confianza y no se realizarán más copias de seguridad o restauraciones.

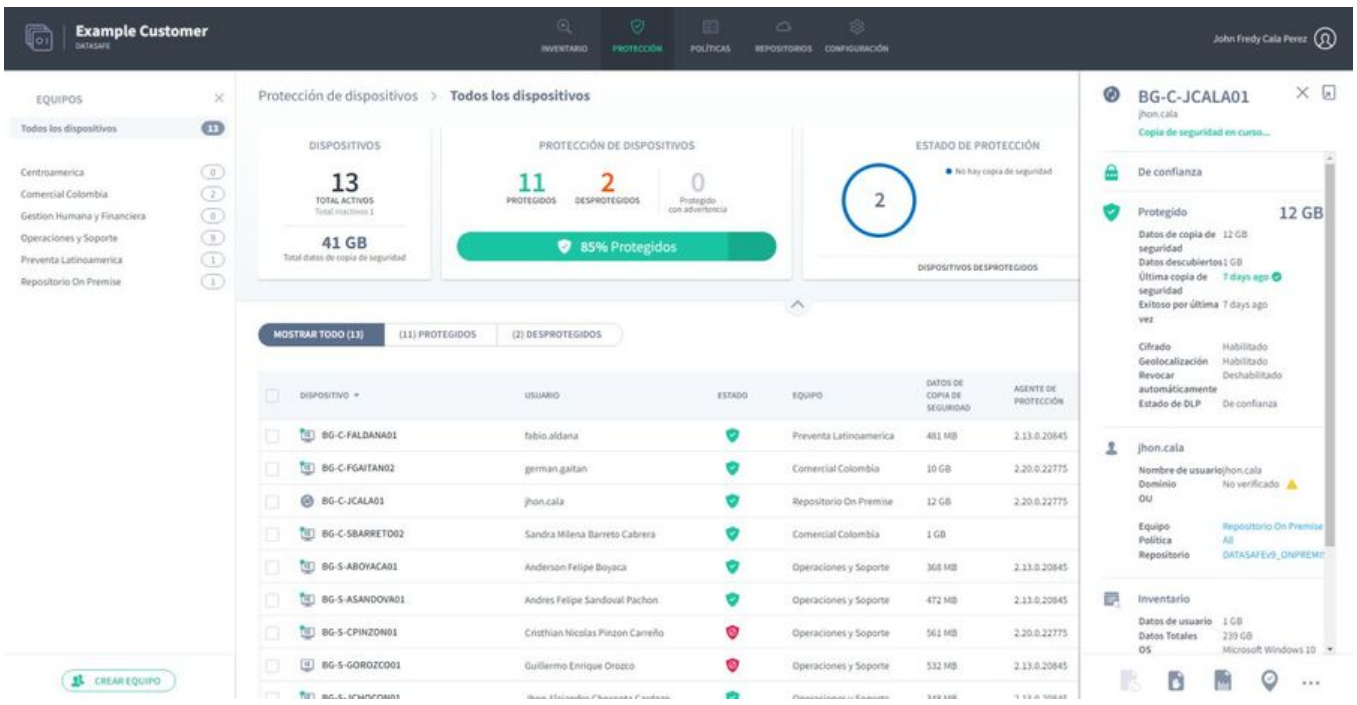
De forma predeterminada, la lista de dispositivos muestra información para todos los dispositivos (filtro **Mostrar todos**). Si lo prefiere, puede hacer clic en una de las otras opciones de filtro. Hay otras tres opciones de filtro posibles, una para cada estado: **protegido, protegido con advertencia, desprotegido**. Las opciones de filtro solo están disponibles si hay dispositivos en ese estado en particular.

Si resalta un dispositivo en la lista, aparece un botón de opción (...) a la derecha del nombre del dispositivo. Haga clic en el botón de opción para mostrar un menú contextual con estas opciones:

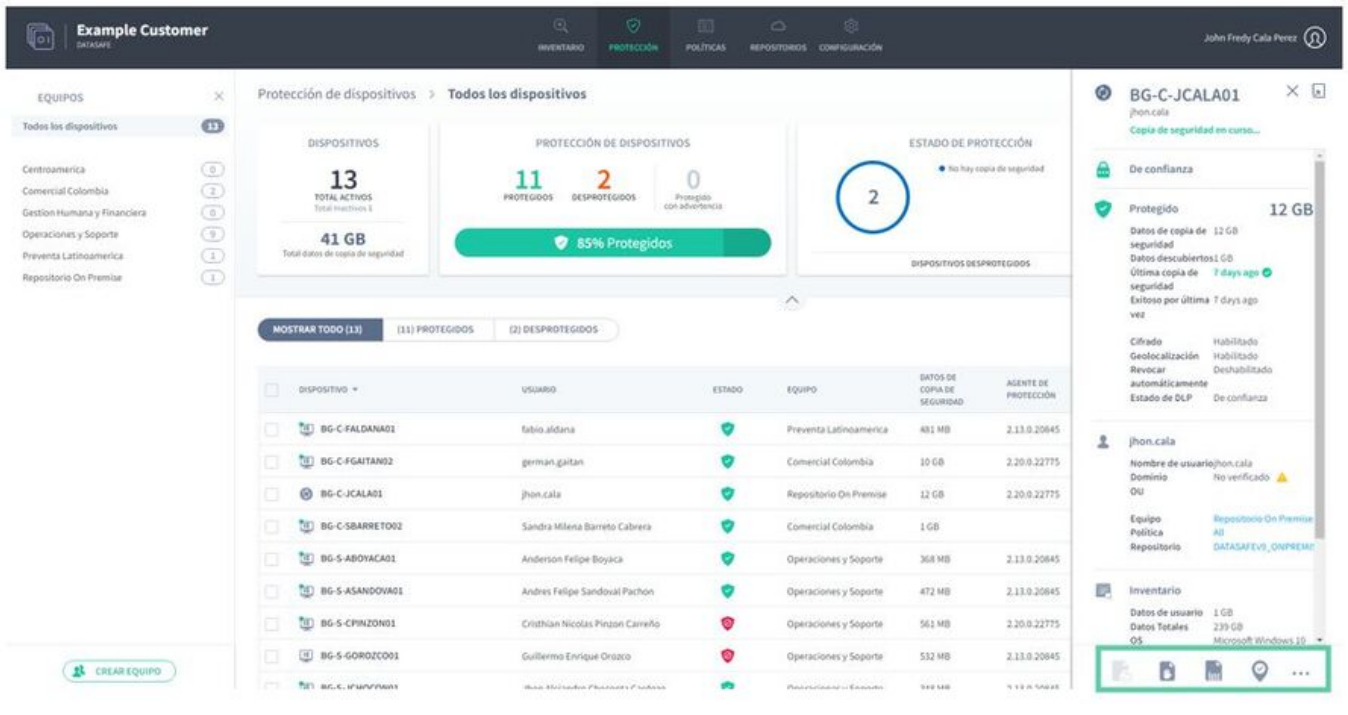
Campo	Descripción
Ver	Muestra la página Dispositivo, que contiene detalles sobre el dispositivo, incluido su hardware y software.
Asignar Equipo	Úselo para asignar el dispositivo a un equipo. Aranda Datasafe solo puede respaldar y proteger los dispositivos que están asignados a los equipos, ya que los equipos deben estar asociados con un repositorio y una política.
Eliminar	Úselo para eliminar un dispositivo. Si elimina el último dispositivo restante de un usuario, se liberará una licencia y estará disponible para que la usen otros usuarios.

Barra lateral del dispositivo

Si hace clic en un dispositivo de la lista de dispositivos, aparece la barra lateral del dispositivo. Muestra información adicional sobre el dispositivo seleccionado. Si hace clic en el ícono Ver en la esquina superior, Aranda Datasafe muestra la página del Dispositivo, que contiene una vista más detallada del dispositivo, incluido su hardware y software.



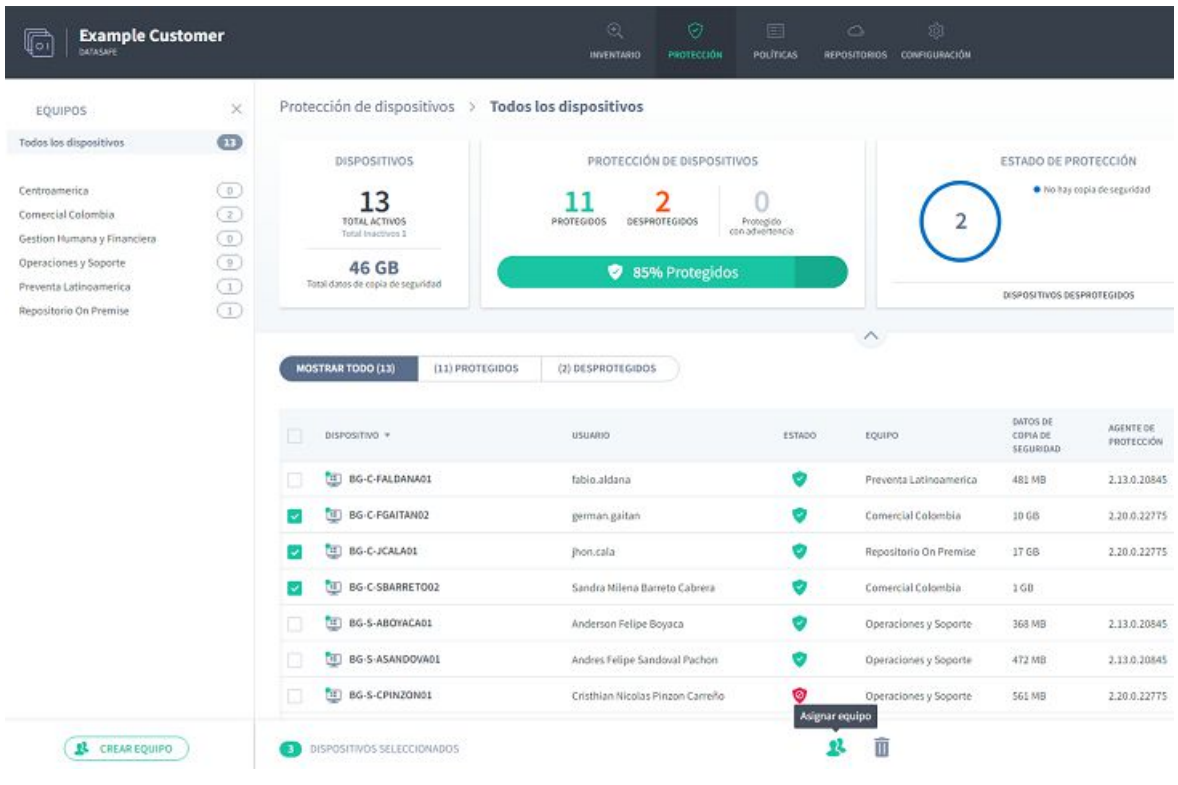
En la parte inferior de la barra lateral del dispositivo, hay íconos para realizar una copia de seguridad manual del dispositivo, revocarlo, borrarlo y utilizar la geolocalización para descubrirlo. Los mismos íconos también están disponibles en la página Dispositivo.



Acciones multidispositivo

Puede utilizar la lista de dispositivos para aplicar una sola acción a varios dispositivos. Por ejemplo, puede asignar varios dispositivos al mismo equipo.

Utilice la casilla de verificación a la izquierda de cada fila de dispositivos para seleccionar un dispositivo. Cuando selecciona las casillas de verificación, las opciones de acción aparecen al final de la lista. Estos funcionan de la misma manera que para dispositivos individuales, excepto que la acción se aplicará a todos los dispositivos que seleccionó.



Filtrado Protección

De forma predeterminada, la página Protección muestra información para todos los equipos y dispositivos. Pero, si es necesario, puede filtrar la página Protección para que solo muestre información que cumpla con ciertos criterios. Por ejemplo, puede filtrar la página Protección para que solo muestre información de los dispositivos de un equipo en particular.

Hay varias formas de filtrar la página Protección (o partes de la página Protección):

Filtrar por equipo

Utilice una búsqueda para filtrar la lista de dispositivos

Filtrar la lista de dispositivos por criterios seleccionados

Mostrar u ocultar columnas en la lista de dispositivos

Filtrar por Equipo

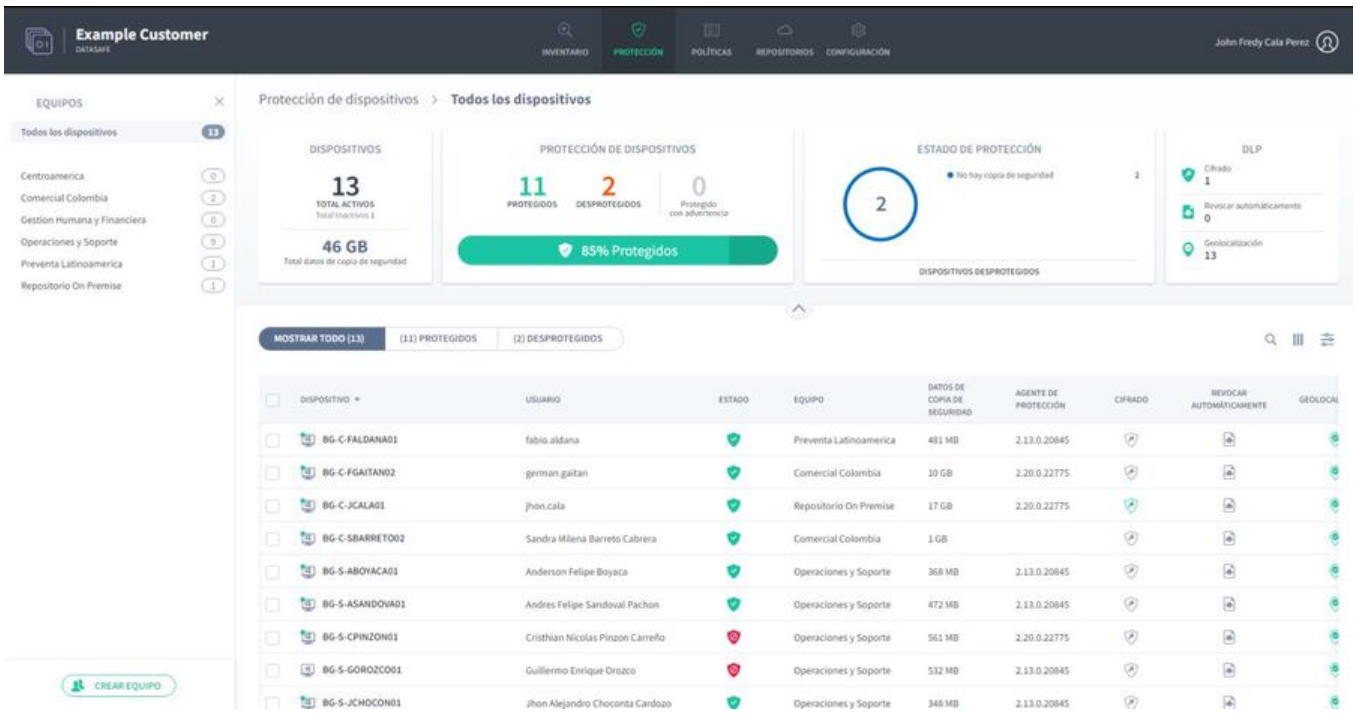
Puede usar la barra lateral de **Equipos** para filtrar la página de **Protección** de modo que solo muestre información sobre los dispositivos en ciertos **Equipos**. Por ejemplo, puede configurar la página Protección para que solo muestre información para un equipo de "Finanzas" y un equipo de "Recursos humanos".

1. Haga clic en **Protección**.

2. En la sección **Equipos**, haga clic en:

- **Todos los dispositivos** para mostrar información sobre todos los dispositivos en todos los equipos (esto es el equivalente a eliminar el filtro de equipo)

- **Sin asignar** para mostrar información solo para aquellos dispositivos que aún no están asignados a un equipo
- **** para mostrar información sobre los dispositivos de un equipo específico.



Cuando selecciona un equipo o equipos, la página**Protección** se actualiza y se filtran las pantallas de información y la lista de dispositivos. Solo muestran información sobre los dispositivos de los equipos seleccionados.

Haga clic en **Todos los dispositivos** en la barra lateral de **Equipos** para eliminar el filtro.

Utilice una búsqueda para filtrar la lista de dispositivos

Puede usar la función de **búsqueda** para filtrar la lista de dispositivos de modo que solo incluya dispositivos que tengan ciertos valores. Por ejemplo, puede usar la búsqueda para filtrar la lista de modo que solo muestre dispositivos con un nombre en particular (o prefijo a un nombre). Esto es útil si tiene un esquema de nomenclatura de dispositivos consistente y solo desea ver dispositivos en particular. Por ejemplo, puede tener dispositivos que comienzan con nombres que comienzan con ERL, por lo que puede buscar ERL.

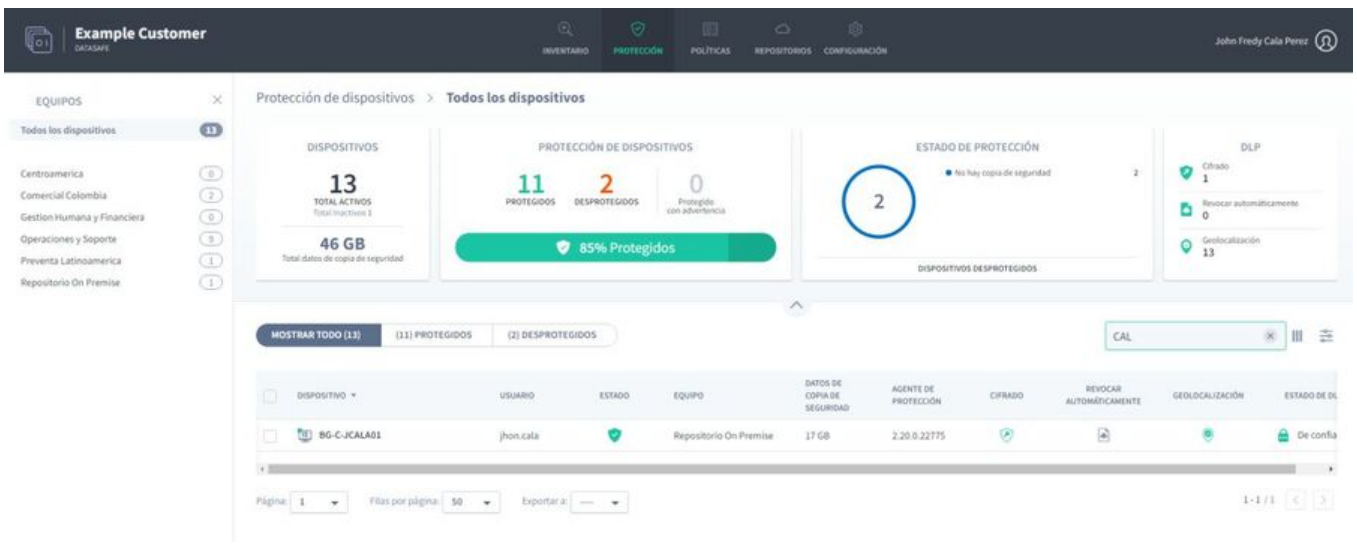
Puede utilizar la búsqueda para filtrar la lista de dispositivos por cualquier valor de texto, incluido el nombre del **dispositivo**, el nombre de **usuario** y el nombre del **equipo**.

Para aplicar un filtro de búsqueda:

1. Haga clic en el ícono de búsqueda que se encuentra sobre la lista de dispositivos.

2. Ingrese los primeros caracteres del valor de texto que desea usar como filtro. Aranda Datasafe aplica el filtro a medida que escribe, por lo que puede hacer coincidencias parciales o puede ingresar el valor de texto completo para ser más específico.

Puede buscar el nombre del dispositivo, el nombre de usuario o el nombre del equipo.



Filtrar la lista de dispositivos por criterios seleccionados

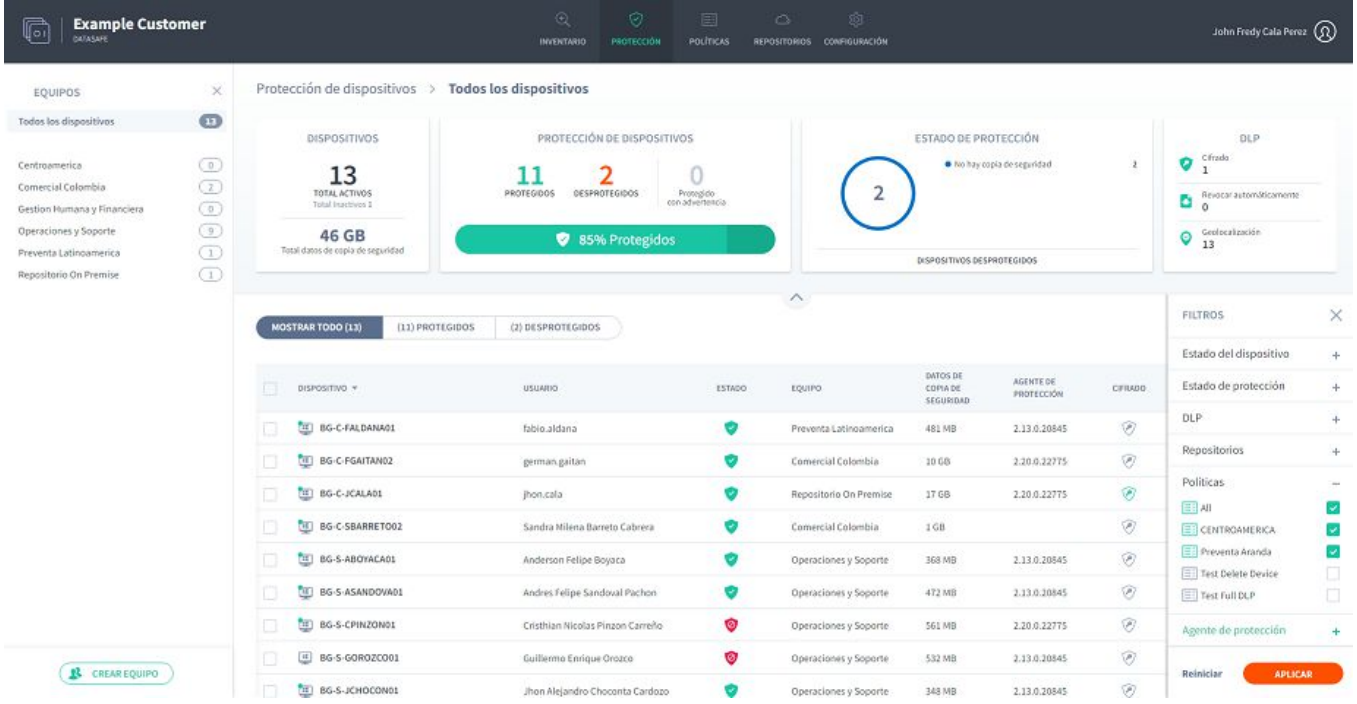
Puede filtrar la lista de dispositivos para que solo muestre los dispositivos que coincidan con los criterios elegidos.

Para filtrar la lista de dispositivos:

1. Haga clic en el ícono de filtro para mostrar las opciones de filtros deslizables.

2. Expanda Categorías de **filtros** y seleccione los criterios de filtros que desea aplicar. La lista de dispositivos solo mostrará los dispositivos que coincidan con todos los criterios que seleccione.

3. Haga clic en Aplicar.



Puede elegir cualquiera de estas opciones de filtro:

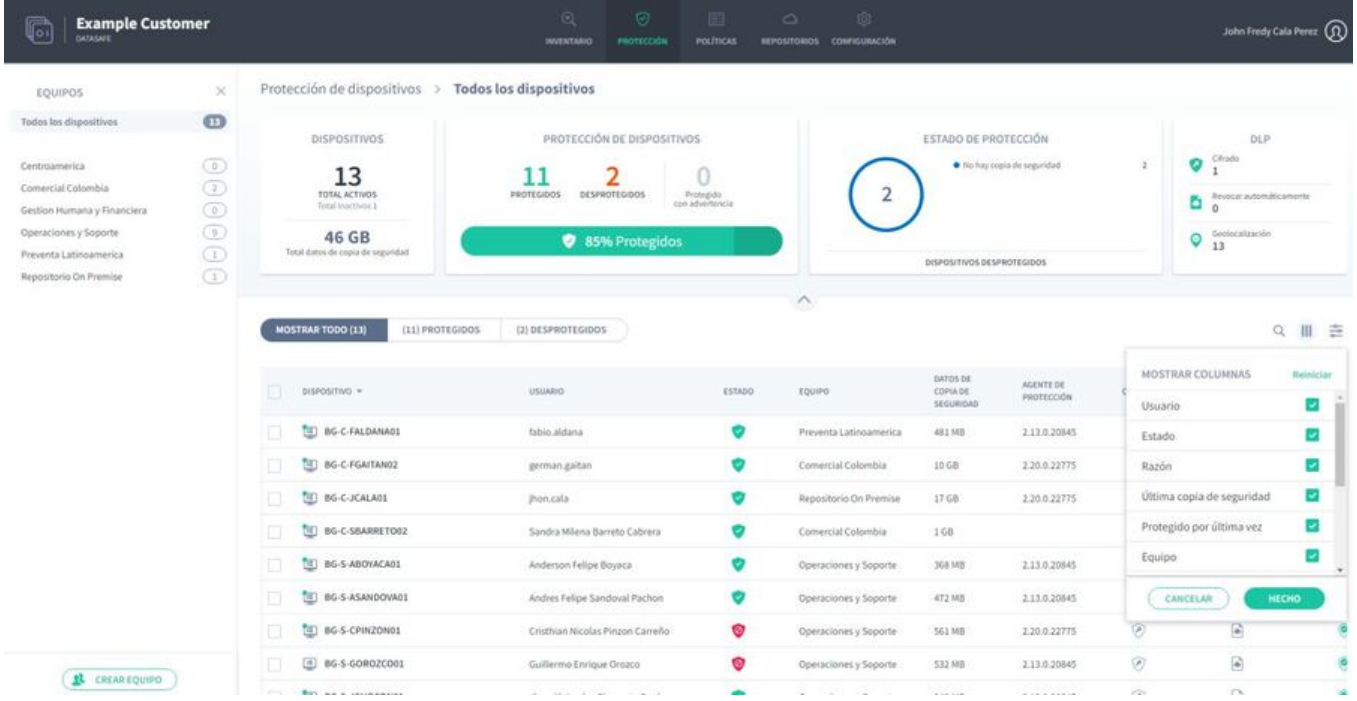
Filtro	Descripción	Opciones
Estado del Dispositivo	Filtrar dispositivos según su estado de activación.	- Activo - Inactivo
Estado Protección	Filtre la lista para que solo muestre dispositivos con un estado de protección particular.	- Protegido - Protegido con advertencia (el dispositivo se ha protegido en los últimos 5 días, pero falló la copia de seguridad más reciente) - Desprotegido. - Sin conexión (Aranda Datasafe descubrió el dispositivo, pero no se puede conectar).
DLP	Filtre los dispositivos por el estado de DLP.	- Confiable: El dispositivo ha sido autenticado - Revocado: Se ha eliminado el certificado de seguridad del dispositivo* - Borrado: Se han eliminado los datos protegidos del dispositivo. Los dispositivos generalmente se revocan o se borran cuando faltan, son robados o no se han conectado a Aranda Datasafe dentro de un período de tiempo establecido.
Repositorios	Filtre la lista para que solo muestre los dispositivos asociados con un repositorio en particular.	Lista de repositorios disponibles
Políticas	Filtre la lista para que solo muestre los dispositivos asociados con una política en particular.	Lista de políticas disponibles
Agente de Protección	Filtre la lista para que solo muestre los dispositivos que utilizan una versión particular del software Protection Agent.	Lista de versiones de Protection Agent disponibles

Para eliminar los filtros, haga clic en el ícono de Filtro y haga clic en**Restablecer** (o desmarque cada una de las casillas de filtro).

Mostrar u ocultar columnas en la lista de dispositivos

Puede optar por mostrar u ocultar columnas en la lista de dispositivos. Por ejemplo, es posible que no le interese qué versión del agente de protección se utilizó para descubrir un dispositivo, por lo que puede ocultarlo de la vista.

Para mostrar / ocultar columnas, haga clic en el ícono Columnas y luego elija qué columnas incluir. Para obtener una descripción de cada columna, consulte la Página de protección.



Políticas Descripción

Políticas Descripción General

Aranda Datasafe necesita saber qué archivos desea proteger y respaldar. Proporciona estas instrucciones configurando una Política.

Una política es un conjunto de reglas que definen:

- Datos protegidos: qué datos se seleccionan para protección y respaldo.
- Opciones de copia de seguridad y restauración: la frecuencia con la que se realizan las copias de seguridad.
- DLP: si se utiliza alguna función de prevención de pérdida de datos para proteger sus datos en caso de pérdida o robo de un dispositivo. Estos incluyen cifrado local, prevención de robo de datos y geolocalización.
- Migración: si se puede realizar una copia de seguridad de la configuración del perfil de usuario de Windows para migrar a otros dispositivos.

Puede crear tantas políticas como necesite. Puede tener una Política para todos o podría tener diferentes Políticas para cada departamento de su organización.

Para ver, crear y editar políticas, utilizará la página de políticas y la página del editor de políticas

Políticas

La página de Políticas brinda acceso a las Políticas en Aranda Datasafe. Puedes usarlo para:

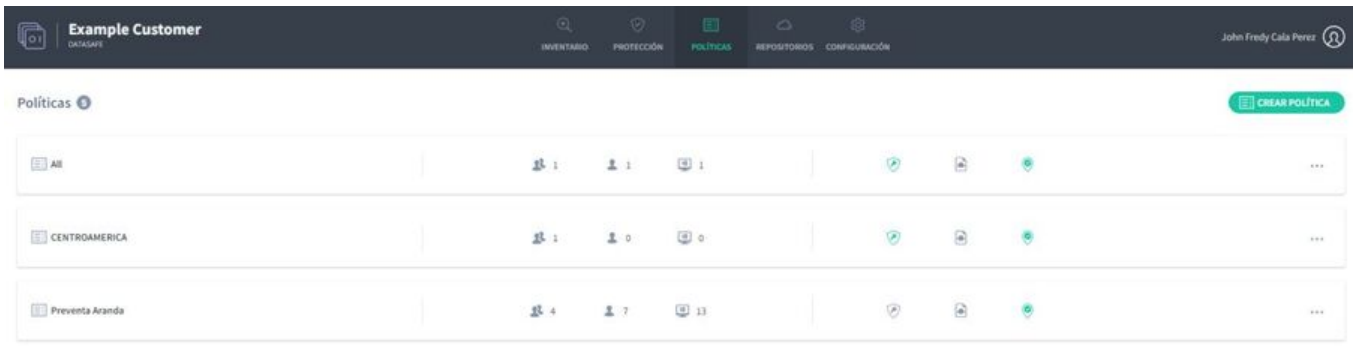
- Ver una lista de políticas
- Ver o editar una política
- Crear una política
- Eliminar una política

Haga clic en **Políticas** para mostrar la página Políticas.

Lista de Políticas

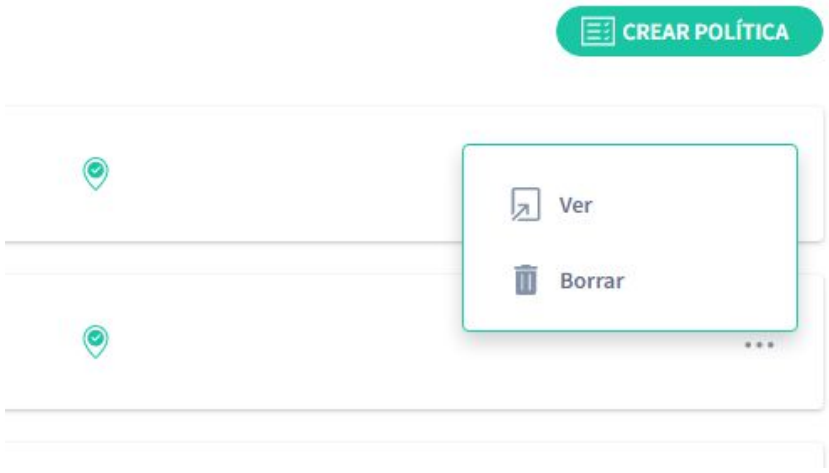
Cuando muestra la página de Políticas, le presenta una lista de las Políticas que se encuentran actualmente en Aranda Datasafe.

El nombre de la Política se muestra a la izquierda y hay una serie de íconos.



Ícono	Descripción
15	Número de equipos que utilizan la política.
15	Número de cuentas de usuario asociadas con la Política.
15	Número de dispositivos asociados con la Política.
	El estado de la función de cifrado (verde = cifrado local activado, gris = cifrado local desactivado)
	El estado de la función de revocación automática (verde = encendido, gris = apagado).
	El estado de la función de geolocalización (verde = encendido, gris = apagado).

En el lado derecho de la fila, hay un menú contextual (...). Si hace clic en él, puede elegir ver la política o eliminarla.



Ver o editar una política

Para ver o editar una política, haga clic en el nombre de la Política o use la opción Ver en el menú contextual.

Cuando ve o edita una política, sus detalles se muestran en la página del editor de políticas.

Editor Políticas

Utilice la página del editor de políticas para ver y editar varias configuraciones para una política, que incluyen:

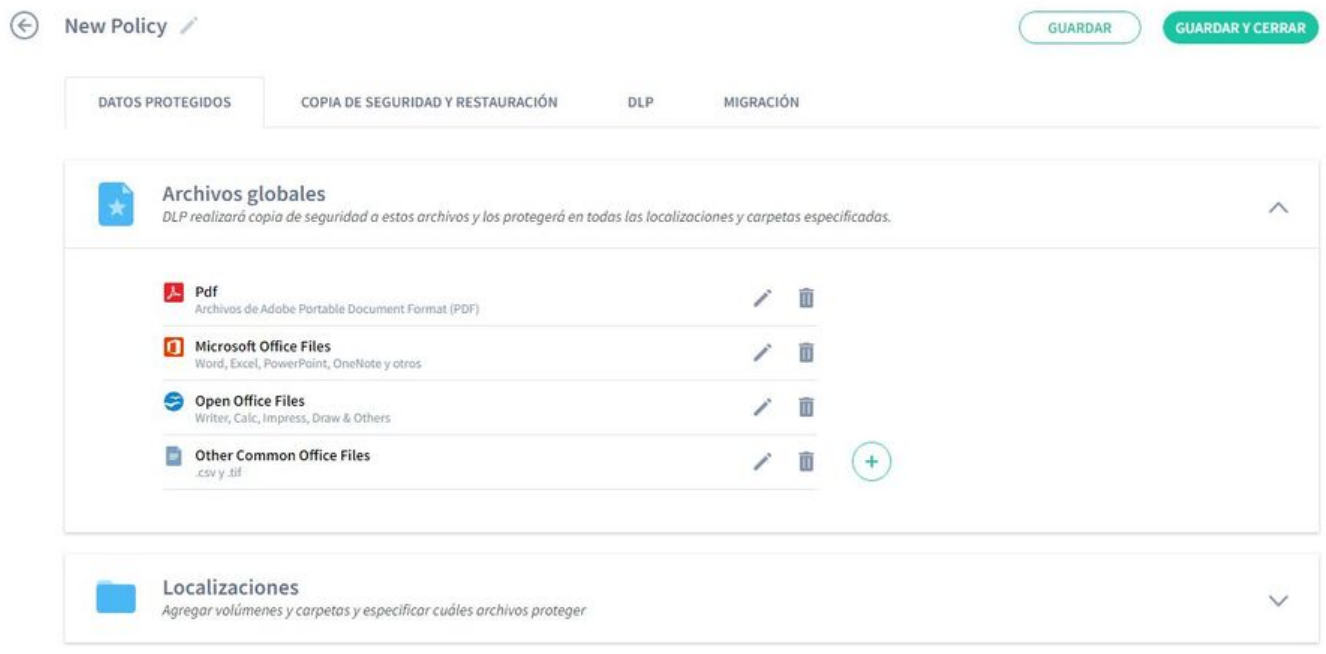
- Qué tipos de datos se respaldan y protegen
- Qué ubicaciones están protegidas y respaldadas
- Qué correo electrónico está protegido y respaldado
- Qué datos no están protegidos ni respaldados
- Cuando se realizarán las copias de seguridad automáticas
- Qué funciones de prevención de pérdida de datos se utilizan
- Qué funciones de migración de datos se utilizan.

Para mostrar la página del editor de políticas, haga clic en**Políticas**.

- Datos protegidos
- Copia de seguridad de restauración
- DLP (prevención de pérdida de datos)
- Migración.

Datos protegidos

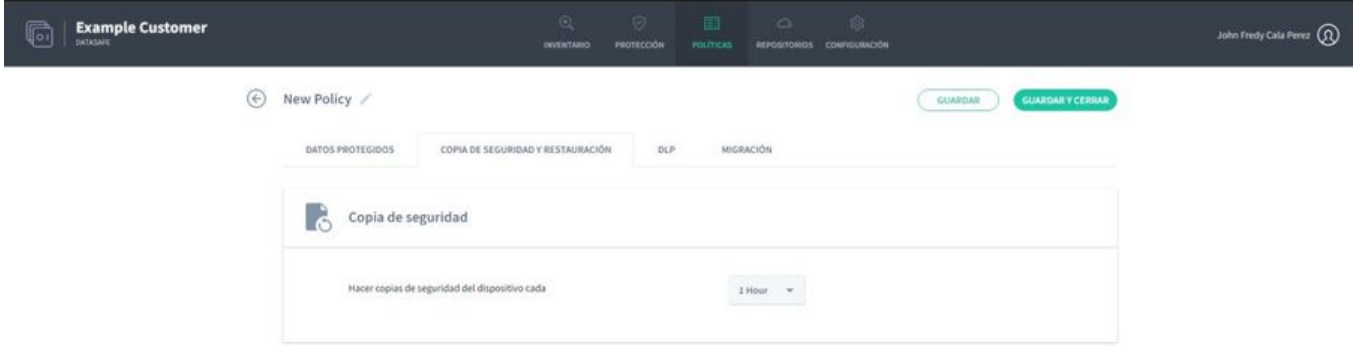
Utilice la configuración de Datos protegidos para elegir qué tipos de archivos y ubicaciones de archivos se respaldarán o excluirán de sus respaldos.



Configuracion	Descripcion	Ver Articulo
Archivos Globales	Los archivos globales son grupos de tipos de archivos, por ejemplo, existe un grupo de archivos globales para los archivos de Microsoft Office. Puede agregar, editar o eliminar grupos de tipos de archivos globales.	Elija qué tipos de archivos son "archivos globales"
Ubicaciones	Elija qué volúmenes y carpetas respaldará y protegerá Aranda Datasafe. Para cada ubicación, puede elegir qué archivos se respaldan (todos, globales y personalizado	Elija qué ubicaciones están protegidas
Unidades en la Nube	Elija qué unidades en la nube respaldará y protegerá Aranda Datasafe. Para cada unidad en la nube, puede elegir qué archivos se respaldan (todos, globales y personalizados).	Elija qué unidades en la nube están protegidas
Emails	Elija qué archivos de correo electrónico respaldará y protegerá Aranda Datasafe.	Copia de seguridad y protección de correo electrónico
Exclusiones Globales	Úselo para definir cualquier tipo de archivo o ubicación que Aranda Datasafe no deba respaldar ni proteger.	Excluya archivos y carpetas de la copia de seguridad y la protección

Copia de seguridad y restauración

Utilice la configuración de Copia de seguridad y restauración para programar copias de seguridad automáticas.



Puede optar por ejecutar copias de seguridad cada:

- 1 hora
- 2 horas
- 4 horas
- 8 horas.

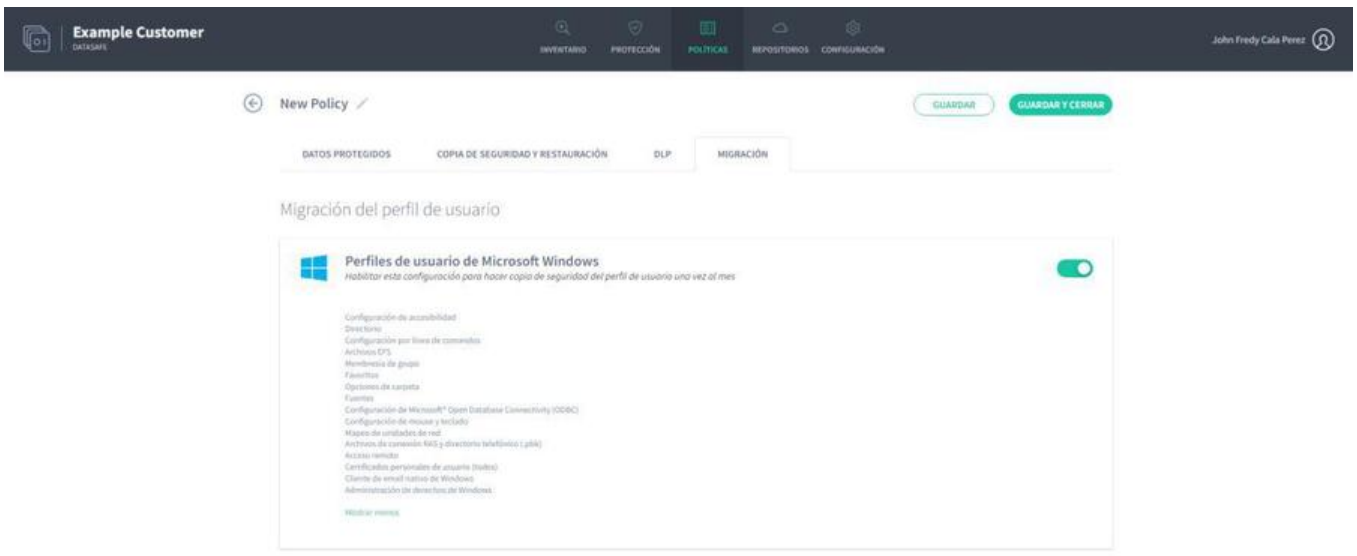
DLP (prevención de pérdida de datos)

Use la configuración de DLP para elegir qué funciones de prevención de pérdida de datos desea que use la Política.

Configuración	Descripción	Ver Articulo
Cifrado	Puede habilitar el cifrado local para cifrar datos en cada dispositivo. Los usuarios no autorizados no podrán ver los archivos cifrados.	Habilitar el cifrado local
Prevención Robo de Información	<p>Si un dispositivo no se conecta a Aranda Datasafe dentro de un período de tiempo determinado, Aranda Datasafe puede revocar el acceso a los archivos en el dispositivo. Mientras está revocado, el usuario no puede acceder a los datos protegidos. Utilice la Prevención de robo de datos para activar o desactivar esta función.	Habilitar la prevención de robo de datos.
Geolocalización	Puede habilitar la geolocalización para dispositivos. Si habilita la geolocalización, puede usar Aranda Datasafe para ver un mapa de la última ubicación conocida de un dispositivo.	Habilitar la geolocalización

Migración

Utilice la configuración de migración para habilitar o deshabilitar la migración de la configuración del perfil de usuario para una política



La función de migración de perfil de usuario está diseñada para usarse cuando está reemplazando un dispositivo. En lugar de configurar el nuevo dispositivo desde cero, puede usar Restaurar para cargarlo con el perfil de usuario y la configuración de otro dispositivo.

Crear Políticas

Una política es un conjunto de reglas que definen:

- Qué datos están protegidos y respaldados
- Con qué frecuencia ocurren las copias de seguridad
- Si se utiliza alguna función de prevención de pérdida de datos para proteger sus datos en caso de pérdida o robo de un dispositivo
- Si se realiza una copia de seguridad de la información de configuración del perfil de Windows.

Puede crear tantas políticas como necesite. Puede tener una Política para todos o puede tener diferentes Políticas para cada equipo.

Para crear una nueva política:

1. Haga clic en **Políticas**.

Si no tiene ninguna política en Aranda Datasafe, haga clic en **Agregar una política**. Si ya tiene algunas políticas, haga clic en **Crear política**.

Aranda Datasafe crea una nueva Política y la abre, lista para que usted defina su configuración.

2. Dé un nombre a la Política. Haga clic en el ícono de edición junto al nombre predeterminado y luego ingrese el nuevo nombre.

Su nueva Política tiene configuraciones predeterminadas, y muchos administradores de Aranda Datasafe encuentran que estas configuraciones son adecuadas para sus necesidades. Si tiene diferentes requisitos, puede cambiar la configuración en las siguientes secciones:

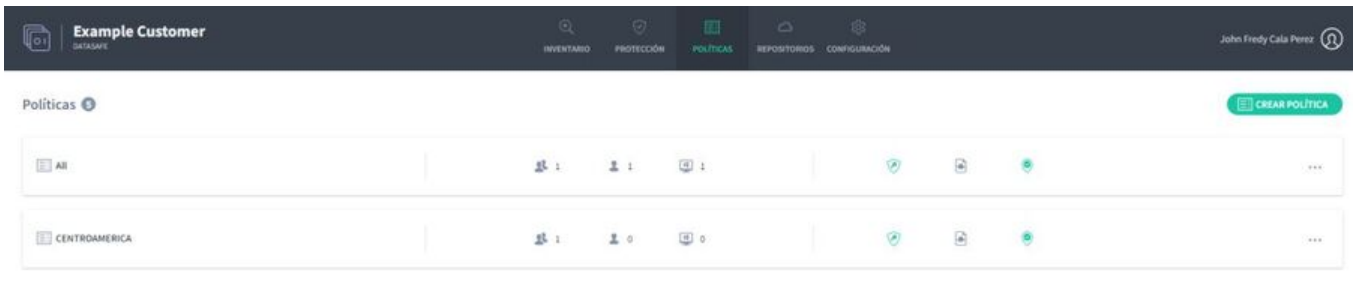
- **Datos protegidos**: se utiliza para definir qué datos se cifran y se respaldan.
- **Copia de seguridad y restauración**: se utiliza para elegir la frecuencia con la que se realizan las copias de seguridad.
- **DLP**: se utiliza para elegir las medidas de prevención de pérdida de datos para la política.
- **Migración**: se utiliza para elegir si se realiza una copia de seguridad de la configuración relacionada con los perfiles de usuario de Windows.

Editar Políticas

Si desea realizar cambios en una política existente:

1. Haga clic en **Políticas**.

2. Haga clic en la Política que desea cambiar.



Aranda Datasafe abre la página del editor de políticas, que puede utilizar para cambiar la configuración de la política.

Puede cambiar la configuración en las siguientes secciones:

- **Datos protegidos**: se utiliza para definir qué datos se cifran y se respaldan.
- **Copia de seguridad y restauración**: se utiliza para elegir la frecuencia con la que se realizan las copias de seguridad.
- **DLP**: se utiliza para elegir las medidas de prevención de pérdida de datos para la política.
- **Migración**: se utiliza para elegir si se realiza una copia de seguridad de la configuración relacionada con los perfiles de usuario de Windows.

Eliminar Políticas

Si ya no necesita una Política o ha creado una Política por error, puede eliminarla.

Precaución: Si elimina una política que está asociada con equipos y dispositivos, esos equipos y dispositivos ya no tendrán una política asignada. Esto significa que no se realizarán copias de seguridad de ellos automáticamente y otras funciones, como la geolocalización, no estarán disponibles.

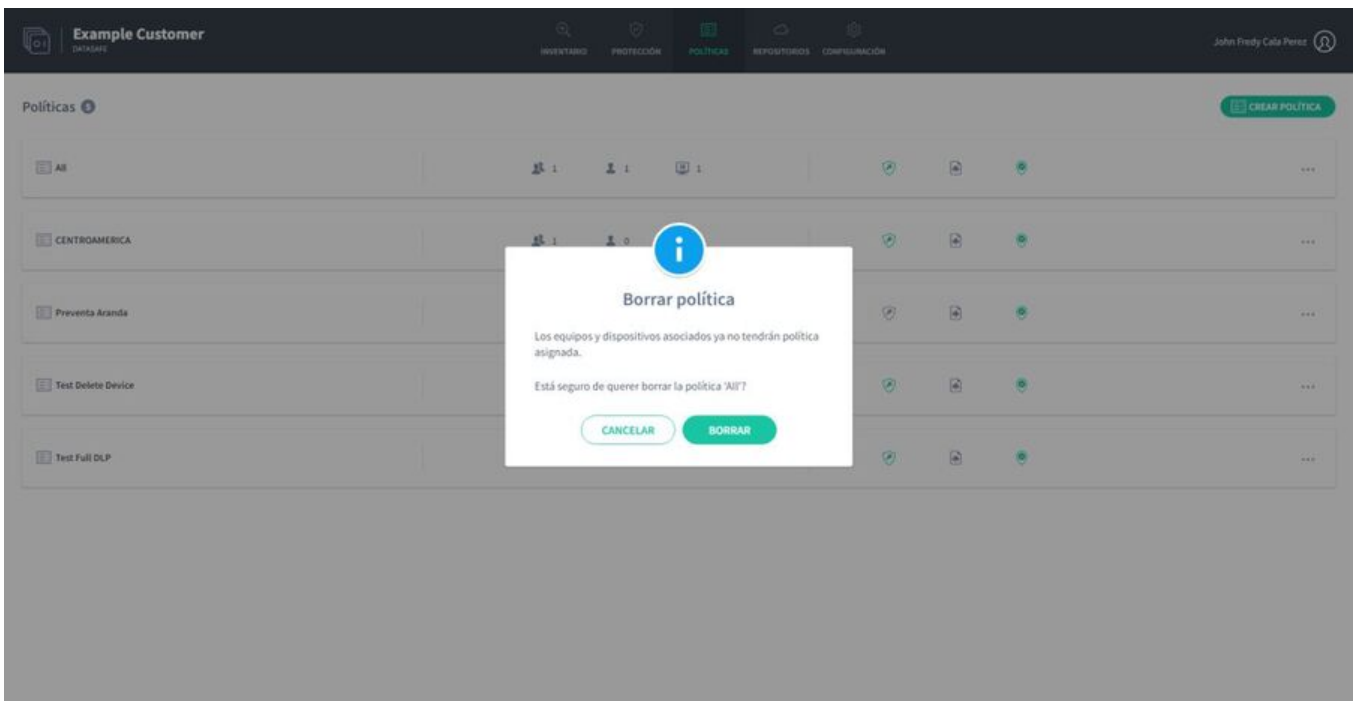
Para eliminar una política:

1. Haga clic en Políticas para mostrar la página Políticas . 2. En la lista de Políticas, busque la Política que desea eliminar.

3. Haga clic en el botón de opción (...) de la Política.

4. Haga clic en Eliminar.

5. Cuando se le indique, haga clic en Eliminar para confirmar.



Archivos Globales

Puede utilizar la función **Archivos globales** para crear colecciones de tipos de archivos. Hace que sea mucho más rápido elegir qué archivos se respaldan, ya que en lugar de tener que elegir cada tipo de archivo por separado para cada ubicación, puede elegir una colección de Archivos globales.

Por ejemplo, de forma predeterminada, cada política tiene una colección de archivos de **Microsoft Office** de **archivos globales**. Esta colección incluye archivos guardados en Word, Excel, PowerPoint, etc. Cuando elige qué tipos de archivos deben respaldarse, puede elegir la colección Archivos globales en lugar de tener que seleccionar cada tipo de archivo de MS Office por separado.

Puede utilizar la configuración de **Archivos globales** en una política para:

- Agregar o eliminar tipos de archivos de las diferentes colecciones de archivos globales
- Cree una nueva colección para diferentes tipos de archivos. Por ejemplo, es posible que desee crear una nueva colección que contenga los tipos de archivo para su software propietario.

Cambiar una colección existente de archivos globales

Para realizar cambios en una colección existente de archivos globales:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. Asegúrese de que se muestre la pestaña **Datos protegidos**.

3. En la lista de **Archivos globales**, busque la colección de Archivos globales que desea cambiar y haga clic en el ícono Editar (lápiz).

4. Utilice el campo **Editar nombre de tipo de archivo** para cambiar el nombre de la colección de archivos globales, si es necesario.

5. Utilice el cuadro **Agregar o quitar extensiones** para agregar o eliminar extensiones de archivo.

Para agregar una extensión de archivo, haga clic en una parte vacía del cuadro e ingrese los caracteres de la extensión del archivo. Presione Entrar y aparecerá un bloque azul para su nuevo tipo de extensión. Haga clic en **Guardar cambios** para confirmar.

Para eliminar un tipo de extensión de archivo, haga clic en la X en el bloque azul correspondiente. Haga clic en **Guardar cambios** para confirmar.

Agregar una nueva colección de archivos globales

Para agregar una nueva colección de archivos globales:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en **Política**).

2. Asegúrese de que se muestre la pestaña **Datos protegidos**.

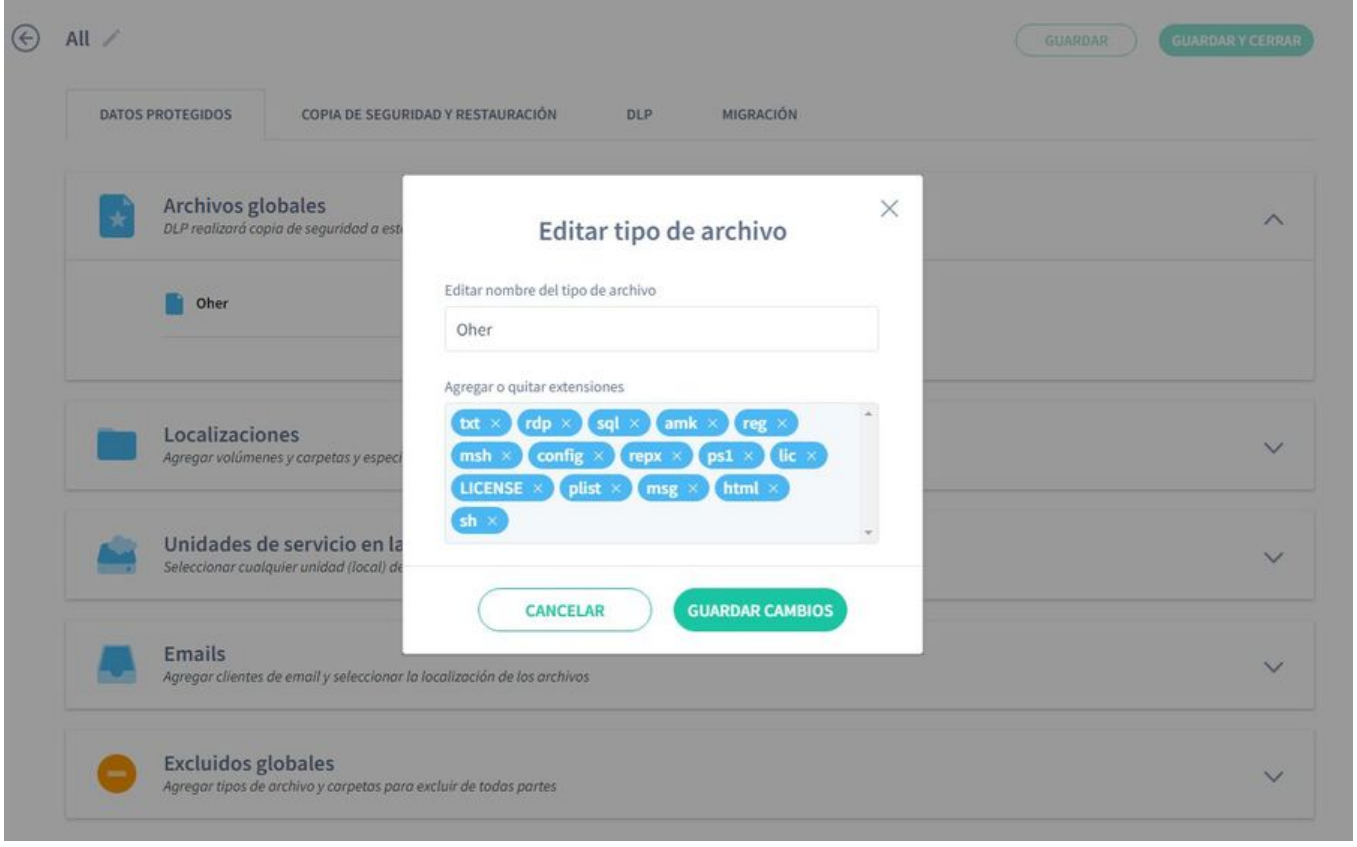
3. En la sección Archivos globales de la pestaña **Datos protegidos**, haga clic en el ícono más (+) para mostrar el cuadro de diálogo Agregar tipo de archivo.

4. Utilice la opción **Seleccionar un tipo de archivo** para establecer el nombre de su nueva colección de archivos globales. Puede elegir de la lista de tipos de archivo disponibles o puede seleccionar Agregar nuevo tipo de archivo.

5. Si seleccionó **Agregar nuevo tipo de archivo** en el paso 2, ingrese el nombre de la nueva colección de archivos globales en el campo **Editar nombre de tipo de archivo**. Si elige un tipo de archivo existente, puede editar el nombre o dejarlo como está.

6. Utilice el cuadro **Agregar o quitar extensiones** para agregar o eliminar extensiones de archivo de la nueva colección de archivos globales. Esto funciona de la misma manera que cuando se edita una colección de archivos globales (ver arriba).

7. Haga clic en **Guardar cambios**.



Eliminar una colección de archivos globales

Para eliminar una colección de Global Files de Aranda Datasafe:

1.Abra el Editor de políticas para la Política que desea cambiar (haga clic en**Políticas** y luego haga clic en Política).

2. Asegúrese de que se muestre la pestaña**Datos protegidos**.

3.En la lista de**Archivos globales**, busque la colección de Archivos globales que desea eliminar y haga clic en su ícono de papelera.

Ubicaciones Protegidas

Puede configurar Aranda Datasafe para realizar copias de seguridad y proteger archivos en ubicaciones específicas en una computadora (solo unidades locales, de forma predeterminada). Algunas ubicaciones comunes se incluyen de forma predeterminada, incluidos Todos los volúmenes, Escritorio y Documentos, y puede agregar otras ubicaciones si es necesario.

Para elegir las ubicaciones a proteger, use la configuración de**Ubicaciones** en una Política. Para cada ubicación, puede elegir qué archivos se respaldan y protegen:

- todos los archivos
- solo archivos globales
- archivos que elija manualmente.

Puede utilizar la sección Ubicaciones para:

Agregar una ubicacion.

Editar una ubicación.

Eliminar una ubicación.

Agregar Ubicación

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en Políticas y luego haga clic en Política).

2. En la pestaña**Datos protegidos**, expanda la configuración de**Ubicaciones**.

3. Haga clic en el ícono más (+) para mostrar un menú contextual. El menú contextual tiene opciones para algunas ubicaciones comúnmente protegidas, incluidas Descargas y Videos. Para agregar su propia ubicación, haga clic en **Agregar nueva ubicación**.

4. Ingrese un **nombre de ubicación** significativo para que otras personas comprendan dónde está esta ubicación.

5. En el campo **Ruta**, ingrese la ubicación de la carpeta de los archivos que desea proteger.

6. Si desea incluir varias carpetas, haga clic en el ícono más (+) para **Agregar otra ruta**. Esto crea otro campo de ruta.

7. Haga clic en **Guardar cambios** para confirmar.

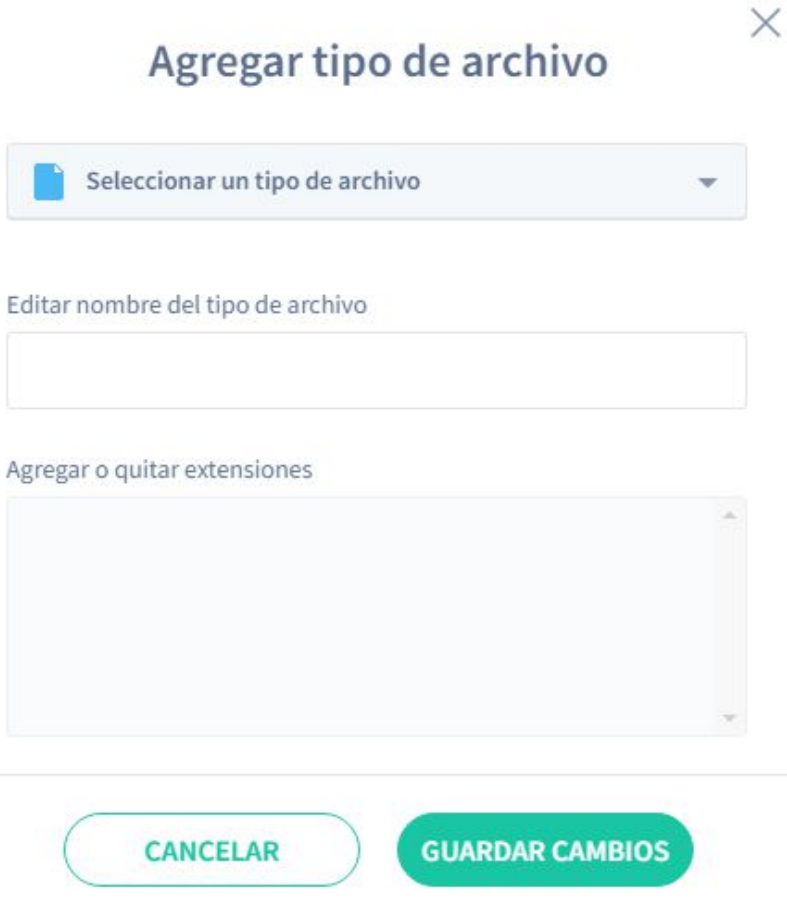
8. Elija si desea proteger **Todos los archivos**.

Si habilita esta función, todos los archivos en la ubicación estarán protegidos, con la excepción de cualquier tipo de archivo excluido (el archivo global excluye o la selección de archivo personalizada excluye). Si lo desactiva, puede elegir qué archivos proteger.

9. Elija si desea proteger los **rchivos globales** para esta ubicación. Si habilita esta función, todos los tipos globales serán respaldados y protegidos. Si lo desactiva, los tipos de archivos globales no se incluirán (a menos que los agregue como secciones de archivos personalizados en el siguiente paso).

10. . Utilice **Selección de archivo personalizada** para incluir o excluir cualquier tipo de archivo en particular para esta ubicación. Si habilita esta función, puede utilizar la sección Incluye y excluye (consulte los pasos siguientes). Por ejemplo, puede optar por incluir una colección de archivos globales en lugar de todos los tipos de archivos globales.

En la sección **Incluye**, haga clic en **Agregar tipo de archivo**.



11. Utilice el cuadro de diálogo Agregar tipo de archivo para elegir los tipos de archivos que desea proteger para esta ubicación. Puede elegir cualquiera de sus colecciones de archivos globales y luego **Agregar o quitar extensiones** para especificar qué tipos de archivos se respaldarán.

Alternativamente, puede hacer clic en **Agregar nuevo tipo de archivo** para crear su propia selección personalizada (ingrese el nombre en el campo **Editar nombre del tipo de archivo** y use **Agregar o quitar extensiones** para elegir los tipos de archivo). Haga clic en **Guardar cambios** para confirmar.

12. En la sección Exclusiones, use **Agregar tipo de archivo** para excluir para elegir cualquier tipo de archivo que no deba protegerse para esta ubicación. Por ejemplo, si desea que Aranda Datasafe proteja todos los archivos globales, excepto los PDF, la forma más rápida es habilitar Archivos globales para la ubicación y luego excluir los PDF.

Utilice el cuadro de diálogo Agregar tipo de archivo para elegir los tipos de archivos que no desea que estén protegidos para esta ubicación.

Puede elegir cualquiera de sus colecciones de archivos globales y luego agregar o quitar extensiones para especificar qué tipos de archivos se excluirán. Alternativamente, puede agregar una nueva extensión de archivo para excluirla. Haga clic en Guardar cambios para confirmar.

13. En la sección **Exclusiones**, use **Agregar una carpeta para excluir** para elegir carpetas específicas que no deben protegerse para esta ubicación. Haga clic en Agregar una carpeta para excluir para mostrar un menú contextual. A continuación, puede elegir **Carpetas del sistema, Carpetas temporales o Agregar una carpeta nueva**. Si agrega una nueva carpeta, aparece el cuadro de diálogo Agregar carpeta y puede establecer el nombre de la carpeta y la(s) ruta(s).

Haga clic en Guardar cambios para confirmar que las carpetas no estarán protegidas.

14. Haga Click en **Guardar Cambio**.

Editar Ubicación

Para realizar cambios en una ubicación existente:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. En la pestaña **Datos protegidos**, expanda la configuración de **Ubicaciones**.

3. Haga clic en el ícono Editar (lápiz) de la Ubicación que desea cambiar.

4. Utilice la configuración de **Todos los archivos, Archivos globales y Selección de archivos** personalizados para realizar los cambios. Estos funcionan de la misma manera que cuando se agrega una ubicación (ver arriba).

5. Haga clic en **Guardar Cambios**.

Eliminar Ubicación

Para eliminar una ubicación de una política:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. **En la pestaña Datos protegidos, expanda la configuración de Ubicaciones**

3. Haga clic en el ícono de la papelera de la ubicación que desea eliminar.

Unidades de Nube Protegidas

Puede configurar Aranda Datasafe para realizar copias de seguridad y proteger archivos en servicios de almacenamiento en la nube, como One Drive, Google Drive y Dropbox.

Para elegir qué servicios en la nube proteger, use la configuración de **Unidades en la Nube** en una Política. Para cada unidad en la nube, puede elegir qué archivos se respaldan y protegen:

- todos los archivos
- solo archivos globales
- archivos que elija manualmente.

Agregar una unidad en la nube

Para agregar una unidad en la nube a una política para que esté protegida:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. En la pestaña **Datos protegidos**, expanda la configuración de **Unidades en la Nube**.

3. Haga clic en el ícono más (+) para mostrar un menú contextual.

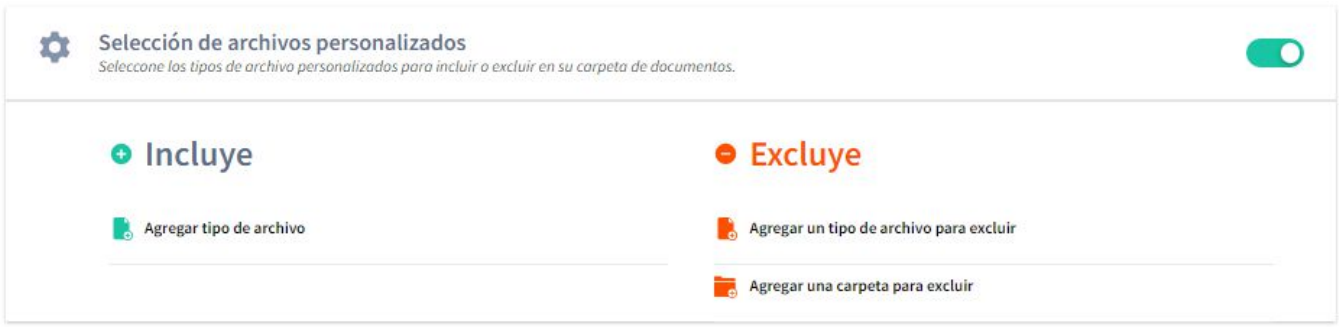
4. Elija la unidad en la nube que desea agregar, por ejemplo, One Drive.

5. Elija si desea proteger **Todos los archivos**.

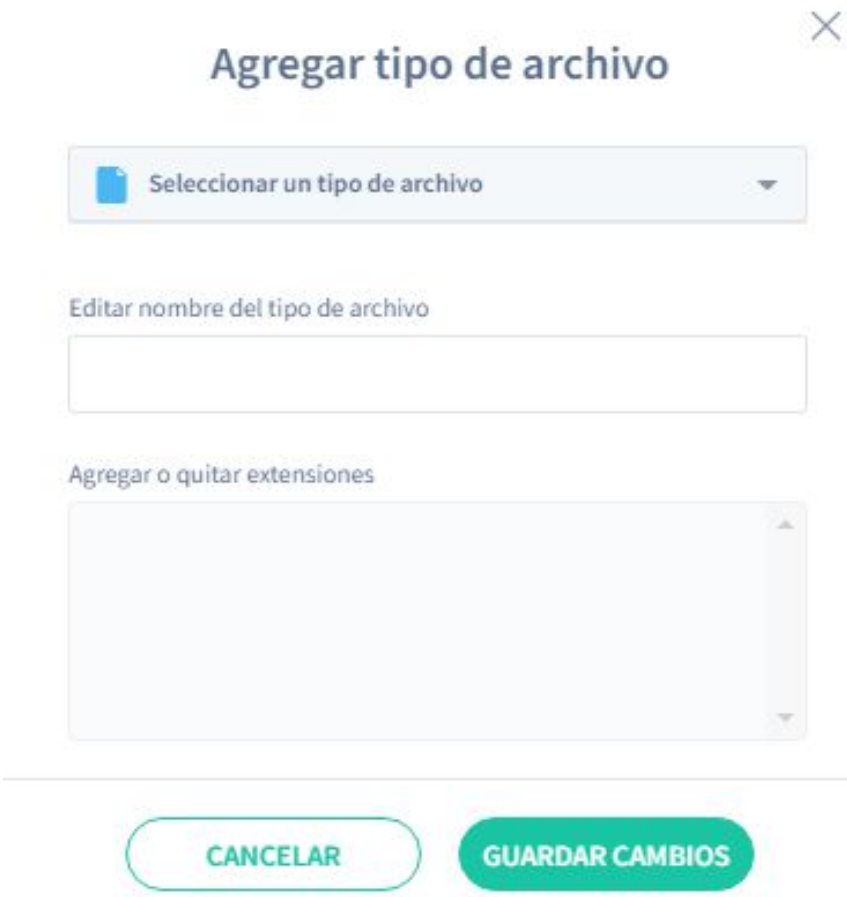
Si habilita esta función, todos los archivos en la unidad en la nube estarán protegidos, con la excepción de cualquier tipo de archivo excluido (el archivo global excluye o la selección de archivo personalizada excluye). Si lo desactiva, puede elegir qué archivos proteger.

6. Elija si desea que los **archivos globales** estén protegidos para esta unidad en la nube. Si habilita esta función, todos los tipos globales serán respaldados y protegidos. Si lo desactiva, los tipos de archivos globales no se incluirán (a menos que los agregue como secciones de archivos personalizados en el siguiente paso).

7. Utilice la selección de **archivos personalizados** para incluir o excluir cualquier tipo de archivo en particular para esta unidad en la nube. Si habilita esta función, puede utilizar la sección **Inclusiones y Exclusones** (consulte los pasos siguientes). Por ejemplo, puede optar por incluir una colección de archivos globales en lugar de todos los tipos de archivos globales.



8. En la sección **Inclusiones**, haga clic en **Agregar tipo de archivo**.



Utilice el cuadro de diálogo Agregar tipo de archivo para elegir los tipos de archivos que desea proteger para esta unidad en la nube. Puede elegir cualquiera de sus colecciones de archivos globales y luego **Agregar o quitar extensiones** para especificar qué tipos de archivos se respaldarán.

Alternativamente, puede hacer clic en **Agregar nuevo tipo de archivo** para crear su propia selección personalizada (ingrese el nombre en el campo **Editar nombre de tipo de archivo** y use **Agregar o quitar extensiones** para elegir los tipos de archivo). Haga clic en **Guardar cambios** para confirmar.

9. En la sección **Exclusiones**, use **Agregar tipo de archivo** para excluir para elegir cualquier tipo de archivo que no deba protegerse para esta unidad en la nube. Por ejemplo, si desea que Aranda Datasafe proteja todos los archivos globales, excepto los PDF, la forma más rápida es habilitar Archivos globales para la unidad en la nube y luego excluir los PDF.

Utilice el cuadro de diálogo **Agregar tipo de archivo** para elegir los tipos de archivos que no desea que estén protegidos para esta unidad en la nube.

Puede elegir cualquiera de sus colecciones de archivos globales y luego agregar o quitar extensiones para especificar qué tipos de archivos se excluirán. Alternativamente, puede agregar una nueva extensión de archivo para excluirla. Haga clic en **Guardar cambios** para confirmar.

10. En la sección **Exclusiones**, use **Agregar una carpeta** para excluir para elegir carpetas específicas que no deben protegerse para esta unidad en la nube. Haga clic en Agregar una carpeta para excluir para mostrar un menú contextual. A continuación, puede elegir **Carpetas del sistema, Carpetas temporales o Agregar una carpeta nueva**. Si agrega una nueva carpeta, aparece el cuadro de diálogo Agregar carpeta y puede establecer el nombre de la carpeta y la (s) ruta (s).

Haga clic en **Guardar cambios** para confirmar que las carpetas no estarán protegidas

Editar una unidad en la nube

Para realizar cambios en una unidad en la nube existente:

1. . Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. En la pestaña **Datos protegidos**, expanda la configuración de **Unidades en la Nube**.

3. Haga clic en el ícono Editar (lápiz) de la unidad de nube que desea cambiar.

4. Utilice la configuración de **Todos los archivos, Archivos globales y Selección de archivos** personalizados para realizar los cambios. Estos funcionan de la misma manera que cuando se agrega una unidad en la nube (ver más arriba).

5. Haga clic en **Hecho**.

Eliminar una unidad en la nube

Para eliminar una unidad en la nube de una política:

1. Busque en el Editor de políticas la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. En la pestaña **Datos protegidos**, expanda la configuración de **Unidades en la Nube**.

3. Haga clic en el ícono de la papelera de la unidad de nube que desea eliminar.

Protección y respaldo de correo electrónico

Puede configurar Aranda Datasafe para hacer una copia de seguridad y proteger los archivos de su cliente de correo electrónico. Por ejemplo, puede agregar Microsoft Outlook como cliente de correo electrónico y luego configurar Aranda Datasafe para hacer una copia de seguridad y proteger todos los archivos PST de Outlook o solo aquellos archivos PST que están activos.

La configuración de correo electrónico se encuentra en la política que se utiliza para hacer una copia de seguridad de su dispositivo.

Agregar un cliente de correo electrónico para respaldo

Para agregar un cliente de correo electrónico:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en Políticas y luego haga clic en Política).

⚐ **Nota:** El editor de políticas se muestra automáticamente cuando crea una nueva política.

2. Asegúrese de que se muestre la pestaña**Datos protegidos**.

3. Expanda la sección **Correos electrónicos**.

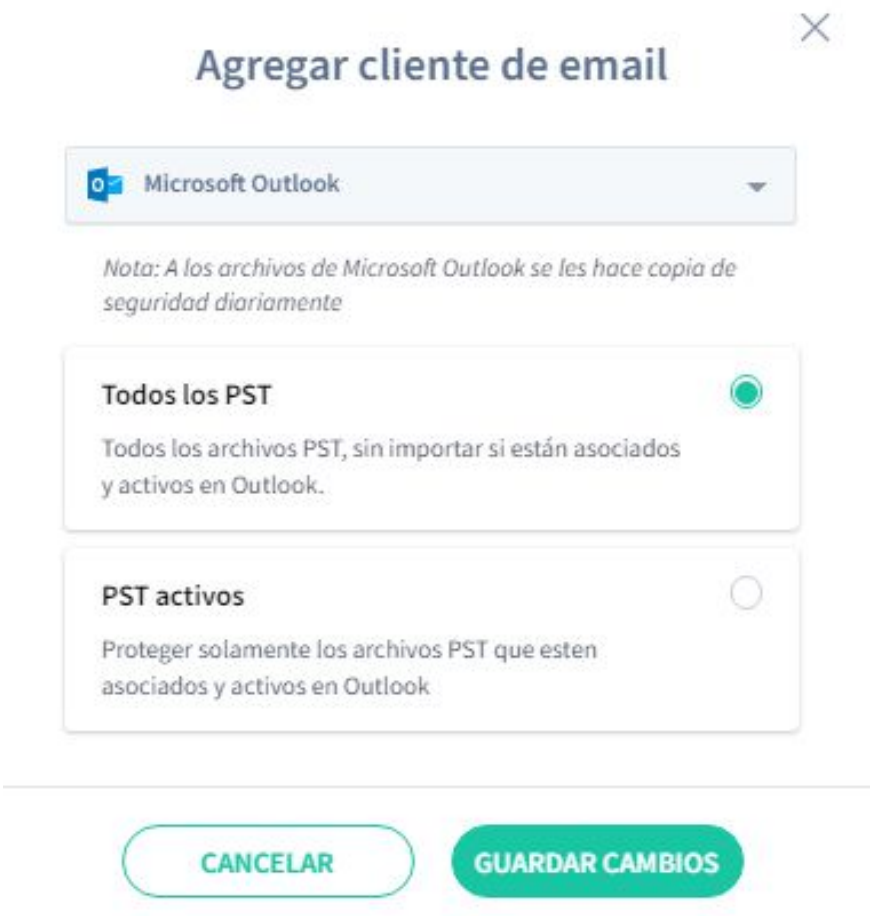
4. Haga clic en el ícono más (+).

5. Seleccione el cliente de correo electrónico, por ejemplo, Microsoft Outlook.

6. Elija qué archivos PST desea respaldar:

- Todos los archivos PST: Aranda Datasafe realizará una copia de seguridad de todos los archivos PST, incluso si están inactivos o no están asociados con el cliente de correo electrónico.
- PST activos: Aranda Datasafe solo hará una copia de seguridad de los archivos PST que están asociados con el cliente de correo electrónico y que están actualmente activos en el perfil de Outlook.

7. Haga clic en **Guardar cambios**.



Editar un cliente de correo electrónico

Para realizar cambios en un cliente de correo electrónico existente:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. Asegúrese de que se muestre la pestaña**Datos protegidos**.

3. Expanda la sección **Correos electrónicos**.

4. Haga clic en el ícono Editar (lápiz) del cliente de correo electrónico que desea cambiar.

5. Utilice el cuadro de diálogo Editar cliente de correo electrónico para elegir qué archivos se respaldan:

- **Todos los archivos PST**: Aranda Datasafe realizará una copia de seguridad de todos los archivos PST, incluso si están inactivos o no están asociados con el cliente de correo electrónico.
- **PST activos**: Aranda Datasafe solo hará una copia de seguridad de los archivos PST que están asociados con el cliente de correo electrónico y que están activos actualmente.

6. Haga clic en **Guardar cambios**.

Eliminar un cliente de correo electrónico

Para eliminar un cliente de correo electrónico:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en Políticas y luego haga clic en Política).

2. Asegúrese de que se muestre la pestaña Datos protegidos.

3. Expanda la sección Correos electrónicos.

4. Haga clic en el ícono Papelera del cliente de correo electrónico que desea eliminar.

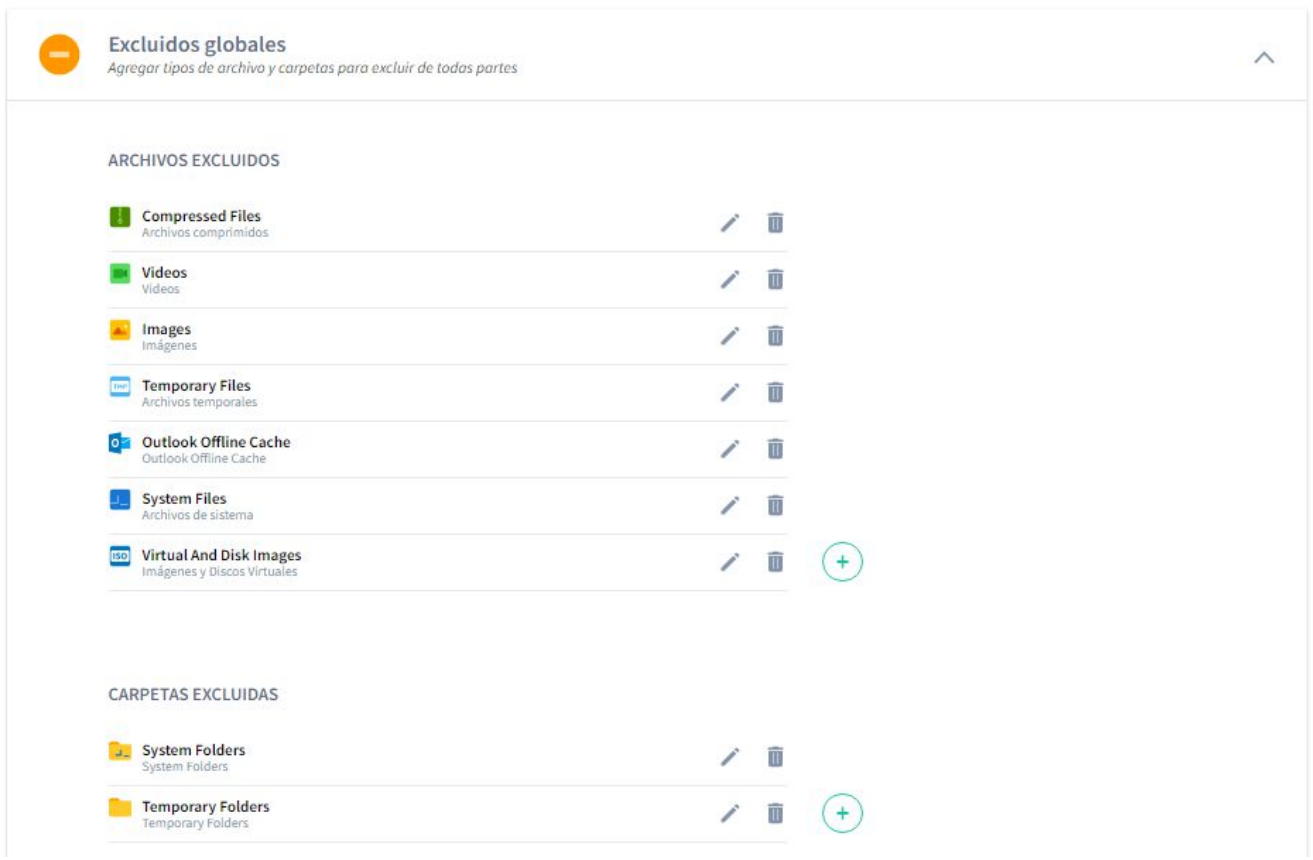
Excluir archivos y carpetas de la copia de seguridad y la protección

Es posible que desee excluir ciertos tipos de archivos del respaldo y la protección de Aranda Datasafe. Por ejemplo, puede excluir archivos de imagen, videos y música. También puede excluir determinadas carpetas.

Hay dos formas de excluir archivos y carpetas:

- Puede excluir para una ubicación específica
- Puede excluir para todas las ubicaciones.

En este artículo, explicamos cómo utilizar la función**Exclusiones globales** para excluir archivos y carpetas de todas las ubicaciones. La función de Exclusiones globales es útil cuando sabe que hay ciertos tipos de archivos que nunca desea que estén protegidos para ninguna ubicación. Le permite crear un grupo de tipos de archivos que puede excluir para todas las ubicaciones en una sola acción.



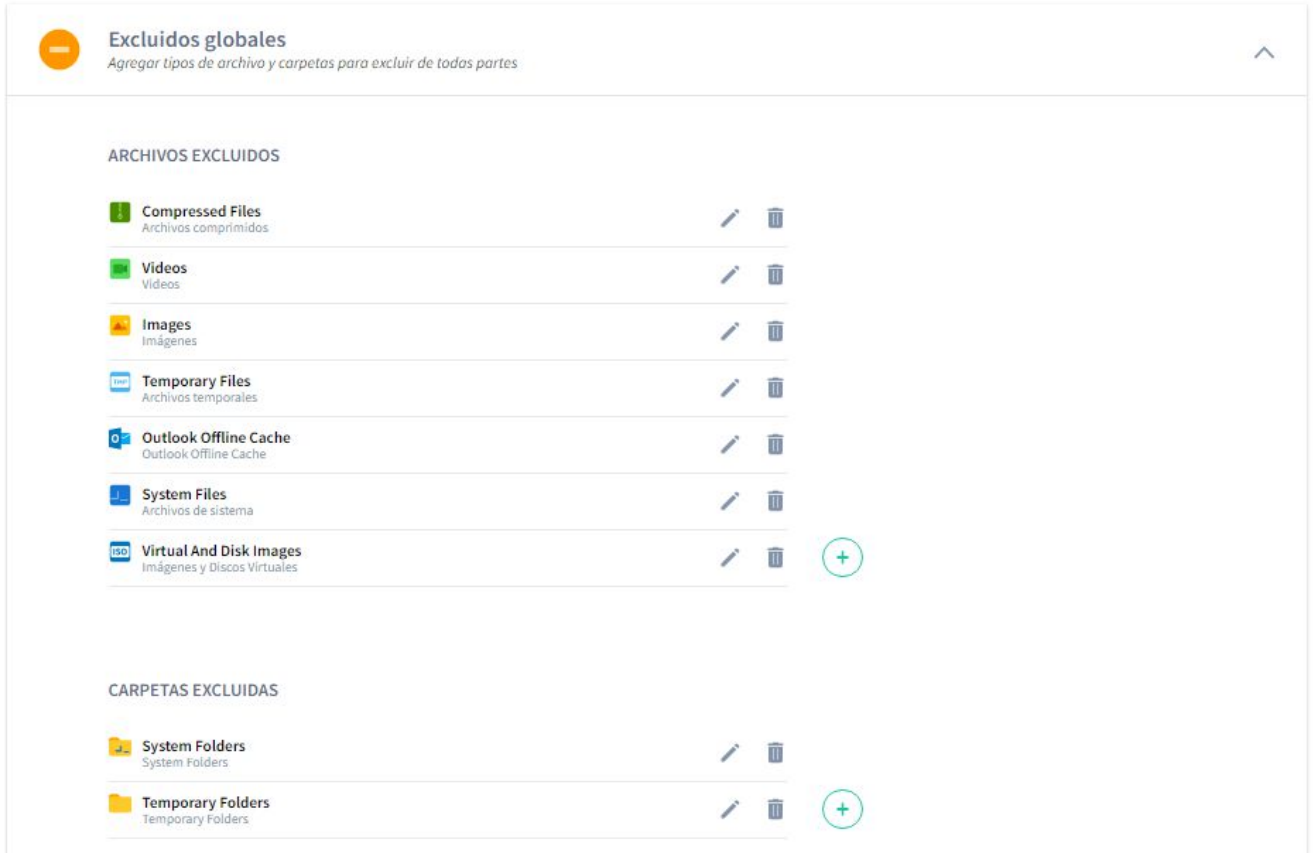
Para saber cómo excluir archivos para una ubicación específica, consulte [Elegir qué archivos y carpetas] están protegidos.

Excluir archivos de la protección para todas las ubicaciones

Para evitar que se realice una copia de seguridad y se proteja a ciertos tipos de archivos para todas las ubicaciones:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en**Políticas** y luego haga clic en Política).

2. En la pestaña**Datos protegidos**, expanda la configuración de**Exclusión global**.



3. En la sección Archivos excluidos, haga clic en el ícono más (+) para mostrar el cuadro de diálogo Agregar tipo de archivo.

4. Utilice la opción **Seleccionar un tipo de archivo** para establecer el nombre de su nuevo grupo de archivos globales. Puede elegir de la lista de tipos de archivo disponibles o puede seleccionar **Agregar nuevo tipo de archivo**.

5. Si seleccionó **Agregar nuevo tipo de archivo** en el paso 4, ingrese el nombre del nuevo grupo de Archivos globales en el campo **Editar nombre de tipo de archivo**. Si elige un tipo de archivo existente, puede editar el nombre o dejarlo como está.

6. Utilice el cuadro **Agregar o quitar extensiones** para agregar o eliminar extensiones de archivo del nuevo grupo Archivos globales. Se excluirán las extensiones de archivo que agregue al cuadro; Aranda Datasafe no protegerá estos tipos de archivos para dispositivos que utilicen esta Política.

7. Haga clic en **Guardar cambios**.

Editar las reglas de exclusión de archivos globales

Para cambiar los archivos que se incluyen en las exclusiones globales:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. Asegúrese de que se muestre la pestaña **Datos protegidos**.

3. En la lista de **exclusiones globales**, busque el grupo que desea cambiar y haga clic en el ícono **Editar** (lápiz).

4. Utilice el campo **Editar nombre de tipo de archivo** para cambiar el nombre del grupo, si es necesario.

5. Utilice el cuadro **Agregar o quitar extensiones** para agregar o eliminar extensiones de archivo.

Para agregar una extensión de archivo, haga clic en una parte vacía del cuadro e ingrese los caracteres de la extensión del archivo. Presione Entrar y aparecerá un bloque azul para su nuevo tipo de extensión. Haga clic en **Guardar cambios** para confirmar.

Para eliminar un tipo de extensión de archivo, haga clic en la X en el bloque azul correspondiente. Haga clic en **Guardar cambios** para confirmar.

Excluir carpetas de la protección para todas las ubicaciones

Puede excluir carpetas de la protección de Aranda Datasafe. Por ejemplo, sus usuarios pueden tener carpetas de datos personales donde almacenan datos no comerciales y no desea que se haga una copia de seguridad de esta información.

Para excluir carpetas de todas las ubicaciones:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. Asegúrese de que se muestre la pestaña **Datos protegidos**.

3. En la sección **Exclusiones globales**, haga clic en el ícono más (+).

4. Puede elegir Carpetas del sistema o Carpetas temporales, o hacer clic en Agregar nueva carpeta para elegir una carpeta específica. Si agrega una nueva carpeta, aparece el cuadro de diálogo Agregar carpeta y puede establecer el nombre de la carpeta y la (s) ruta (s).

5.Haga clic en **Guardar cambios**.

Editar las carpetas excluidas

Si ha establecido Carpetas excluidas en las exclusiones globales para una política, puede editarlas para:

- Cambiar el nombre de la carpeta
- Cambiar el camino
- Agregue rutas adicionales.

Para editar carpetas de exclusión global:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. Asegúrese de que se muestre la pestaña **Datos protegidos**.

3. En la sección **Exclusiones globales**, haga clic en el ícono Editar (lápiz) del grupo de exclusión global que desea cambiar.

4. Utilice el campo **Nombre de carpeta** para cambiar el nombre del grupo.

5.Utilice los campos **Ruta** para cambiar las ubicaciones de las carpetas.

6.Haga clic en **Guardar Cambios**.

Eliminar archivos o carpetas de las exclusiones globales

Para eliminar archivos o carpetas de las exclusiones globales de una política:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. Asegúrese de que se muestre la pestaña **Datos protegidos**.

3.En la sección **Exclusiones globales**, haga clic en el ícono de la papelera para el grupo o carpeta de exclusión global que desea eliminar.

Cuando elimina un grupo de archivos o carpetas de las exclusiones globales en una politica, ya no están excluidos de la protección de Aranda Datasafe. (A menos que también estén excluidos en la configuración de Ubicación).

Programar Copias de Seguridad Automática

Aranda Datasafe hará una copia de seguridad automática de los dispositivos que utilizan una Política. La primera copia de seguridad se realiza aproximadamente 10 minutos después de que un dispositivo se activa por primera vez y, después de eso, las copias de seguridad se ejecutan según un programa regular.

Puede establecer la programación en la configuración de **Copia de seguridad y restauración** para una Política.

Establecer la programación para las copias de seguridad automáticas

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. Haga clic en la pestaña **Copia de seguridad y restauración**.

3. Utilice la opción Ejecutar copias de seguridad del dispositivo en todas las opciones para elegir la frecuencia con la que se realizarán las copias de seguridad automáticas. puedes elegir:

- 1 hora
- 2 horas
- 4 horas
- 48 horas
- Haga clic en **Guardar** o **Guardar y cerrar** para confirmar.

Ejemplo: Si tiene una política de 'Finanzas' y la ha configurado para realizar copias de seguridad cada 2 horas. También tiene un equipo de 'Finanzas' y le ha asignado la política de 'Finanzas'.

Los dispositivos del equipo de Finanzas tendrán una copia de seguridad de sus datos automáticamente cada 2 horas (ya que ese es el horario definido en la política utilizada por su equipo).

Para los dispositivos de otros equipos, el programa de respaldo podría ser diferente, ya que sus equipos pueden usar una política diferente que está configurada para respaldar en un momento diferente, como cada 8 horas.

Habilitar Cifrado Local

Prerrequisitos: Antes de habilitar las funciones de DLP, asegúrese de que se hayan configurado los Servicios de certificados de Active Directory.

Puede configurar la política para habilitar el cifrado de los archivos que se encuentran en los dispositivos del usuario. A esto lo llamamos "cifrado de archivos local".

Una vez habilitada, cada dispositivo que use la Política recibirá un certificado (también conocido como clave) y se aplicará el cifrado local. Solo los usuarios autenticados pueden acceder a los datos de un dispositivo si el certificado está disponible.

El certificado se utiliza para controlar el acceso a los datos de un dispositivo. Al revocar el certificado en Aranda Datasafe, lo eliminas del dispositivo y los datos en el dispositivo se vuelven inaccesibles.

Si habilita la función de **Prevención de robo de datos**, el certificado se revoca automáticamente en los dispositivos que no se conectan con Aranda Datasafe dentro de un período de tiempo determinado (consulte Habilitar la prevención de robo de datos).

Para habilitar o deshabilitar el cifrado de archivos locales en una política:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. Haga clic en la pestaña **DLP**.

3. Utilice el control deslizante **Cifrado** para habilitar o deshabilitar el cifrado de archivos locales (el verde está habilitado, el gris está deshabilitado).

4. Haga clic en **Guardar o Guardar y cerrar** para confirmar.

Habilitar Prevención de Robo de Datos

Con la función de **prevención de robo de datos** de Aranda Datasafe, puede configurar los dispositivos para revocar el acceso a archivos si no se conectan con Aranda Datasafe dentro de un período de tiempo determinado. Para revocar un dispositivo, Aranda Datasafe elimina el certificado de cifrado del dispositivo.

Mientras se revoca un dispositivo, no se puede utilizar para acceder a datos protegidos.

Puede habilitar o deshabilitar la función de prevención de robo de datos en una politica. Cuando la Prevención de robo de datos está habilitada, todos los dispositivos que utilizan la Política deberán conectarse con Aranda Datasafe con regularidad o serán revocados.

Prerequisitos: Antes de habilitar las funciones de DLP, asegúrese de que se hayan configurado los Servicios de certificados de Active Directory.
La función de prevención de robo de datos solo está disponible si la función de cifrado de archivos local está habilitada para la política. (Utiliza el certificado de cifrado que se genera cuando se utiliza el cifrado de archivos local).

Para habilitar o deshabilitar la prevención de robo de datos:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. Haga clic en la pestaña **DLP**.

3. Utilice el control deslizante de **Prevención de robo de datos** para habilitar o deshabilitar la Prevención de robo de datos (el verde está habilitado, el gris está deshabilitado).

Aparece un mensaje que le recuerda que configure los Servicios de certificados de Active Directory (AD CS). Se recomienda configurar AD CS antes de habilitar DLP. Haga clic en **Aceptar** para cerrar el mensaje.

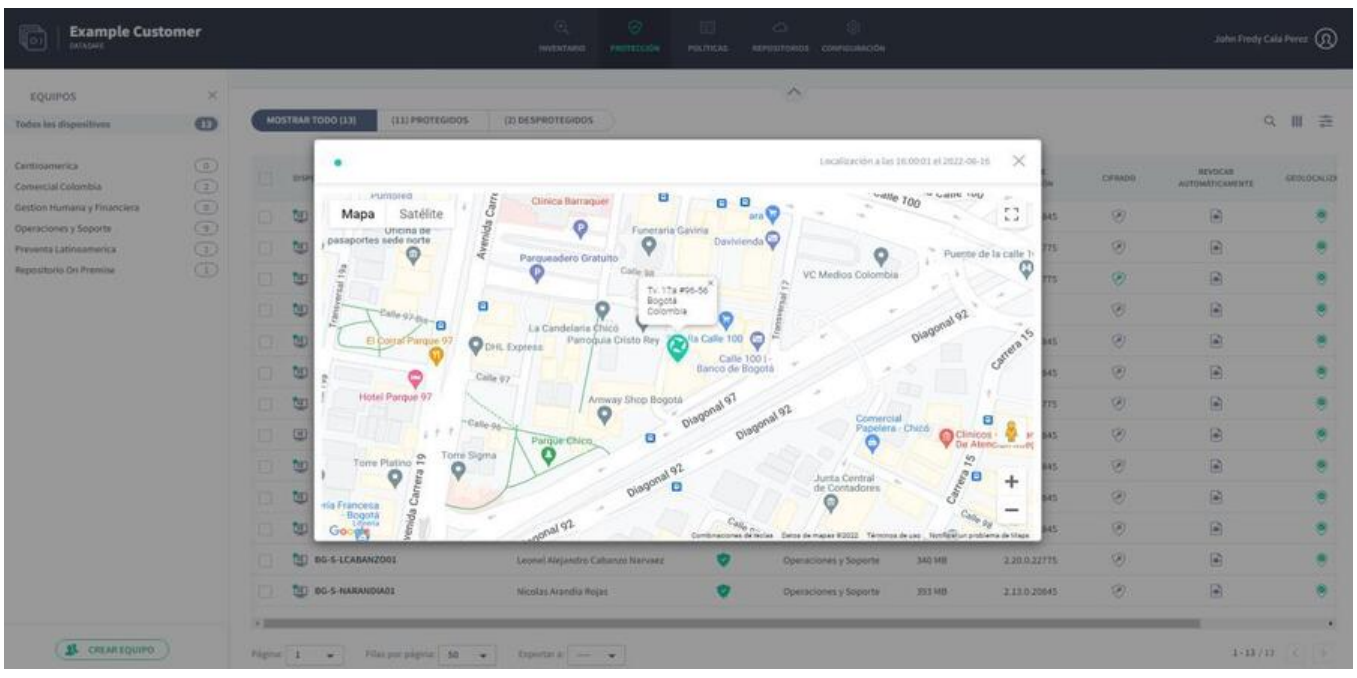
4. Utilice la opción **Revocar si el dispositivo se desconecta durante en días** para definir cuánto tiempo esperará Aranda Datasafe antes de bloquear un dispositivo.

5. Haga clic en **Guardar o Guardar y cerrar** para confirmar.

Habilitar Geolocalización

Prerequisitos: Antes de habilitar las funciones de DLP, asegúrese de que se hayan configurado los Servicios de certificados de Active Directory.
Puede utilizar la función de geolocalización para encontrar la última ubicación conocida de sus dispositivos protegidos. Se puede usar con cualquier dispositivo que tenga wi-fi habilitado.

Cuando la geolocalización está habilitada, puede usar Aranda Datasafe para ubicar un dispositivo y mostrará la última ubicación conocida en un mapa de Google incrustado.



Puede habilitar o deshabilitar la función de **geolocalización** en una política. Si lo habilita, todos los dispositivos que usan esa Política y tienen Wi-Fi habilitado pueden ubicarse **usando Localizar Dispositivo** en Aranda Datasafe.

Para habilitar o deshabilitar la geolocalización en una política:

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en Políticas y luego haga clic en Política).

2. Haga clic en la pestaña **DLP**.

3. Utilice el control deslizante de **Geolocalización** para habilitar o deshabilitar el cifrado local (el verde está habilitado, el gris está deshabilitado).

4. Haga clic en **Guardar** o **Guardar y cerrar** para confirmar.

Habilitar la migración de perfiles de usuario

La función de **migración** está diseñada para ayudarlo a migrar la configuración del perfil de usuario de Windows de un dispositivo protegido a otro. Este tipo de datos incluye configuraciones de accesibilidad, configuraciones de mouse y teclado, favoritos y muchas otras configuraciones específicas del usuario.

Por ejemplo, digamos que tiene una computadora portátil respaldada y protegida por Aranda Datasafe. Decide reemplazar la computadora portátil con una computadora portátil más nueva y de mayor especificación. Al utilizar la función de migración, puede transferir la configuración del perfil de usuario de Windows de la computadora portátil antigua a la nueva. Esto es mucho más rápido y fácil que configurar la nueva computadora portátil desde cero.

Puede habilitar o deshabilitar la función de migración para cada política.

1. Abra el Editor de políticas para la Política que desea cambiar (haga clic en **Políticas** y luego haga clic en Política).

2. Haga clic en la pestaña **Migración**.

3. Utilice el control deslizante para habilitar o deshabilitar los **perfiles de usuario de Microsoft Windows** (el verde está habilitado, el gris está deshabilitado).

4. Haga clic en **Guardar** o **Guardar y cerrar** para confirmar.

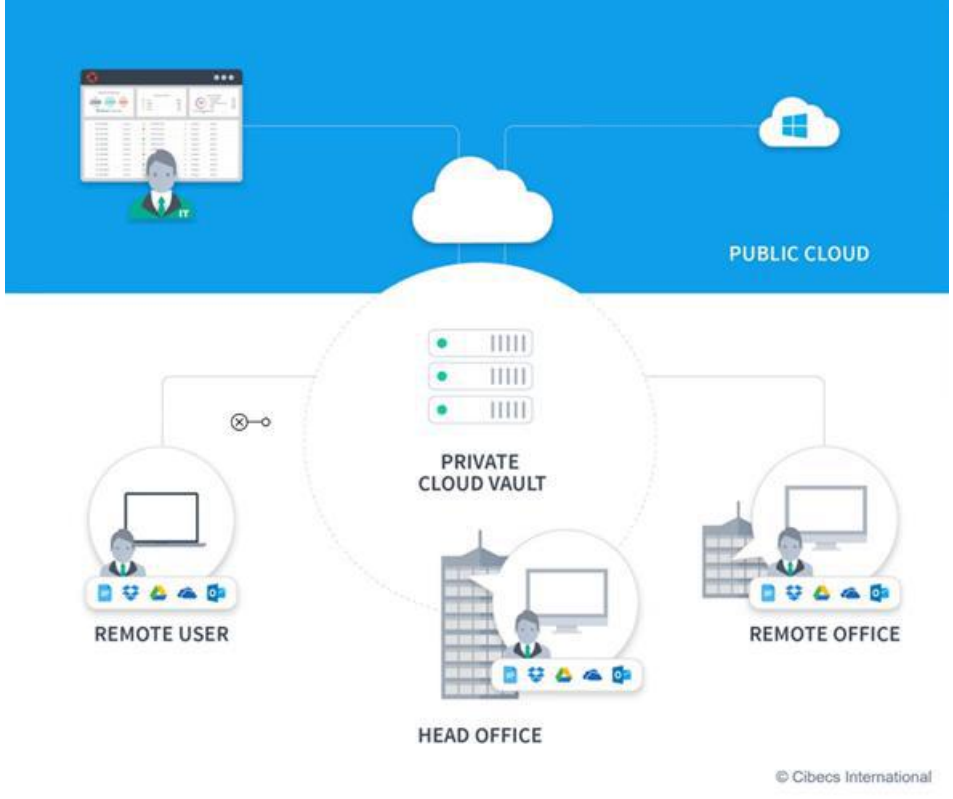
Para transferir la configuración del perfil de usuario de Windows de una máquina a otra, puede hacer una copia de seguridad manual del dispositivo que va a ser reemplazado. Luego inicie sesión en el nuevo dispositivo y realice una restauración y elija qué configuración de perfil y datos usar. Para obtener más información, consulte Migrar datos de perfil de usuario a un nuevo dispositivo.

Repositorios

Repositorios Descripción General

Un repositorio es un área de almacenamiento que se puede instalar en un servidor en sus instalaciones o en un servidor accesible de forma remota. Almacena datos de respaldo cifrados de sus dispositivos activados.

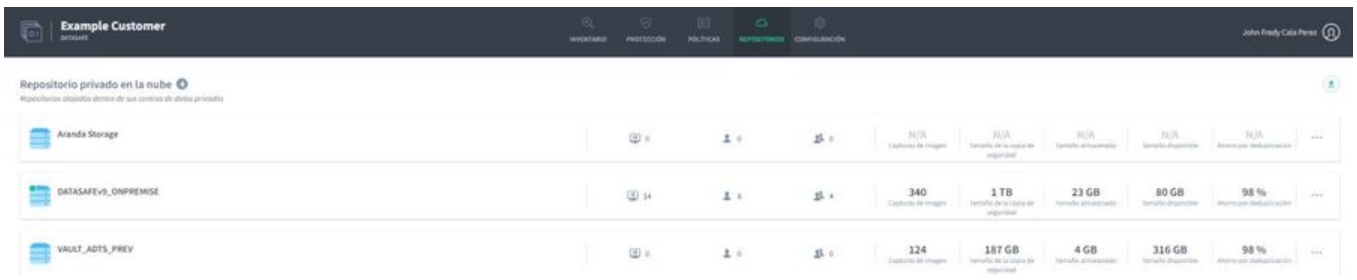
Para una máxima eficiencia, Aranda Datasafe utiliza la deduplicación a nivel de bloque en el lado de la fuente para garantizar que solo los datos que sean nuevos o que hayan cambiado se carguen en el repositorio. Los datos sin cambios ya existen el repositorio, por lo que no es necesario volver a cargarlos.



Repositorios

Puede utilizar la página repositorios para ver información sobre sus repositorios, que son áreas de almacenamiento para sus copias de seguridad.

Para mostrar la página repositorios, haga clic en repositorios en el banner superior.



La página de repositorios proporciona una lista de sus repositorios. Puede buscar en la lista repositorios por nombre y también puede descargar el instalador de repositorios y desconectar un repositorio .

Listado de repositorios

Campo	Descripción
Estado Online	- En línea: ícono verde - Sin conexión: ícono gris
Alias de repositorio	El nombre que se le dio al repositorio cuando se creó. Suele ser un nombre descriptivo que hace que el repositorio sea fácil de identificar.
Hostname de repositorio	El FQDN (nombre de dominio completo) de repositorio. Este nombre de host se utilizará para conectarse a un repositorio.
Dispositivos	La cantidad de dispositivos que están asociados con el repositorio por medio del Equipo al que pertenecen. Estos dispositivos realizarán una copia de seguridad en el repositorio asociada.
Usuarios	La cantidad de dispositivos que están asociados con el repositorio por medio del Equipo al que pertenecen. Estos usuarios tendrán sus datos respaldados en el repositorio asociada.
Equipos	La cantidad de equipos asignados al repositorio.
Instantánea	La cantidad de copias de seguridad que se han realizado para un repositorio. Un “snapshot” es una copia de seguridad realizada en un momento determinado.
Tamaño de Respaldo	El tamaño de los datos de respaldo antes de que se haya aplicado la deduplicación.
Respaldo Almacenado	La cantidad de espacio de almacenamiento utilizado para almacenar los datos de la copia de seguridad.
Ahorro Deduplicacion	La cantidad de espacio de almacenamiento ahorrado mediante el uso de la deduplicación, que se muestra como un porcentaje. En lugar de realizar una copia de seguridad de cada archivo cada vez, Aranda Datasafe solo realiza una copia de seguridad de los archivos que han cambiado desde la última copia de seguridad. Esto se llama deduplicación y significa que se requiere menos espacio para sus copias de seguridad y el proceso de copia de seguridad es más eficiente.

Instalar y configurar un repositorio

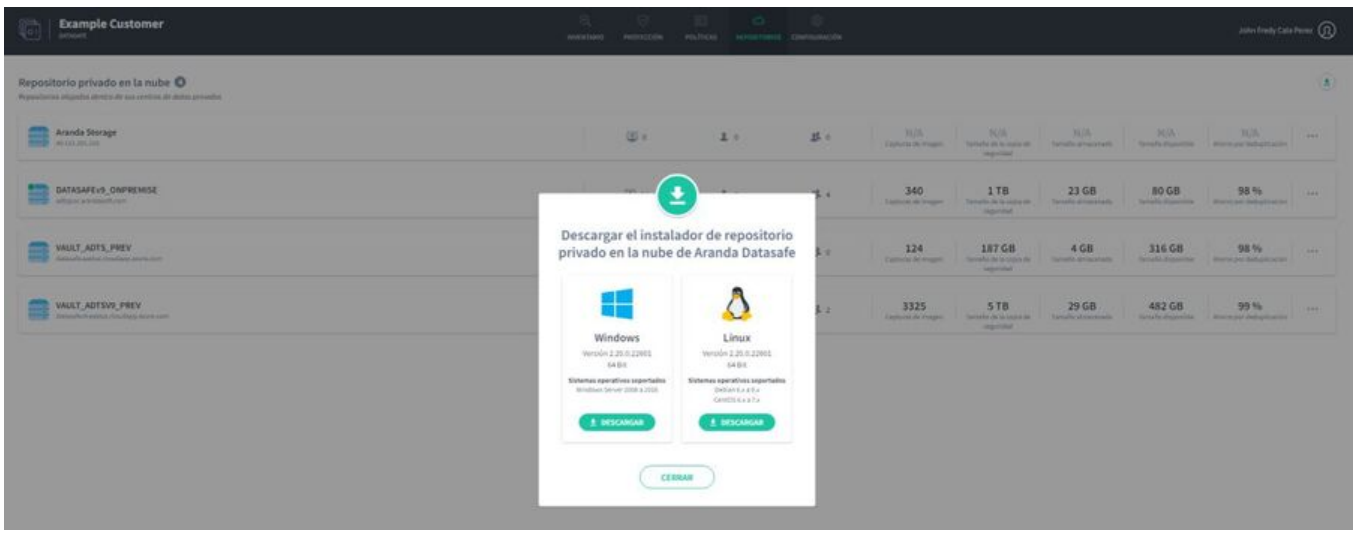
Para agregar un nuevo repositorio para almacenamiento, primero debe descargar el instalador de repositorio. Luego puede ejecutarlo en su servidor y registrarlo para que se conecte a Aranda Datasafe.

> ⚐ **Nota:** Para registrar un repositorio, deberá tener la dirección de correo electrónico y la contraseña de una cuenta de usuario de Aranda Datasafe con el rol de **Administrador o Oficial de Seguridad**.

Para descargar e instalar el paquete Private Cloud Vault:

1. Haga clic en **repositorios**.

2. Haga clic en Descargar **Private Cloud Vault**.



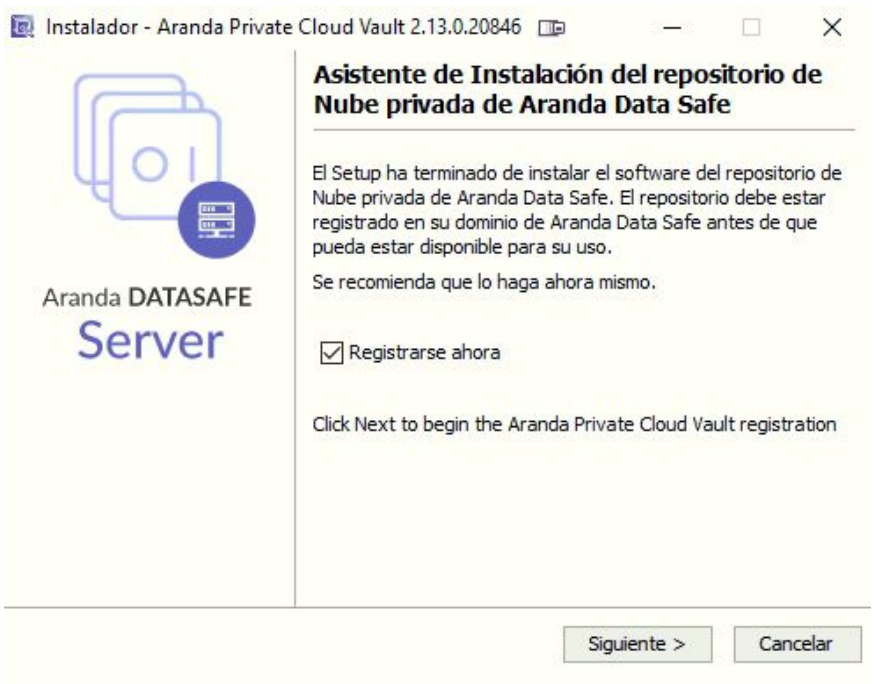
3. Cuando se descargue el paquete Private Cloud Vault, búsquelo en su computadora y cópielo en su servidor.

4. En el servidor, instale el software Private Cloud Vault. Puede instalarlo en la ubicación predeterminada o elegir otra ubicación si lo prefiere.

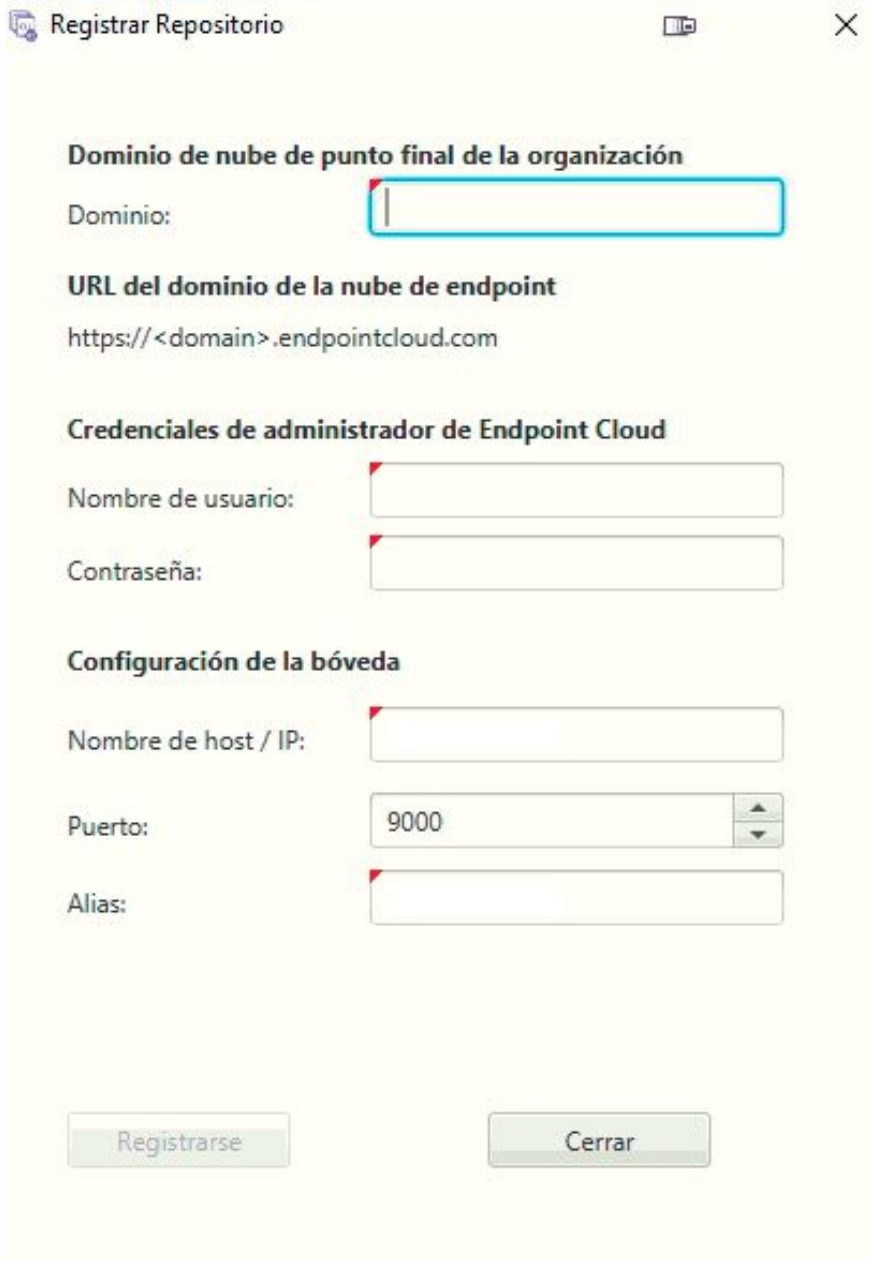
Importante: Debe elegir una ubicación que tenga una cantidad adecuada de espacio de almacenamiento para sus datos. Por lo general, recomendamos 20 GB por usuario, pero esto puede variar según el tipo y la cantidad de datos que utilice su organización.

Siga los pasos del asistente de instalación.

Cuando haya instalado el software, asegúrese de que Registrarse ahora esté marcado y luego haga clic en Siguiente.



5. Ingrese los detalles de registro:



Campo	Descripción
Dominio	El nombre de su tenant de Aranda Datasafe. Este suele ser el nombre de su organización y es la primera parte de la dirección de su Aranda Datasafe.
Nombre de usuario	Ingrese el nombre de usuario de una cuenta de Aranda Datasafe que tenga el rol de Administrador o Oficial de seguridad. Solo estas cuentas de usuario tienen permiso para registrar un repositorio.
Contraseña	Ingrese la contraseña para la cuenta de Aranda Datasafe.
Nombre de host / IP	ingrese el nombre o la dirección IP del servidor que tiene instalado el software de repositorio. Si el servidor está en una dirección de Internet, ingrese la URL en su lugar.
Puerto	9000. (El puerto debe establecerse en 9000).
Alias	Ingrese el nombre del repositorio como aparecerá en Aranda Datasafe.

Importante: Los agentes de descubrimiento y los agentes de protección deben poder comunicarse con el repositorio por el puerto 9000.

6. Haga clic en **Registrarse**.

Eliminar un repositorio

Si ya no necesita un repositorio, puede eliminarlo de Aranda Datasafe "separándolo". Cuando elimine un repositorio:

- Ya no puede restaurar dispositivos desde el repositorio eliminado
- El repositorio no se puede asignar a ningún Equipo (si tiene Equipos que usan el repositorio eliminado, deberá asignarles un repositorio diferente, de lo contrario, sus dispositivos no serán respaldados).

Para eliminar un repositorio:

1. Haga clic en **repositorios**.

2. Busque el repositorio que desea eliminar.

3. Seleccione el botón de opción (...) del repositorio y haga clic en **Eliminar repositorio**.

4. Para confirmar que desea eliminar el repositorio, ingrese DETACH en letras mayúsculas en el cuadro de diálogo.

5. Haga clic en Desconectar para eliminar el repositorio.

Administradores

Administradores Descripción General

Aranda Datasafe tiene un inicio de sesión seguro para evitar el acceso no autorizado. Para iniciar sesión, deberá tener una cuenta de administrador o una cuenta de oficial de seguridad .

Para obtener una cuenta, debe ser invitado a Aranda Datasafe por otro administrador . Recibirás la invitación por correo electrónico y puedes seguir el enlace para configurar tu cuenta.

Cuando inicie sesión, las funciones que están disponibles para usted dependerán del rol asignado a su cuenta. Pero todos los administradores y oficiales de seguridad pueden usar Aranda Datasafe

para monitorear, administrar y configurar el respaldo y la protección de los datos de su organización.

Administradores Configuración

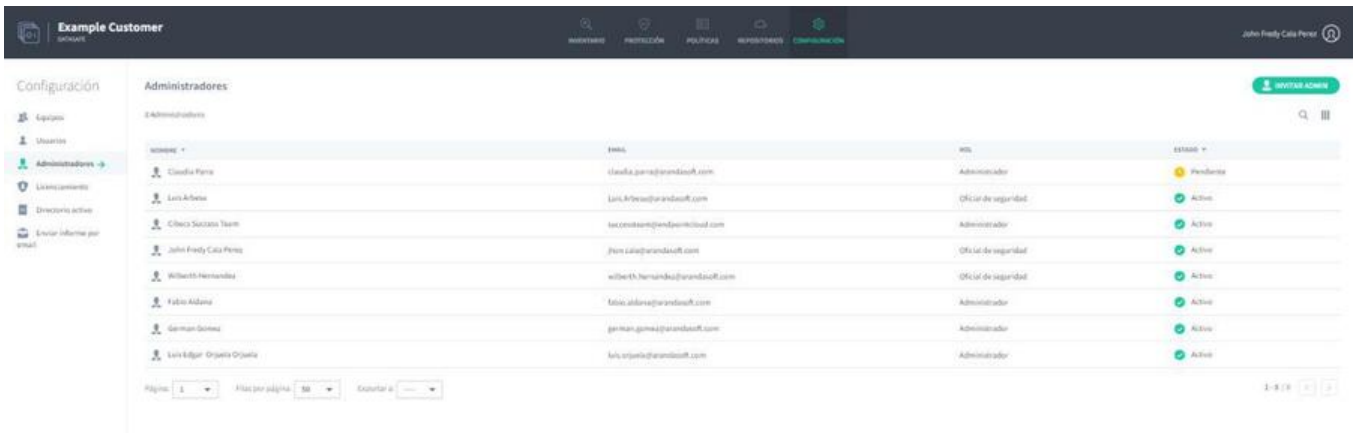
La página de **configuración** tiene una sección de **administradores **que puede utilizar para:

- Ver el nombre y la dirección de correo electrónico de cada administrador.
- Ver si alguien es un administrador o un oficial de seguridad de Aranda Datasafe
- Invite a alguien a convertirse en administrador de Aranda Datasafe
- Eliminar un administrador o un oficial de seguridad.

Para mostrar la sección Administradores:

1. Haga clic en **Configuración**.

2. En el panel lateral, haga clic en **Administradores**.



Para cada administrador, puede ver el:

Campo	Descripción
Nombre	El nombre del administrador.
Email	La dirección de correo electrónico utilizada para invitar al administrador a Aranda Datasafe.
Rol	El rol del administrador afecta las funciones que están disponibles para ellos. Los posibles roles son: **Oficial de seguridad**: tiene todos los permisos de administradores y también puede descargar y registrar AD Connector, y puede cambiar la función de los administradores. El oficial de seguridad tiene la clave para los datos de respaldo de la organización. Se recomienda que se implementen al menos dos oficiales de seguridad por tenant del cliente. **Administrador**: tiene acceso a todas las funciones de Aranda Datasafe, pero no puede descargar ni registrar AD Connector ni cambiar la función de los administradores.
Estado	Muestra si el administrador ha activado su cuenta (Activa) o aún no ha respondido a la invitación por correo electrónico (Pendiente).

Si coloca el cursor sobre un administrador, puede seleccionar su menú contextual (...). Desde aquí puedes:

- Asignar permisos de oficial de seguridad a un administrador activo La opción Asignar oficial de seguridad solo está disponible si inicia sesión como oficial de seguridad.
- Eliminar un administrador.

Invitar Administrador

Si desea darle acceso a alguien a Aranda Datasafe, puede invitarlo a unirse como administrador. Cuando envía la invitación, Aranda Datasafe crea un nuevo usuario de nivel de administrador automáticamente y envía un correo electrónico al nuevo usuario. Pueden usar el correo electrónico para activar su cuenta.

Para invitar a un nuevo administrador:

1. Haga clic en **Configuración**.

2. Haga clic en **Administradores**.

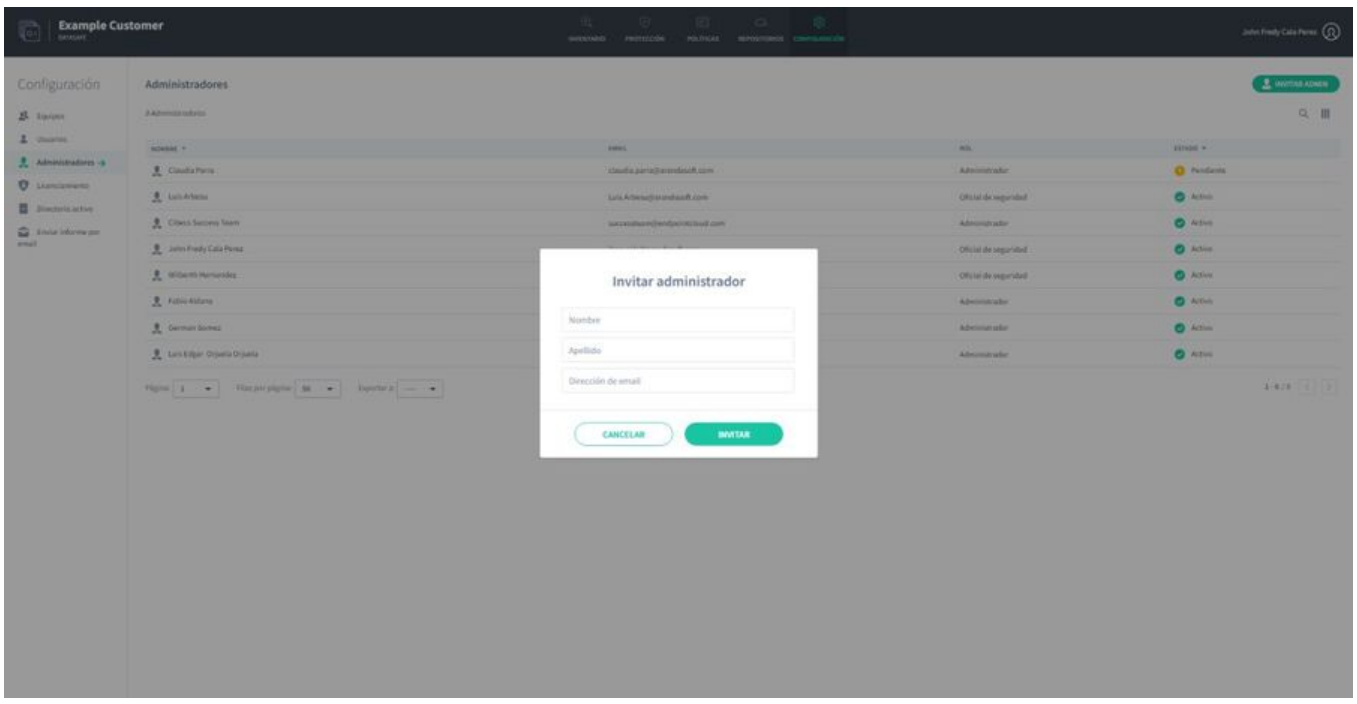
3. Haga clic en **Invitar administrador**.

4. En el cuadro de diálogo Invitar administrador, ingrese el nombre, apellido y dirección de correo electrónico del usuario que desea agregar como administrador.

5. Haga clic en **Invitar**.

El usuario recibirá una invitación por correo electrónico. Cuando reciben el correo electrónico, pueden usarlo para activar su cuenta. Una vez activados, podrán iniciar sesión en Aranda Datasafe y acceder a las funciones de nivel de administrador.

Para obtener más información sobre la invitación por correo electrónico, consulte Activar su cuenta.



Activar Cuenta

Si vas a utilizar Aranda Datasafe, deberías recibir un correo electrónico invitándote a activar tu cuenta.

Si no recibe el correo electrónico, revise sus carpetas de correo no deseado y correo no deseado. Si aún no puede encontrar el correo electrónico, comuníquese con el servicio de soporte de Aranda.

Cuando tenga el correo electrónico, haga clic en **Activar cuenta**. Su navegador abre la página web de activación. La primera vez que acceda a Aranda Datasafe, debe ingresar una contraseña y luego volver a ingresarla para confirmar. Haga clic en **Activar** para iniciar sesión.

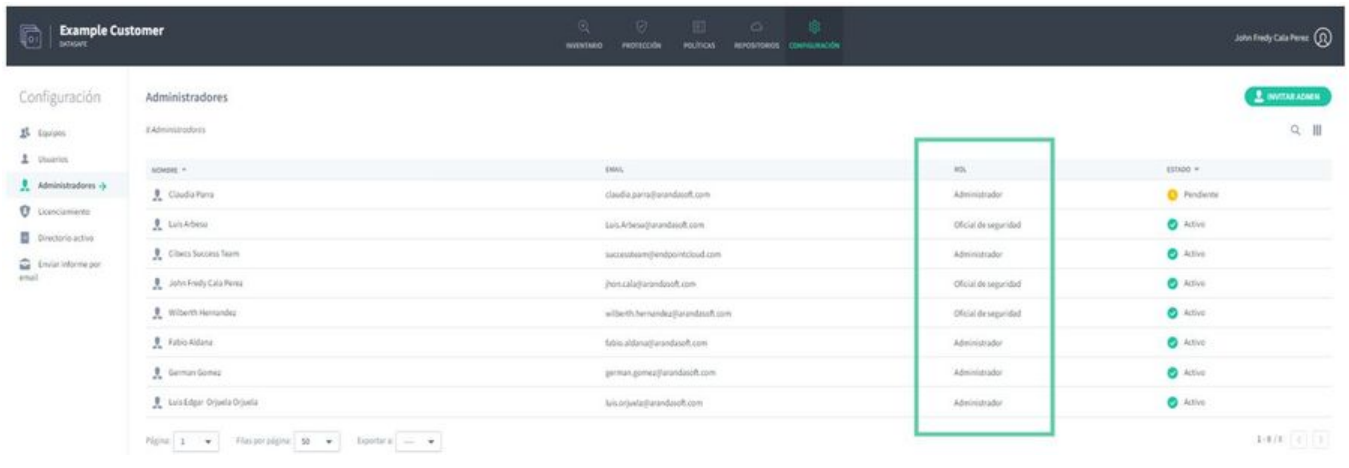
Rol de Administrador

Cuando activa una invitación para unirse a Aranda Datasafe, se le da una cuenta automáticamente. La cuenta tiene una función, ya sea de**administrador** o de**oficial de seguridad**.

Si se le otorga una cuenta de administrador, puede acceder a todas las funciones de Aranda Datasafe**pero no puede descargar y registrar AD Connector**.

Solo las personas con el rol de oficial de seguridad pueden descargar y registrar AD Connector.

Puede ver su función en la sección**Administradores** en la página**Configuración** (consulte Administradores - Página Configuración).



Rol oficial de Seguridad

El rol de**Oficial de seguridad** es el rol de mayor rango. Los usuarios con este rol tienen acceso a una gama más amplia de funciones en Aranda Datasafe que otros usuarios, por lo que debe tener cuidado al asignar este rol.

Los oficiales de seguridad son los únicos usuarios que pueden:

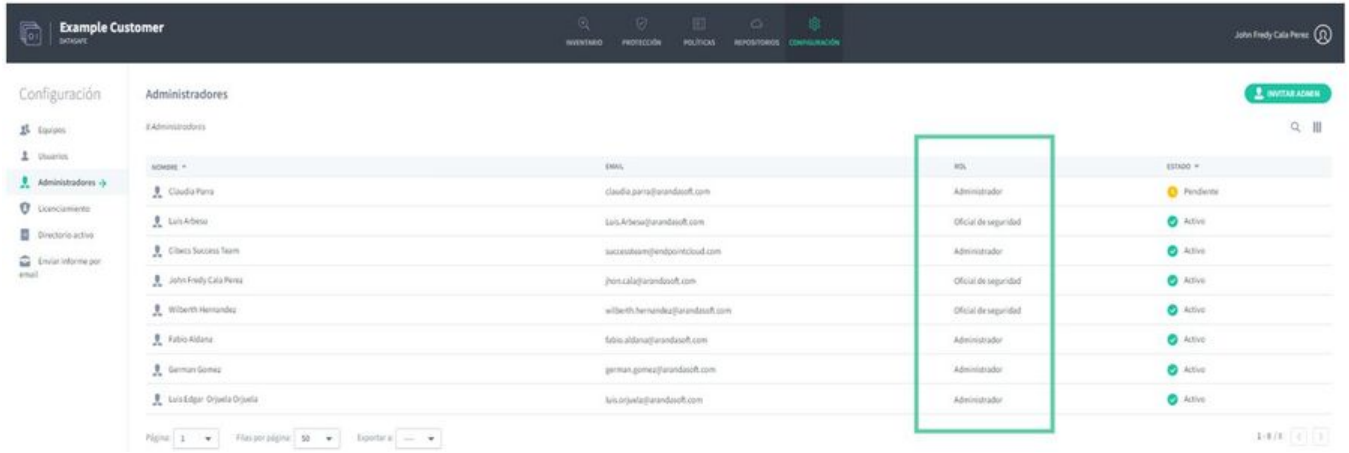
- Descargue y registre el conector AD. Esto es necesario para permitir que Aranda Datasafe proteja sus dispositivos y datos.
- Permitir el acceso a datos cifrados, necesarios para restaurar los datos de un usuario.

Aranda Datasafe debe tener al menos un usuario con el rol de**Oficial de Seguridad**.

Para verificar si su cuenta de usuario tiene el rol de**Oficial de seguridad**:

1. Haga clic en **Configuración**.

2. Haga clic en**Administradores**.



3. Busque su cuenta de usuario en la lista y vea si tiene el rol de**Oficial de seguridad**.

Solo los usuarios con el rol de**Oficial de seguridad** pueden cambiar el rol de una cuenta de usuario.

Cambiar Función de Cuenta

Si inicia sesión como oficial de seguridad, puede cambiar el rol de una cuenta de administrador. Esto es útil cuando desea actualizar un administrador a oficial de seguridad, para que pueda registrar el conector AD y restaurar los datos de los usuarios.

Para cambiar el rol de una cuenta:

1. Inicie sesión como oficial de seguridad.

2. . Haga clic en**Configuración**.

3. Haga clic en **Administradores**.

4. Haga clic en el botón de contexto (...) del administrador que desea cambiar.

5. Haga clic en **Asignar oficial de seguridad**.

6. Ingrese su contraseña para confirmar el cambio.

Eliminar un administrador o un oficial de seguridad

Si inicia sesión en Aranda Datasafe como oficial de seguridad, puede eliminar otras cuentas de administrador y oficial de seguridad. Por lo general, solo eliminará las cuentas que ya no estén en uso, por ejemplo, si un miembro del personal ha dejado la organización.

Precaución: Si elimina una cuenta, el usuario de esa cuenta no podrá iniciar sesión en Aranda Datasafe.

Para eliminar un administrador o un oficial de seguridad:

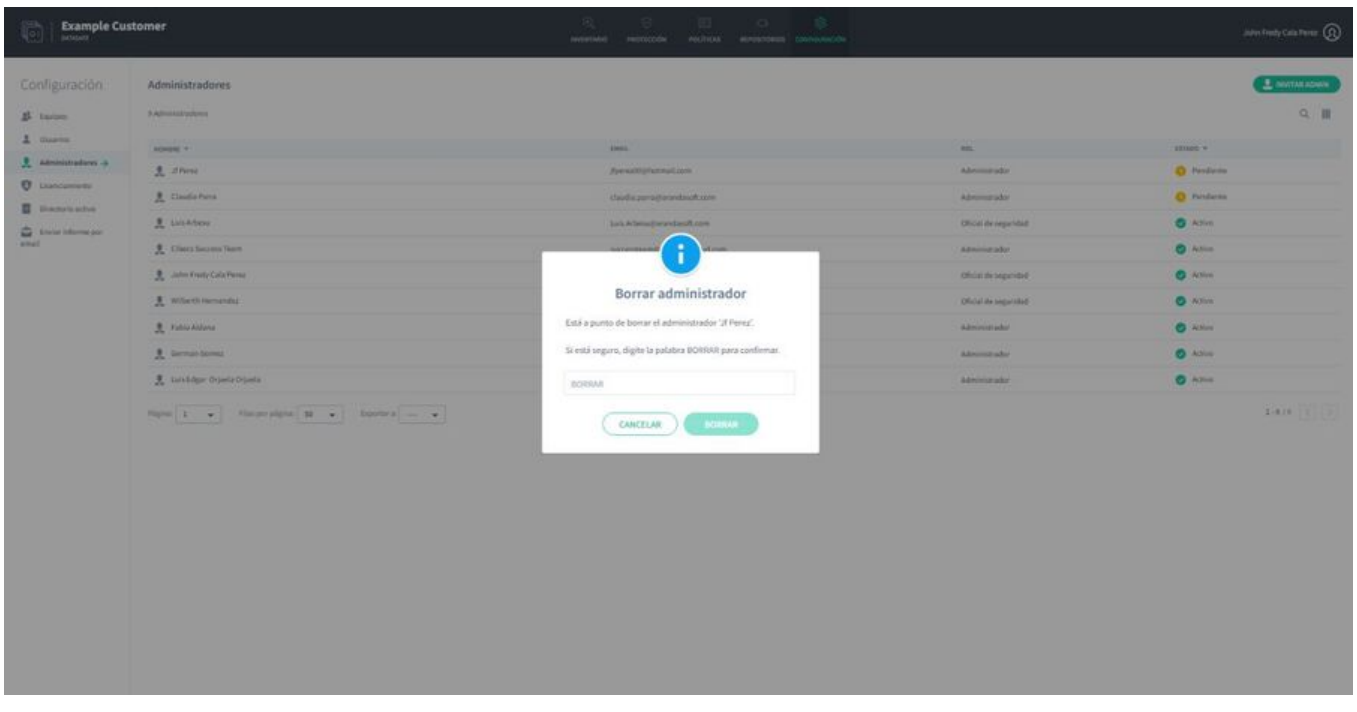
1. Haga clic en **Configuración**.

2. Haga clic en**Administradores**.

3. Haga clic en el botón de contexto (...) del administrador o oficial de seguridad que desea eliminar.

4. Haga clic en**Eliminar**.

5. Escriba Eliminar en el cuadro de diálogo para confirmar y luego haga clic en**Eliminar**.



Equipos

Equipos

En Aranda Datasafe, necesita organizar sus dispositivos en equipos. Por lo general, los usuarios de Aranda Datasafe crean equipos para grupos significativos, como departamentos en una empresa o las ubicaciones geográficas de diferentes instalaciones. Pero no hay limitaciones: puede crear equipos para cualquier agrupación que desee.

Cuando Aranda Datasafe descubre sus dispositivos por primera vez, están "sin asignar". Esto significa que no están en un equipo.

Necesita crear sus propios equipos para poder:

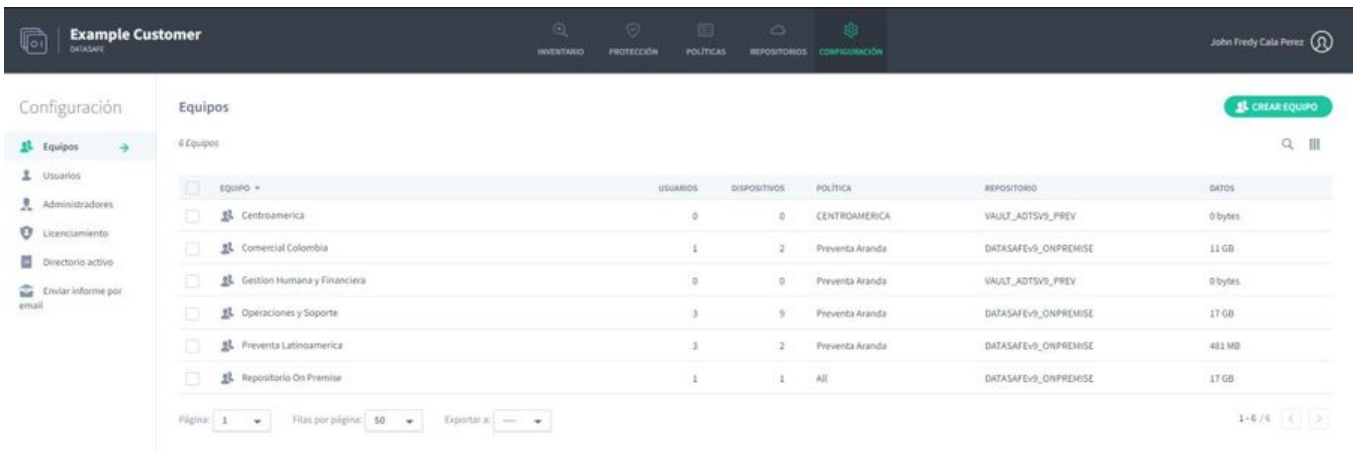
- Asignar una **política** al equipo. Una política es un conjunto de reglas que definen:
    - Qué datos están protegidos y respaldados
    - Con qué frecuencia ocurren las copias de seguridad
    - Si se utiliza alguna función de **prevención de pérdida de datos** para proteger sus datos en caso de pérdida o robo de un dispositivo. Estos incluyen **cifrado local, prevención de robo de datos y geolocalización**.
    - Si se puede hacer una copia de seguridad de los datos del perfil de usuario de Windows para **migrarlos** a otros dispositivos.
- Asignar un área de almacenamiento **(repositorio)**. El repositorio es un área de almacenamiento en un servidor y Aranda Datasafe la usa cuando hace una copia de seguridad de los dispositivos del Equipo.
- Ver y filtrar información sobre dispositivos en equipos específicos.

Para crear, editar y ver equipos, puede usar la página de **Inventario**, la página de **Protección** o la página de **Configuración** (que tiene una sección de **Equipos**).

Equipos Configuración

Puede usar la sección **Equipos** en la página **Configuración** para ver, editar y eliminar sus Equipos.

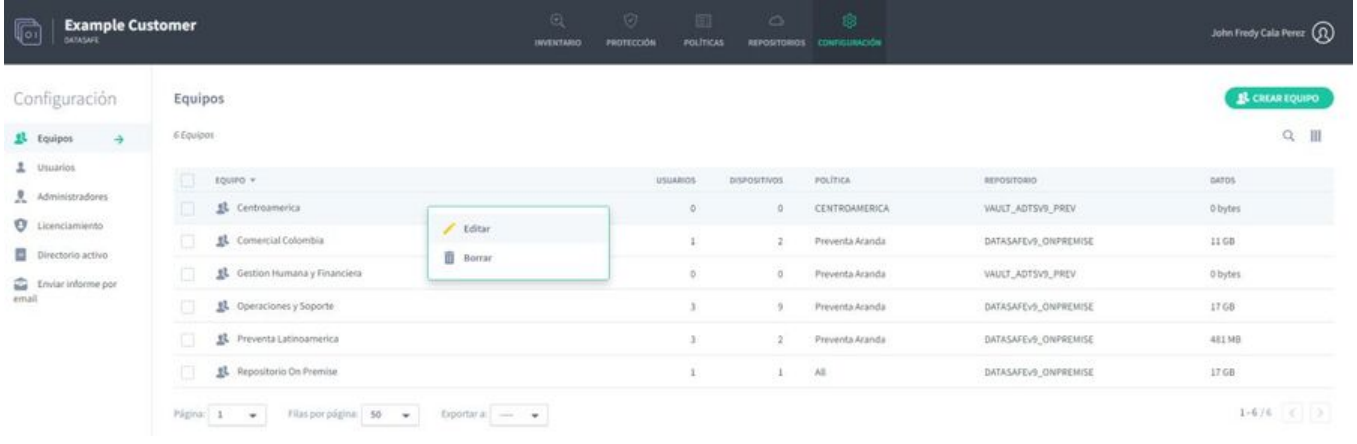
Para mostrar la sección **Equipos**, haga clic en Configuración. La sección Equipos se muestra de forma predeterminada (si es necesario, puede mostrarla haciendo clic en Equipos en la barra lateral).



Para cada equipo, puede ver:

Campo	Descripción
Usuarios	El número de usuarios en el equipo
Dispositivos	La cantidad de dispositivos asignados al equipo.
Política	La Política que se asigna al Equipo. Una política es un conjunto de reglas que definen: - Qué datos están protegidos y respaldados - Con qué frecuencia ocurren las copias de seguridad - Si se utiliza alguna función de **prevención de pérdida de datos** para proteger sus datos en caso de pérdida o robo de un dispositivo. Estos incluyen **cifrado local, prevención de robo de datos y geolocalización**. - Si se puede realizar una copia de seguridad de los datos del perfil de usuario de Windows para **migrarlos** a otros dispositivos.
Repositorio	El repositorio asignado al equipo. El repositorio es un área de almacenamiento en un servidor y Aranda Datasafe la usa cuando hace una copia de seguridad de los dispositivos del equipo.
Data	La cantidad de espacio de almacenamiento utilizado para hacer una copia de seguridad de los datos del equipo.

Si ubica el cursor sobre un equipo, puede seleccionar su menú contextual (...). Desde aquí, puede editar el equipo o eliminarlo.



Filtrado de Equipos Configuración

De forma predeterminada, la sección **Equipos** en la página **Configuración** muestra información para todos los equipos y dispositivos. Pero, si es necesario, puede filtrar la sección **Equipos** para que solo muestre información que cumpla con ciertos criterios. Por ejemplo, puede utilizar la búsqueda para filtrar la sección Equipos de modo que solo muestre información de los dispositivos de un **equipo** en particular.

Hay varias formas de filtrar la sección Equipos:

Utilice una búsqueda para filtrar la lista de equipos.

Mostrar u ocultar columnas en la lista de equipos

Utilice una búsqueda para filtrar la lista de equipos

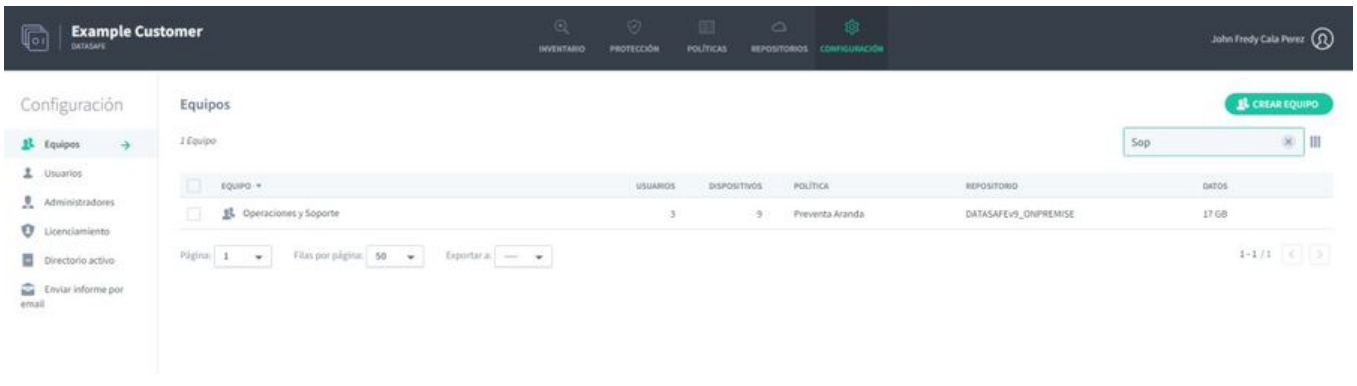
Puede usar la función de **búsqueda** para filtrar la lista de equipos de modo que solo incluya equipos que tengan ciertos valores. Por ejemplo, puede usar la búsqueda para filtrar la lista de modo que solo muestre los equipos que están asociados con un repositorio en particular.

Puede usar la búsqueda para filtrar la lista de **equipos** por cualquier valor de texto, incluido el nombre del **equipo**, el nombre de la **política** y el nombre del **repositorio**.

Para aplicar un filtro de búsqueda:

1. Haga clic en el ícono de búsqueda que se encuentra sobre la lista de equipos.

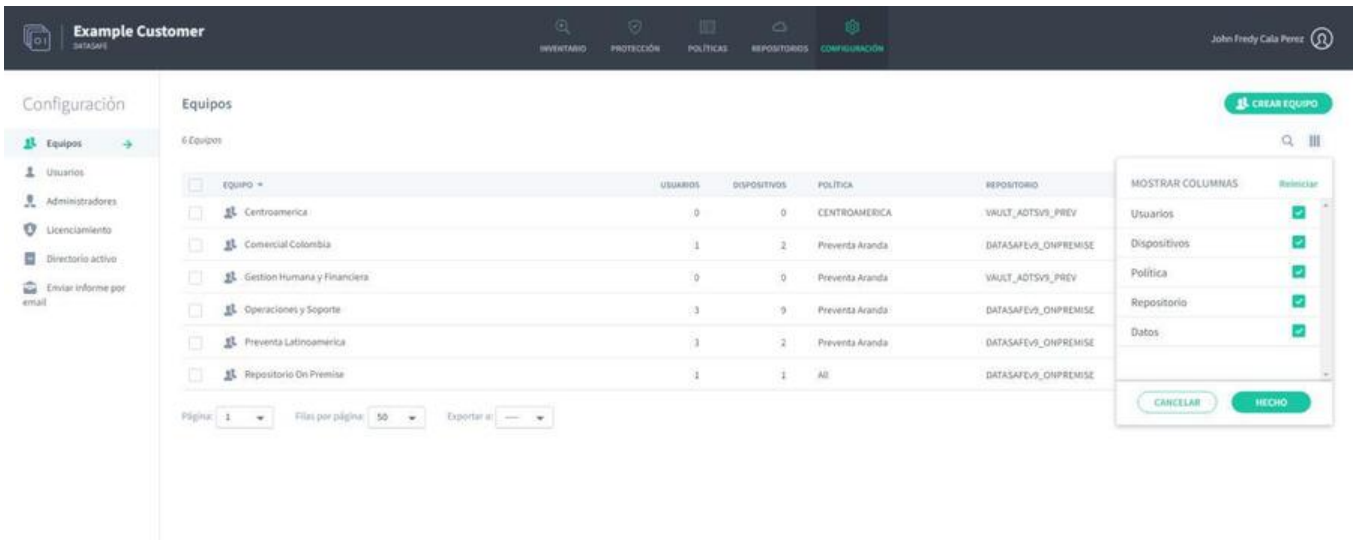
2. Ingrese los primeros caracteres del valor de texto que desea usar como filtro. Aranda Datasafe aplica el filtro a medida que escribe, por lo que puede hacer coincidencias parciales o puede ingresar el valor de texto completo para ser más específico.



Mostrar u ocultar columnas en la lista de equipos

Puede optar por mostrar u ocultar columnas en la lista de equipos. Por ejemplo, es posible que no le interese qué repositorio usa cada equipo, por lo que puede ocultar la columna repositorio.

Para mostrar / ocultar columnas, haga clic en el ícono Columnas y luego elija qué columnas incluir.



Ver Dispositivos en Equipo

Puede utilizar las páginas de **Inventario** o **Protección** para ver información sobre los dispositivos en cualquier Equipo.

1. Haga clic en Inventario o Protección.

2. En la sección Equipos, haga clic en:

- **Todos los dispositivos** para mostrar información sobre todos los dispositivos en todos los equipos
- **Sin asignar** para mostrar información solo para aquellos dispositivos que aún no están asignados a un equipo
- para mostrar información sobre los dispositivos de un equipo específico.

Cuando hace clic en una opción de Equipo, la página de **Inventario** o **Protección** se actualiza y las pantallas del tablero y la lista se filtran para mostrar solo información sobre los dispositivos en el Equipo seleccionado.

Haga clic en **Todos los dispositivos** en la barra lateral de **Equipos** para eliminar el filtro.

Crear un Equipo

Aranda Datasafe utiliza Equipos para organizar sus dispositivos en grupos.

Cada equipo tiene una:

- **Política**: define cuándo se hará una copia de seguridad de los dispositivos del equipo y también qué configuración de migración y prevención de pérdida de datos usarán los dispositivos.
- **Repositorio**: define dónde se almacenarán los datos de respaldo de los dispositivos del equipo.

Cuando crea un equipo, elige una política y un repositorio. También puede editar un Equipo para cambiar su nombre o asociarlo con una Política o repositorio diferente.

Crear un equipo

Puede crear un nuevo equipo y luego asignarle una política y un repositorio. Cuando el equipo está configurado, puede asignarlo sus dispositivos.

Debería crear un nuevo equipo si:

- No hay equipos en Aranda Datasafe
- Los equipos existentes no cumplen con sus requisitos, por ejemplo, no usan la prevención de robo de datos, pero usted la necesita para sus dispositivos.
- Los equipos existentes realizan una copia de seguridad en un repositorio que no es adecuado para sus dispositivos.

Para crear un equipo:

1. Hay tres formas de crear un equipo: desde la página **Inventario**, la página **Protección** o desde la sección **Equipos** en la página Configuración. Entonces puede:

Hacer clic en **Inventario**.

o:

Hacer clic en **Protección**.

o:

Hacer clic en **Configuración** y use la sección **Equipos**.

2. Haga clic en Crear equipo (esquina inferior izquierda de la pantalla Inventario o Protección, esquina superior derecha en la página Equipos - Configuración).

3. Ingrese un nombre para el nuevo equipo.

4. Utilice el cuadro combinado **Asignar una política** para elegir la Política para el equipo. Todos los dispositivos del Equipo utilizarán la configuración definida en la Política (programación de copias de seguridad, configuración de prevención de pérdida de datos, etc.).

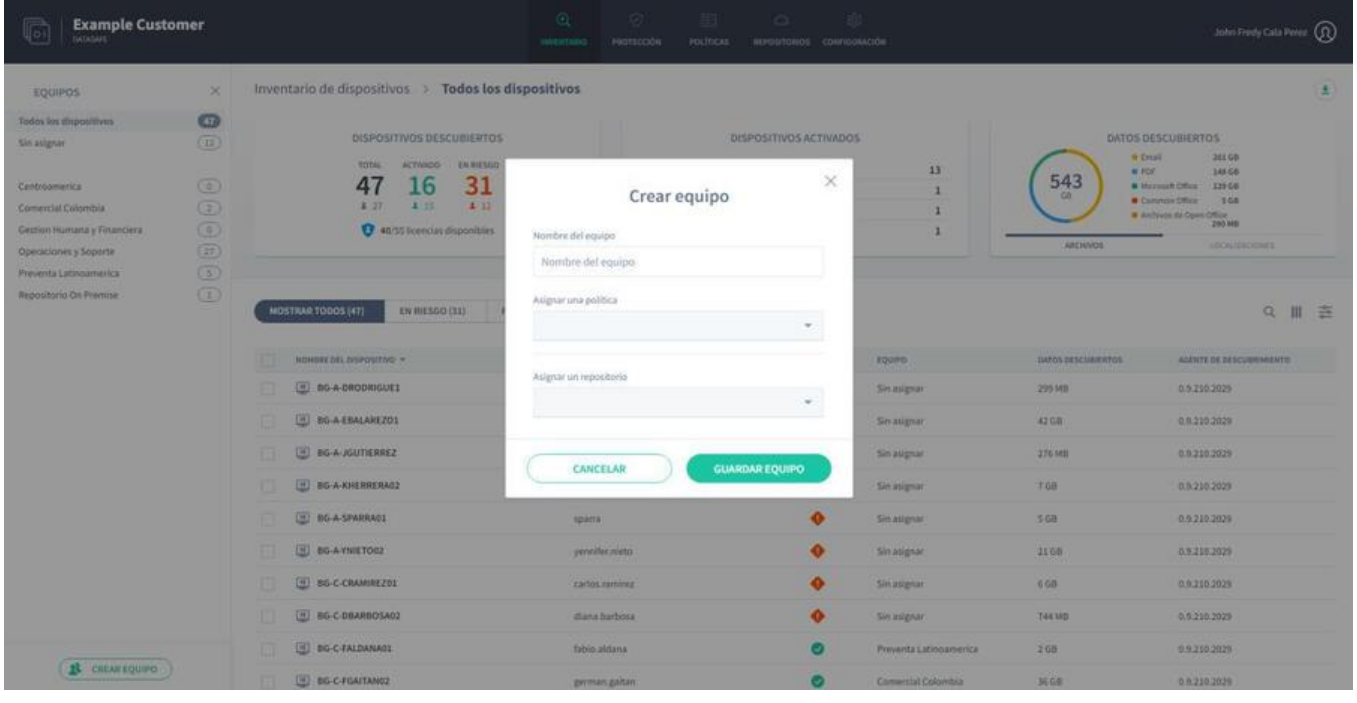
5. Utilice el cuadro combinado **Asignar un repositorio** para elegir el área de almacenamiento que se usará para almacenar los datos de respaldo para los dispositivos en el equipo.

6. Haga clic en **Guardar equipo**.

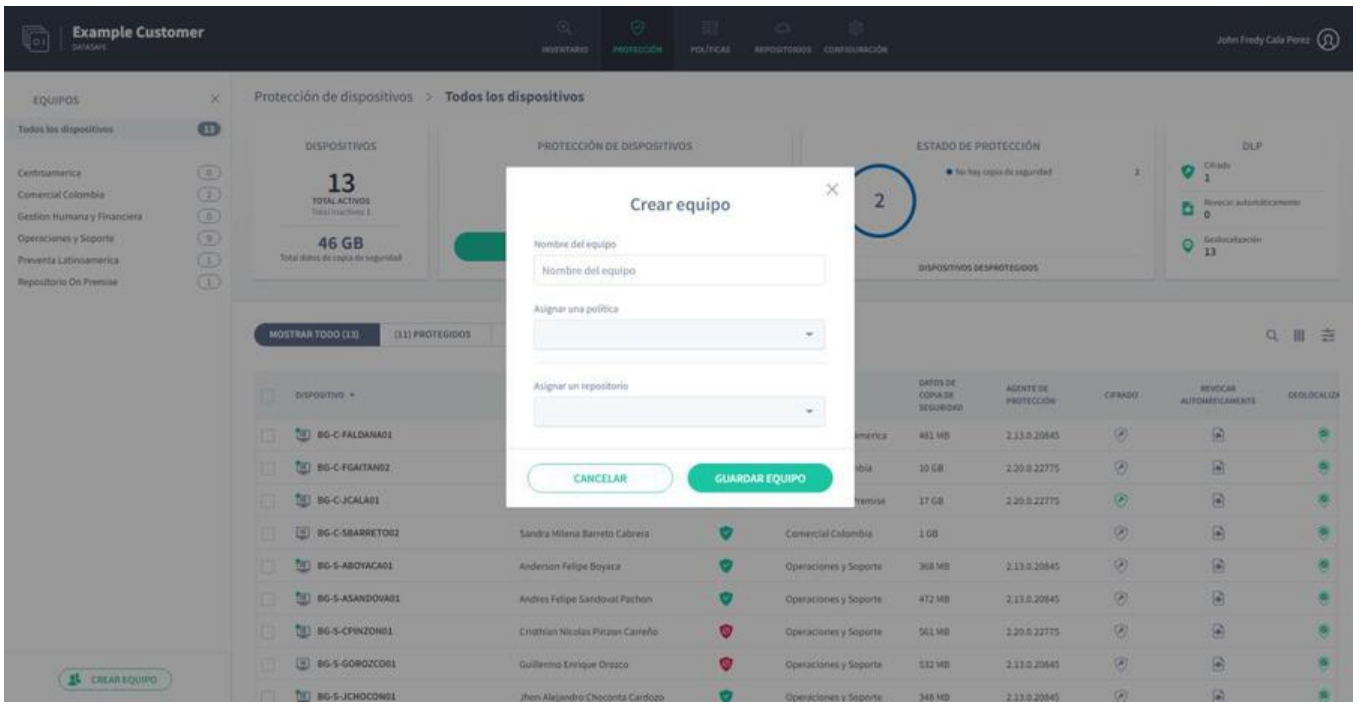
Su nuevo equipo aparece en la sección **Equipos** de la página **Inventario** y la página Protección. También aparece en la lista de **equipos** en la página **Configuración**).

7. Repita los pasos 2 a 6 inclusive para crear tantos equipos nuevos como necesite.

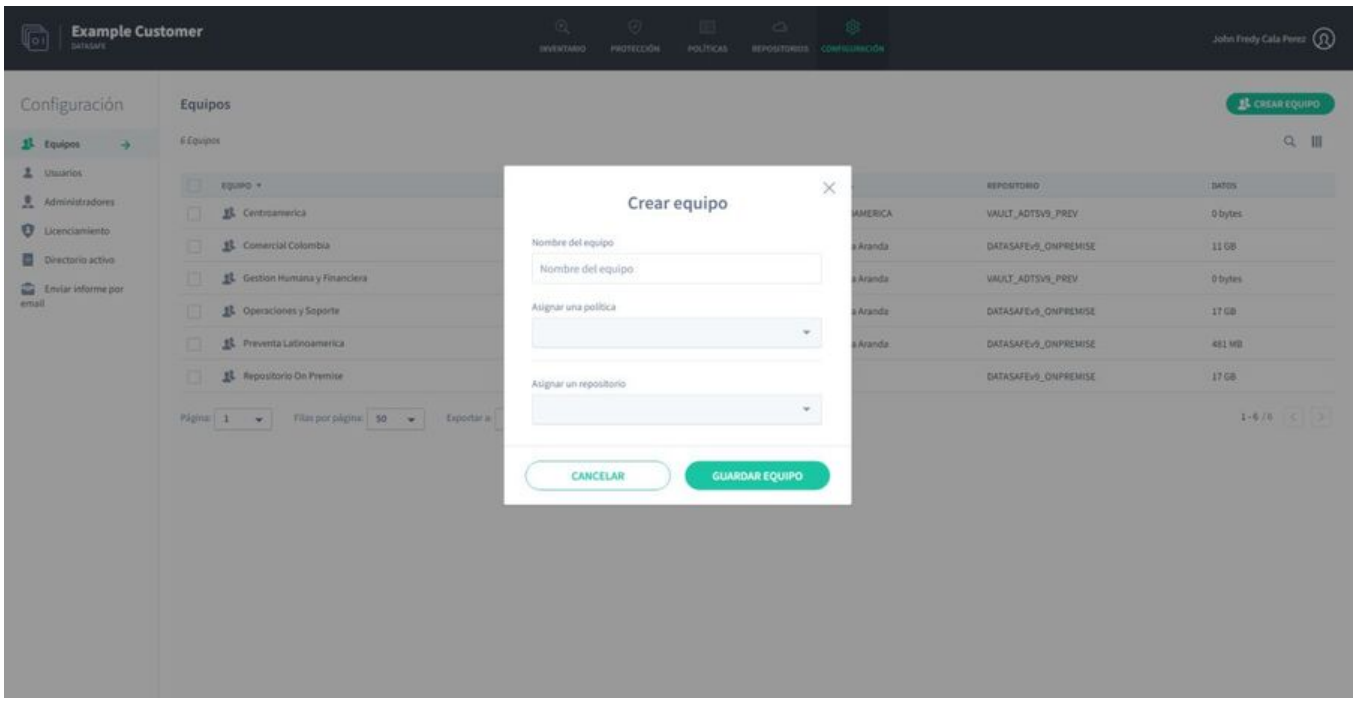
Creación de un equipo a partir del inventario:



Creando un equipo desde la página de Protección:



Creando un equipo desde la página de Configuración:



Editar un Equipo

Si desea realizar cambios en un equipo existente:

1. Hay tres formas de editar un equipo: desde la página **Inventario**, la página **Protección** o desde la sección **Equipos** en la página **Configuración**. Entonces puede:

Hacer clic en **Inventario**.

o:

Hacer clic en **Protección**.

o:

Hacer clic en **Configuración** y use la sección **Equipos**.

2. Pase el cursor sobre el equipo que desea editar y luego haga clic en su botón de opción (...).

3. Haga clic en **Editar**.

4. Utilice el campo **Nombre del equipo** para cambiar el nombre del equipo, si es necesario.

5. Utilice el cuadro combinado **Asignar una política** para elegir la Política para el equipo. Todos los dispositivos del Equipo utilizarán la configuración definida en la Política (programación de copias de seguridad, configuración de prevención de pérdida de datos, etc.).

6. Utilice el cuadro combinado **Asignar un repositorio** para elegir el área de almacenamiento que se usará para almacenar los datos de respaldo para los dispositivos en el Equipo.

7. Haga clic en **Guardar equipo**.

Asignar Políticas a Equipos

Puede asignar una política a cada uno de sus equipos. Una política es un conjunto de reglas que definen:

- Qué datos están protegidos y respaldados
- Con qué frecuencia ocurren las copias de seguridad
- Si se utiliza alguna función de **prevención de pérdida de datos** para proteger sus datos en caso de pérdida o robo de un dispositivo. Estos **incluyen cifrado local, prevención de robo de datos y geolocalización**.
- Si se puede realizar una copia de seguridad de los datos del perfil de usuario de Windows para migrarlos a otros dispositivos.

Normalmente, asigna una política a un equipo cuando crea el equipo por primera vez. Pero también puede editar un equipo para que use una política diferente:

1. Haga clic en **Inventario** o **Protección**.

2. Pase el cursor sobre el nombre del equipo y luego haga clic en el botón de opción (...).

3. Haga clic en **Editar**.

4. Utilice el cuadro combinado **Asignar una política** para cambiar la política del equipo.

5. Haga clic en **Guardar equipo**.

Asignar Repositorio a un Equipo

Puede asignar un repositorio a cada uno de sus equipos. Un repositorio es un área de almacenamiento en un servidor, y es donde Aranda Datasafe almacenará los datos de respaldo para todos los dispositivos en un equipo.

Normalmente, asigna un repositorio a un equipo cuando crea el equipo por primera vez. Pero también puede editar un equipo para que use un repositorio diferente:

1. Haga clic en **Inventario** o **Protección**.

2. Pase el cursor sobre el nombre del equipo y luego haga clic en el botón de opción (...).

3. Haga clic en **Editar**.

4. Utilice el cuadro combinado **Asignar un repositorio** para cambiar el repositorio del equipo.

5. Haga clic en **Guardar equipo**.

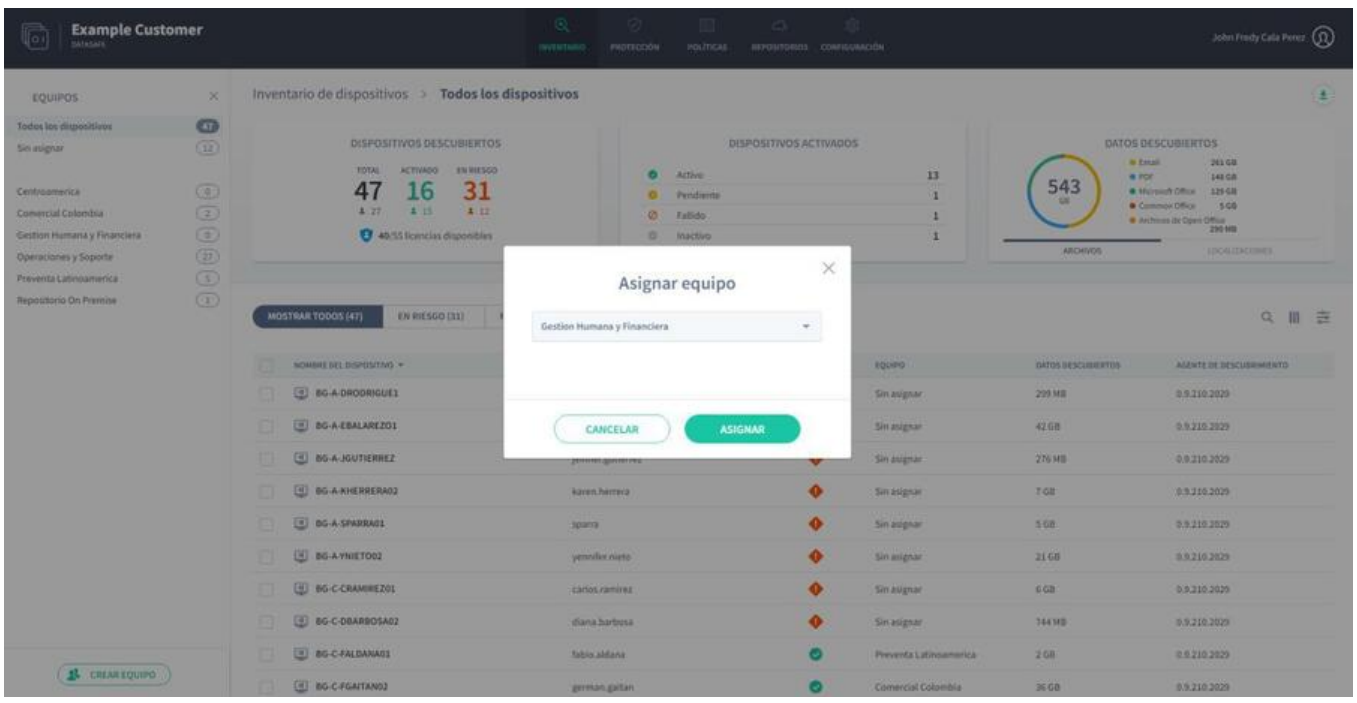
Asignar Dispositivo a un Equipo

Para usar Aranda Datasafe para hacer una copia de seguridad y proteger un dispositivo, el dispositivo debe estar asignado a un Equipo. El equipo está asociado con una política y un repositorio, y estos definen:

- Cuando se realiza una copia de seguridad de los dispositivos
- Qué configuración de Prevención de pérdida de datos se utiliza
- Qué configuraciones de migración se utilizan
- Dónde se almacenan los datos de la copia de seguridad.

Todos los dispositivos de ese equipo utilizan la configuración del equipo. Para asignar un dispositivo a un equipo:

1. Haga clic en **Inventario** o **Protección**.
2. Pase el cursor sobre un dispositivo en la lista de dispositivos.
3. Haga clic en el botón de opción del dispositivo (...).
4. Haga clic en **Asignar equipo**.
5. Asigne el dispositivo a un equipo de la lista.
6. Haga clic en **Asignar**.



La página se actualizará automáticamente y, después de una breve pausa, el dispositivo se asignará a su equipo seleccionado. Ahora puede utilizar la página de **Inventario** o **Protección** para ver información sobre:

- Todos los dispositivos
- Dispositivos no asignados
- Dispositivos en cada uno de sus equipos.

Eliminar Equipo

Puede haber ocasiones en las que necesite eliminar un equipo de Aranda Datasafe. Por ejemplo, es posible que desee eliminar un Equipo si su organización se ha reestructurado o algunos Equipos en Aranda Datasafe ya no existen en su negocio o se han fusionado con otros Equipos.

Si ya no necesita un equipo, puede eliminarlo de su Aranda Datasafe. Cuando elimina un equipo, Aranda Datasafe:

- Elimina el equipo
- Elimina todos los dispositivos asignados al equipo.

Importante: Si desea conservar los dispositivos, debe asignarlos a un equipo diferente antes de realizar la eliminación.

Para eliminar un equipo:

1. Haga clic en **Inventario** o **Protección**.
2. Pase el cursor sobre el Equipo que desea eliminar y luego haga clic en su botón de opción (...).
3. Haga clic en **Eliminar**.
4. Ingrese ELIMINAR en letras mayúsculas y luego haga clic en **Eliminar** para confirmar que desea eliminar el Equipo

Usuarios

Cuando Aranda Datasafe descubre sus dispositivos, crea automáticamente información sobre las cuentas y los dispositivos de los usuarios. Esta información se muestra en varias pantallas, incluida la página Inventario, la página Protección y la página Configuración.

Las cuentas de usuario y la información del dispositivo se muestran como:

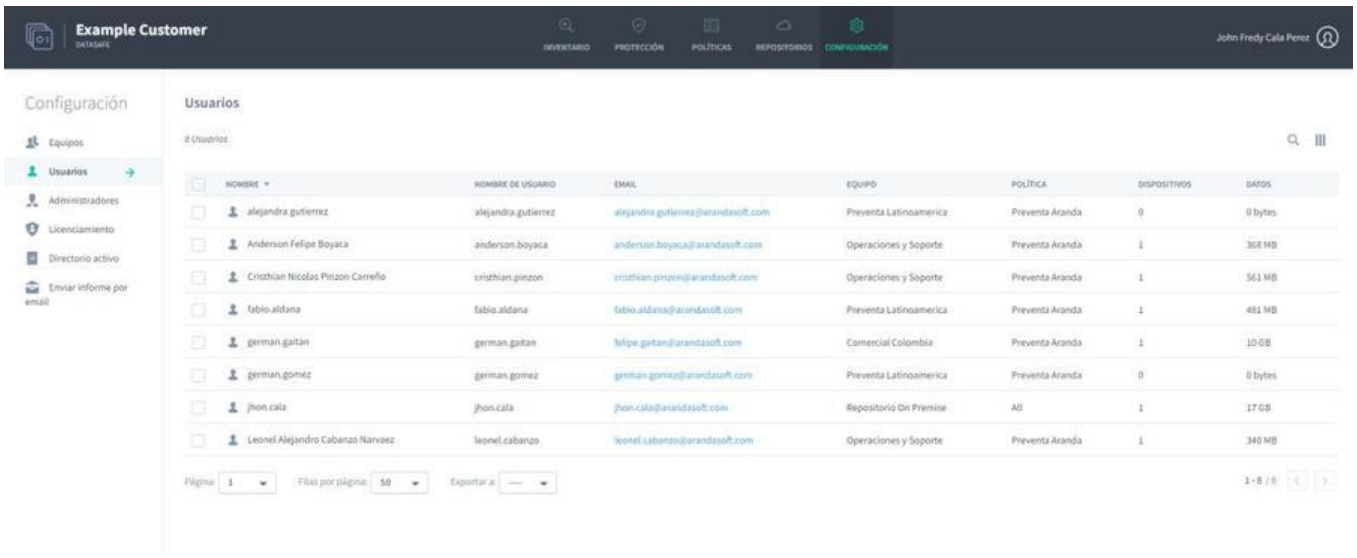
- **Usuario**: un usuario representa un perfil de usuario de Microsoft Windows. Durante el proceso de descubrimiento, Aranda Datasafe se conecta con los dispositivos que están configurados para ser protegidos y recupera la información del perfil del usuario. Crea un usuario para cada perfil de usuario de Windows (normalmente, esto significa un usuario por persona).
- **Nombre del dispositivo**: cada usuario tiene uno o más dispositivos de usuario. Por ejemplo, un usuario podría tener una computadora de escritorio y una computadora portátil. Aranda Datasafe utiliza la información del perfil de usuario de Microsoft Windows para hacer coincidir cada dispositivo con un usuario específico.

Usuarios Configuración

Puede ver los detalles de sus usuarios de Aranda Datasafe en la página de Usuarios.

1. Haga clic en **Configuración**.

2. En la barra lateral, haga clic en **Usuarios**.



La página Usuarios muestra una lista de usuarios y proporciona esta información:

Campo	Descripción
Nombre	El nombre completo del usuario.
Usuario	El nombre de usuario utilizado para iniciar sesión en el dispositivo del usuario.
Email	La dirección de correo electrónico del usuario.
Equipo	El equipo al que está asignado el dispositivo del usuario. Si un usuario tiene varios dispositivos, todos deben estar asignados al mismo equipo.
Política	La política asignada al equipo que utiliza el dispositivo del usuario. Es esta Política la que define cuándo se realiza una copia de seguridad del dispositivo del usuario, qué datos se respaldan y se protegen, y qué funciones de protección y migración están habilitadas.
Equipos	La cantidad de equipos asignados al repositorio.
Dispositivos	La cantidad de dispositivos que el usuario ha respaldado y protegido por Aranda Datasafe.
Datos	La cantidad de datos que Aranda Datasafe ha respaldado para los dispositivos de este usuario.

Filtrado de Usuarios Configuración

De forma predeterminada, la sección **Usuarios** en la página **Configuración** muestra información para todos los usuarios de Aranda Datasafe (que se basan en los perfiles de usuario de Microsoft Windows). Pero, si es necesario, puede filtrar la sección **Usuarios** para que solo muestre información que cumpla con ciertos criterios. Por ejemplo, puede filtrar la sección **Usuarios** para que solo muestre información de un Usuario en particular.

Hay varias formas de filtrar la sección Usuario:

Utilice una búsqueda para filtrar la lista de usuarios.

Mostrar u ocultar columnas en la lista de usuarios.

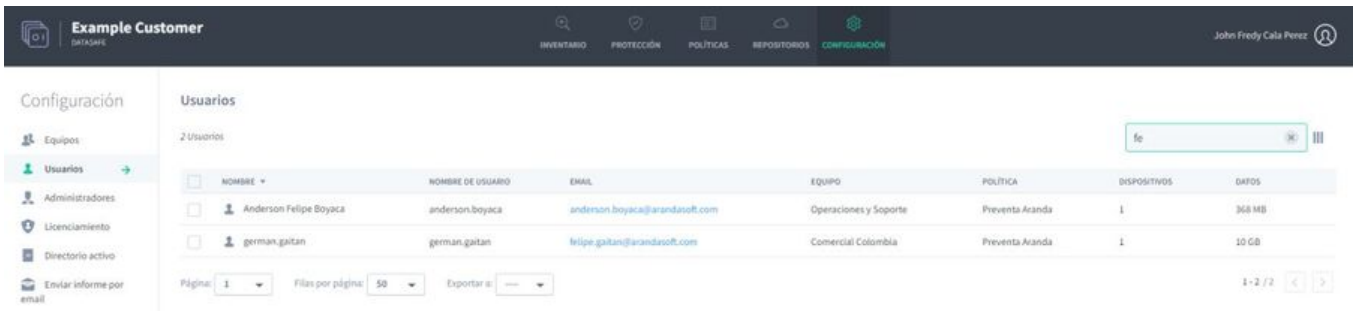
Utilice una búsqueda para filtrar la lista de usuarios

Puede utilizar la función de **búsqueda** para filtrar la lista de usuarios de modo que solo incluya a los usuarios que tienen un nombre en particular (o un nombre parcial).

Para aplicar un filtro de búsqueda:

1. Haga clic en el ícono de búsqueda que se encuentra sobre la lista de usuarios.

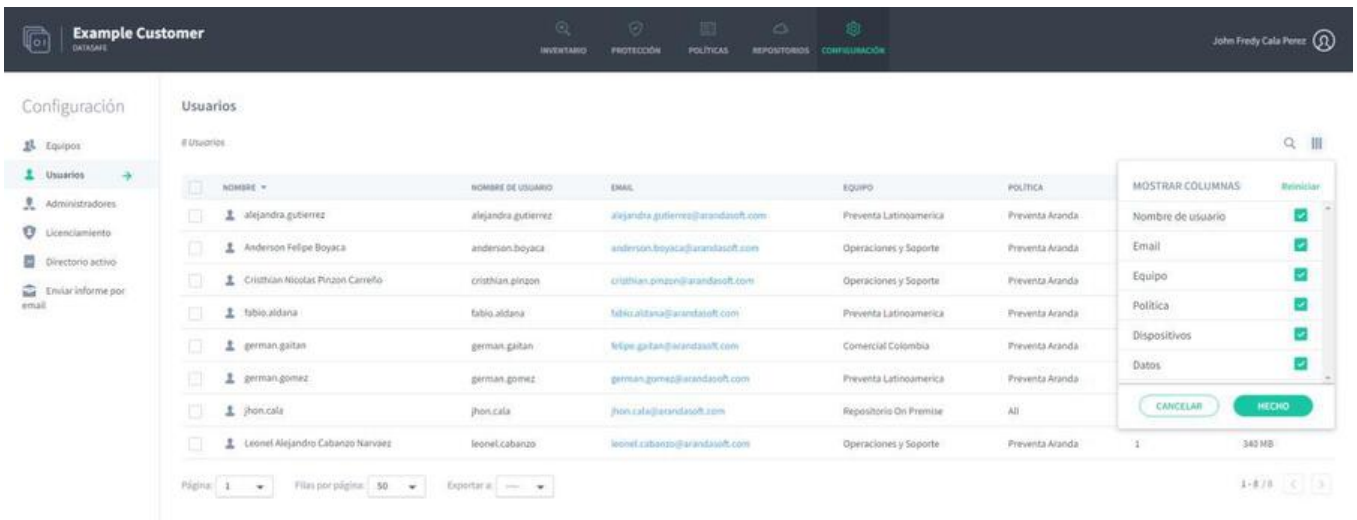
2. Ingrese los primeros caracteres del valor de texto que desea usar como filtro. Aranda Datasafe aplica el filtro a medida que escribe, por lo que puede hacer coincidencias parciales o puede ingresar el valor de texto completo para ser más específico.



Mostrar u ocultar columnas en la lista de usuarios

Puede optar por mostrar u ocultar columnas en la lista de usuarios. Por ejemplo, es posible que no le interese la dirección de correo electrónico de cada usuario, por lo que puede ocultar la columna Correo electrónico.

Para mostrar / ocultar columnas, haga clic en el ícono Columnas y luego elija qué columnas incluir



Crear Nuevo Usuario

Aranda Datasafe crea nuevos usuarios automáticamente como parte del proceso de descubrimiento. No es necesario crear usuarios manualmente.

Si tiene un nuevo miembro del personal y necesita que Aranda Datasafe haga una copia de seguridad y proteja sus dispositivos, instale Discovery Agent en los dispositivos. Aranda Datasafe podrá entonces descubrir los dispositivos y conectarse a ellos.

Cuando Aranda Datasafe se conecta a un dispositivo, crea un Usuario automáticamente, según el perfil de usuario de Microsoft Windows del dispositivo.

Eliminar Usuario

Si desea eliminar un **usuario** de Aranda Datasafe, debe eliminar todos los dispositivos de ese usuario. Cuando Aranda Datasafe no tiene dispositivos para un Usuario:

- Elimina ese usuario automáticamente
- Elimina la licencia del usuario y la pone a disposición para su uso.

Para eliminar los dispositivos de un usuario (y también el usuario):

1. El primer paso es encontrar todos los dispositivos del usuario en una lista de dispositivos. Para ello, puede utilizar la lista de dispositivos en la página de **Inventario** o la página de **Protección**.

Haga clic en **Inventario**. o:

Haz clic en **Protección**.

2. En la sección de la lista de dispositivos, haga clic en el ícono **Buscar**.

3. Ingrese el nombre del usuario en el cuadro de búsqueda. Aranda Datasafe filtra la lista para que solo muestre los dispositivos de ese Usuario.

4. Haga clic en la casilla de verificación en la parte superior de la lista para que se seleccionen todos los dispositivos del usuario.

5. Haga clic en el ícono **Eliminar dispositivo** en la parte inferior de la lista de dispositivos.

6. Ingrese ELIMINAR en mayúsculas y luego haga clic en **Eliminar** para confirmar.

Conector Active Directory

Conector de Active Directory

Active Directory Connector (AD Connector) es una aplicación que Aranda Datasafe usa para autenticar sus cuentas de usuario. Se conecta a su Microsoft Active Directory y le permite a Aranda Datasafe:

- Identificar cada cuenta de usuario de Microsoft
- Identificar los dispositivos que están asociados con cada cuenta de usuario de Microsoft.
- Cree automáticamente usuarios y dispositivos coincidentes en Aranda Datasafe
- Autenticar conexiones de dispositivos a Aranda Datasafe.

Debe instalar AD Connector en un servidor de Windows unido a un dominio que se encuentre en las instalaciones de su empresa. También debe registrar el conector AD para que pueda conectarse a Aranda Datasafe.

Instalar y Registrar conector Active Directory

Active Directory Connector (AD Connector) es una aplicación que Aranda Datasafe usa para autenticar sus cuentas de usuario. Sus datos cifrados solo están disponibles para usuarios autorizados.

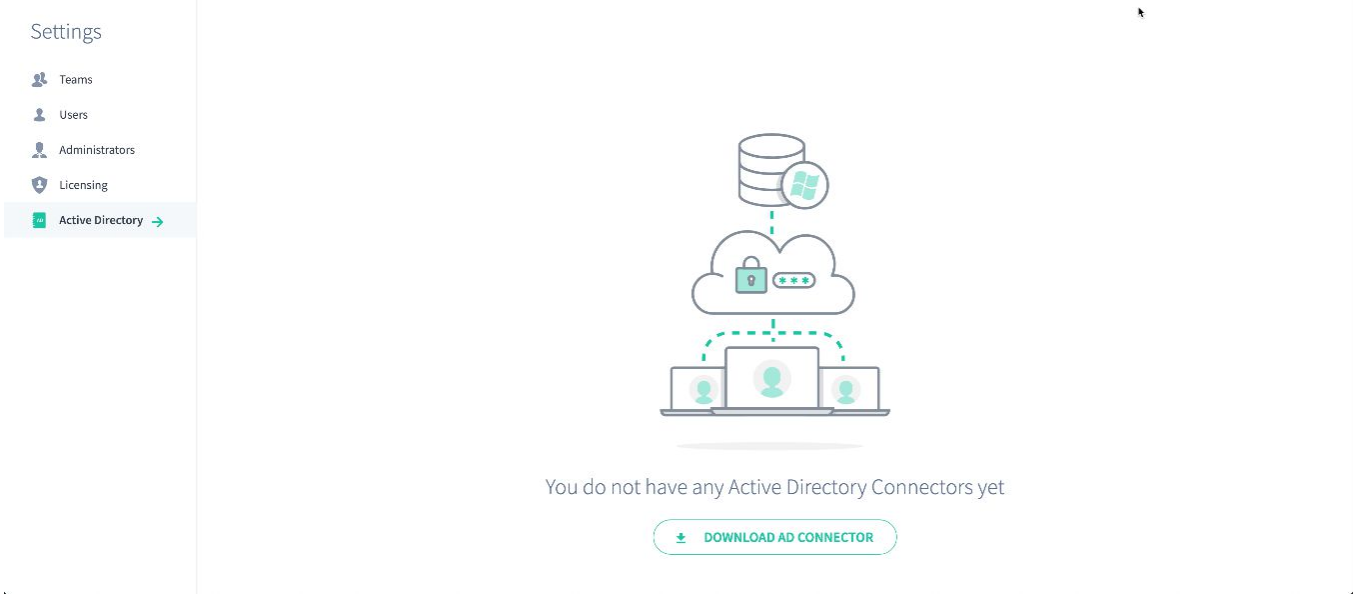
Debe instalar AD Connector en un servidor de Windows unido a un dominio que se encuentre en las instalaciones de su empresa. También debe registrar el conector AD para que pueda conectarse a Aranda Datasafe.

Para descargar, instalar y registrar el software AD Connector:

1. Haga clic en **Configuración**.

2. Haga clic en **Active Directory**.

3. Haga clic en **Descargar Ad Connector** para descargar el archivo ejecutable adconnector. Copie este archivo en su servidor local.



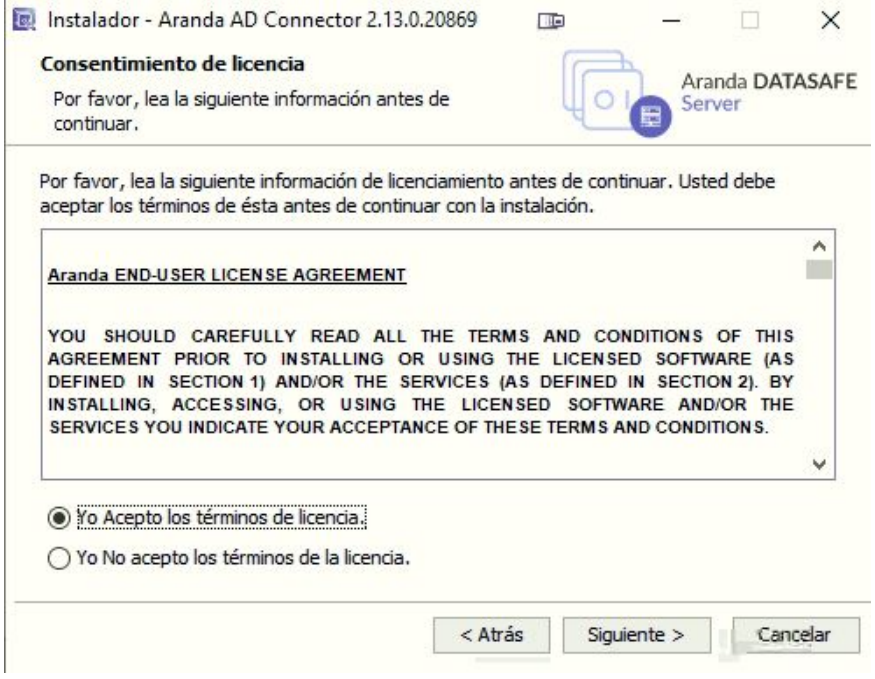
4. Inicie sesión en su servidor local (el servidor en el que se ejecutará AD Connector). Debe iniciar sesión a través de una cuenta de usuario de **administrador de dominio** que tenga permiso para **registrar un nombre principal de servicio (SPN)** para las conexiones Kerberos.

5. Copie el archivo ejecutable de adconnector en el servidor y luego ejecútelo.

6. Siga las instrucciones en pantalla para instalar el conector AD. Puede instalarlo en cualquier directorio (la ubicación predeterminada es la unidad C).

Cuando completa los pasos de instalación, los archivos comienzan a extraerse e instalarse. Cuando se instalan los archivos, el instalador le pregunta si desea registrarse.

7. Asegúrese de que **Registrarse ahora** esté marcado y luego haga clic en **Siguiente**.



8. Ingrese los detalles de registro:

Campo	Descripción
Dominio	El nombre de su tenant de Aranda Datasafe. Este suele ser el nombre de su organización y es la primera parte de la dirección de su tenant de Aranda Datasafe.
Nombre de usuario	Ingrese el nombre de usuario de una cuenta de Aranda Datasafe que tenga el rol de Oficial de seguridad. Solo las cuentas de usuario de Security Officer tienen permiso para registrar un repositorio.
Contraseña	Ingrese la contraseña para la cuenta de Aranda Datasafe.
Dominio	Ingrese el nombre o la dirección IP del servidor que tiene instalado el software AD.
Alias	Ingrese el nombre del conector AD como aparecerá en Aranda Datasafe. Le recomendamos que le dé un nombre descriptivo que reconozcan sus usuarios de Aranda Datasafe.

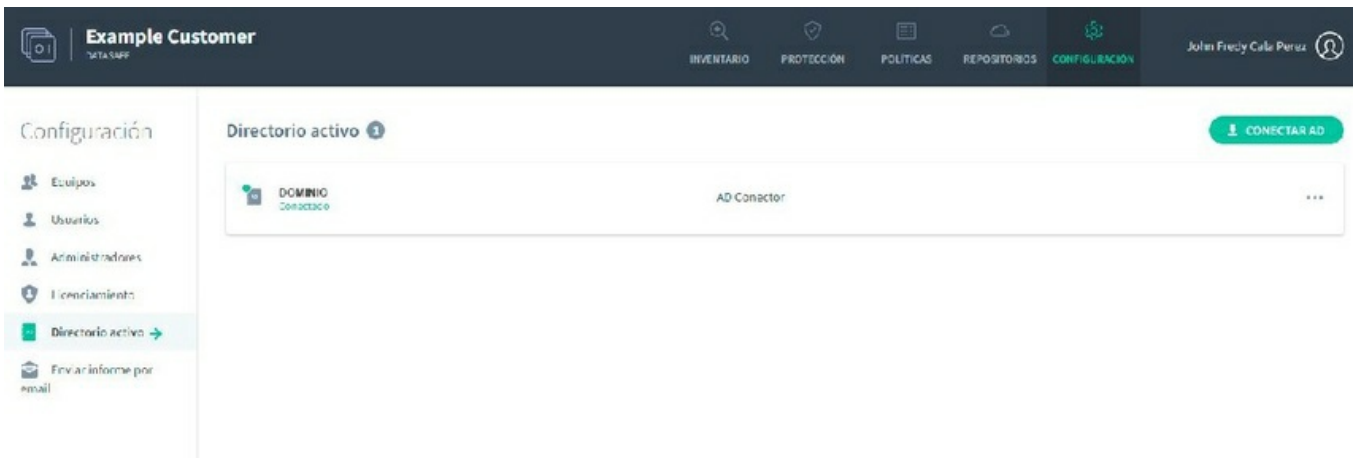
9. Haga clic en **Registrarse**.

Eliminar Conector Active Directory

Para eliminar un conector AD:

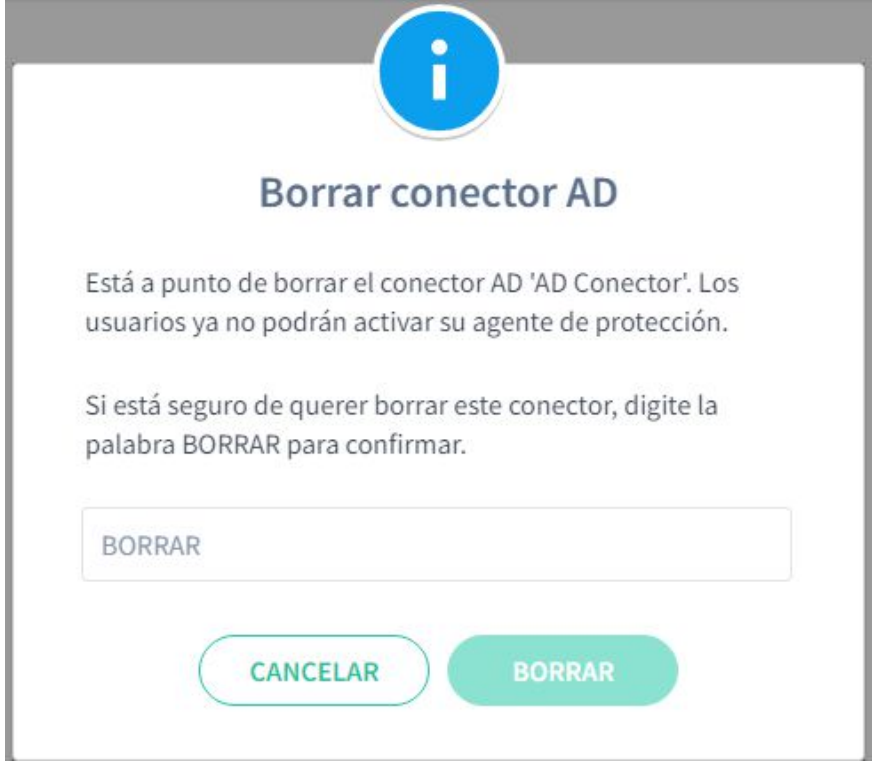
1. Haga clic en **Configuración**.

2. Haga clic en **Active Directory** en la barra lateral.



3. Busque el Active Directory que desea eliminar y luego haga clic en su botón de opción (...) y haga clic en **Eliminar**.

4. Introduzca BORRAR en letras mayúsculas en el cuadro de diálogo para confirmar.



5. Haga clic en **Eliminar**.

Licencias

Licencias

Aranda Datasafe requiere que tengas licencias para tus usuarios. Cuando compra un plan comercial, se le asigna una cantidad de licencias según sus requisitos. Si estos requisitos cambian, puede comprar más licencias y agregarlas a su plan.

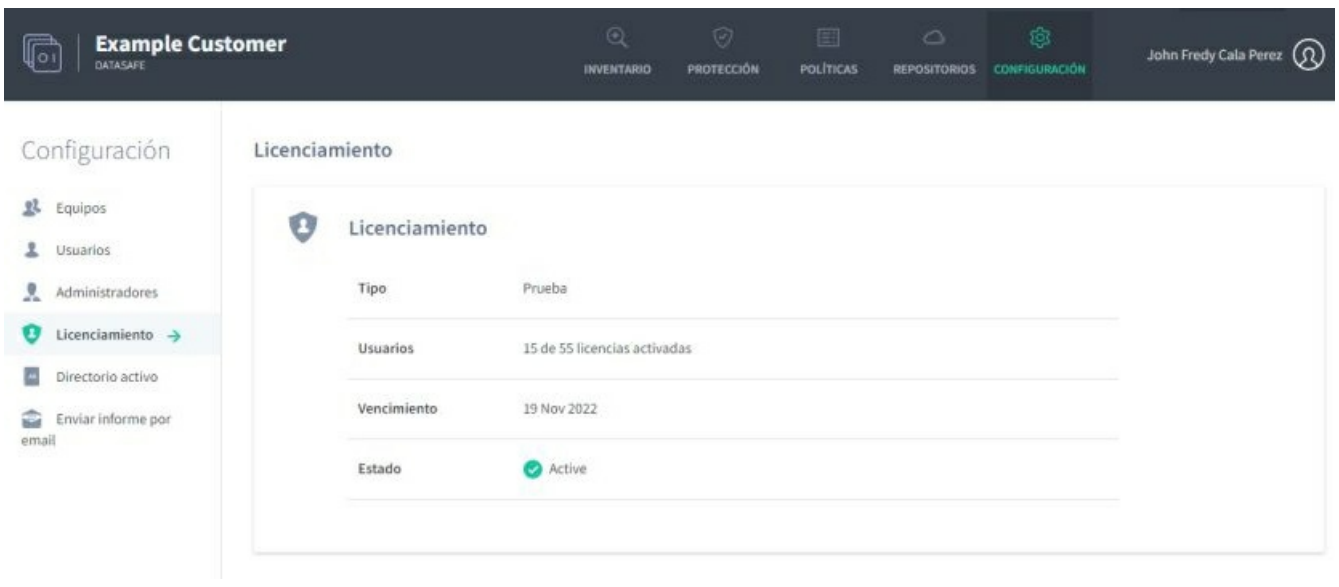
Puede ver información sobre sus licencias en la[página de Licenciamiento](). Muestra la cantidad de licencias que tiene disponibles y el estado de su suscripción a Aranda Datasafe.

Licenciamiento configuracion

Puede ver información sobre su plan y las licencias disponibles en la página de Licencias.

1. Haga clic en **Configuración**.

2. Haga clic en Licencias en la barra lateral.



La página de Licencias muestra:

Campo	Descripción
Tipo	Tu plan Aranda Datasafe.
	Comercial:En el plan comercial, puede utilizar Aranda Datasafe para realizar copias de seguridad y proteger sus dispositivos durante la duración de su suscripción.
Usuarios	El número de licencias que se utilizan actualmente y el número de licencias restantes disponibles.
Expiración*	La fecha y hora de finalización de su suscripción a Aranda Datasafe.
Estado	Muestra si su suscripción a Aranda Datasafe está activa o vencida. Si su suscripción caduca, sus dispositivos ya no están respaldados ni protegidos y, por lo tanto, están en riesgo. Para volver a suscribirse, comuníquese con su administrador de cuentas.

Respaldo y Restauración

Respaldo y Restauración

Aranda Datasafe realiza una copia de seguridad de sus dispositivos activados automáticamente, en horarios programados. Los datos se deduplican y cifran antes de la transferencia y permanecen cifrados durante la transferencia y cuando se almacenan en el repositorio.

¿Qué sucede antes de que se produzca la copia de seguridad?

Para iniciar las copias de seguridad de un dispositivo, deberá activar el dispositivo para su protección. Durante la activación, el agente de protección se descargará e instalará en el dispositivo. El agente de protección pasará por un proceso de autenticación antes de que puedan comenzar la indexación y las copias de seguridad.

Antes de que comience la copia de seguridad, el agente realiza un índice del sistema de archivos. El índice se crea una vez y se actualiza en tiempo real a medida que se agregan, modifican o eliminan archivos del sistema de archivos. La indexación en tiempo real **garantiza que no sea necesario un escaneo que consuma tiempo y recursos** en el momento de la copia de seguridad.

¿Qué sucede durante una copia de seguridad?

Durante una copia de seguridad, se hace referencia al índice para datos comerciales nuevos y modificados; Se crea una instantánea VSS y los datos se deduplican para garantizar que solo los bloques de datos únicos se cifren y transfieran desde el dispositivo del usuario a el repositorio (área de almacenamiento en su servidor).

Backup Automático

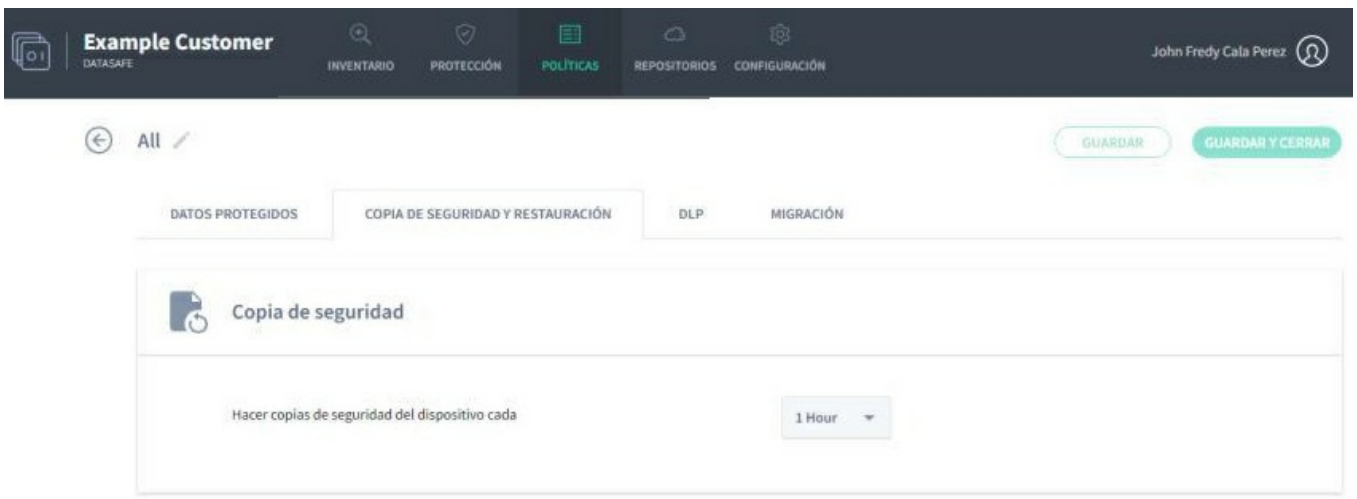
Aranda Datasafe realiza copias de seguridad automáticas de los datos comerciales en sus dispositivos, siempre que:

- El dispositivo está activado
- El dispositivo está asociado a un equipo
- El equipo está asociado con una política y un repositorio.

El **repositorio** define dónde se almacenan los datos de respaldo.

La **Política** define:

- Qué datos comerciales se respaldan
- Cuando se realizan las copias de seguridad.
- Qué funciones de Prevención de pérdida de datos están habilitadas.
- Si se realiza una copia de seguridad de la configuración del perfil de usuario para las migraciones de equipos.



Sus dispositivos se respaldan y protegen automáticamente:

- **Poco tiempo después de que se activen por primera vez** Por lo general, esto es de 10 minutos aproximadamente, pero puede demorar más, ya que la copia de seguridad solo puede ocurrir después de que el Agente de protección haya terminado de indexar.
- **Regularmente** de acuerdo con los intervalos programados que se establecen en las Políticas.

Opciones disponibles: **Cada 1 hora	2 Horas	4 horas	8 horas**.

También puede hacer una copia de seguridad manualmente si lo desea.

Ejecución Copia de Seguridad de Aranda Data Safe

Cuando tiene dispositivos activados en Aranda Datasafe, sus datos comerciales se protegen automáticamente:

- Aproximadamente 10 minutos después de la activación inicial
- Regularmente, de acuerdo con el cronograma de copias de seguridad (que se define en la Política).

También puede hacer una copia de seguridad de un dispositivo manualmente, ya sea en Aranda Datasafe o usando el Agente de protección localmente en el dispositivo. Esto es útil si necesita realizar una copia de seguridad de un dispositivo de inmediato y la próxima copia de seguridad programada no debe realizarse hasta dentro de algún tiempo.

A continuación, explicamos las diversas formas en que puede**ejecutar una copia de seguridad remota en Aranda Datasafe**

Ejecute una copia de seguridad remota desde la página de protección.

Ejecute una copia de seguridad remota desde la página del dispositivo

Ejecute una copia de seguridad remota desde la página de protección

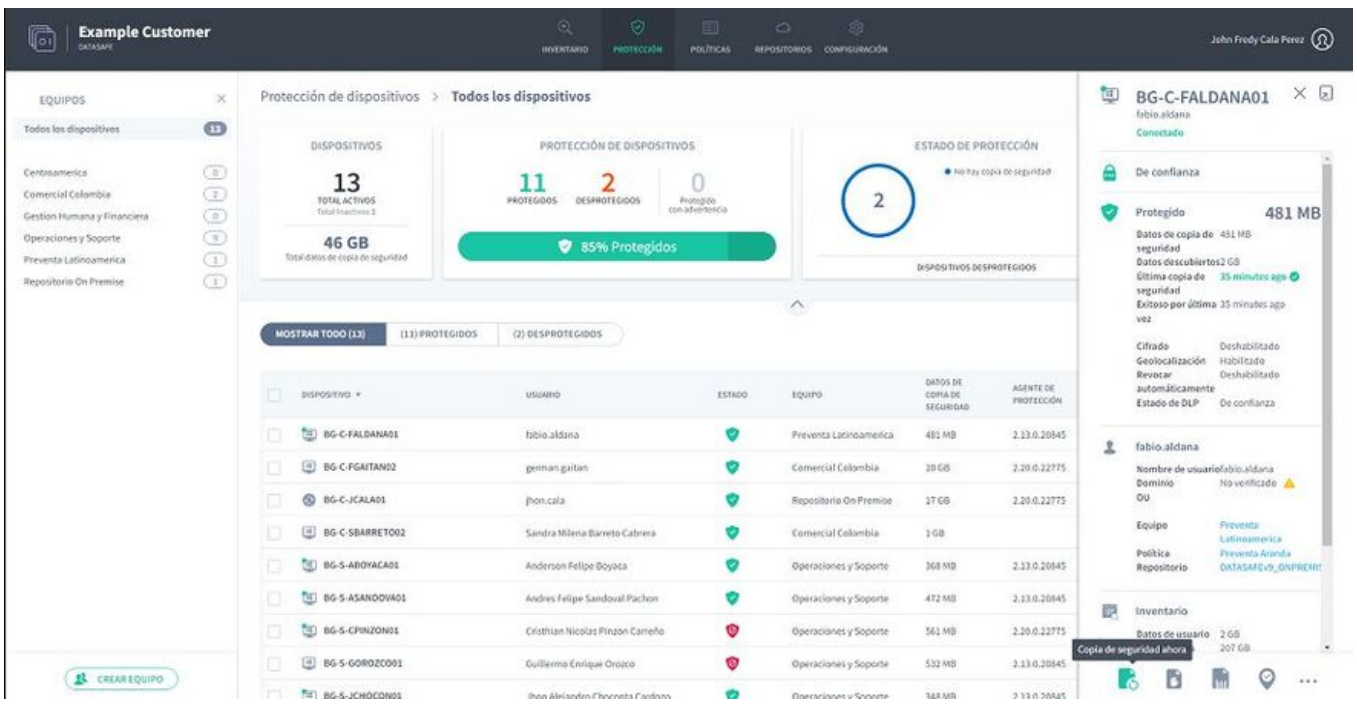
Para ejecutar una copia de seguridad desde la página de**Protección** de Aranda Datasafe:

1. Haga clic en **Protección**.

2. En la lista de dispositivos, haga clic en el dispositivo que desea respaldar. Sus detalles aparecen en un panel lateral.

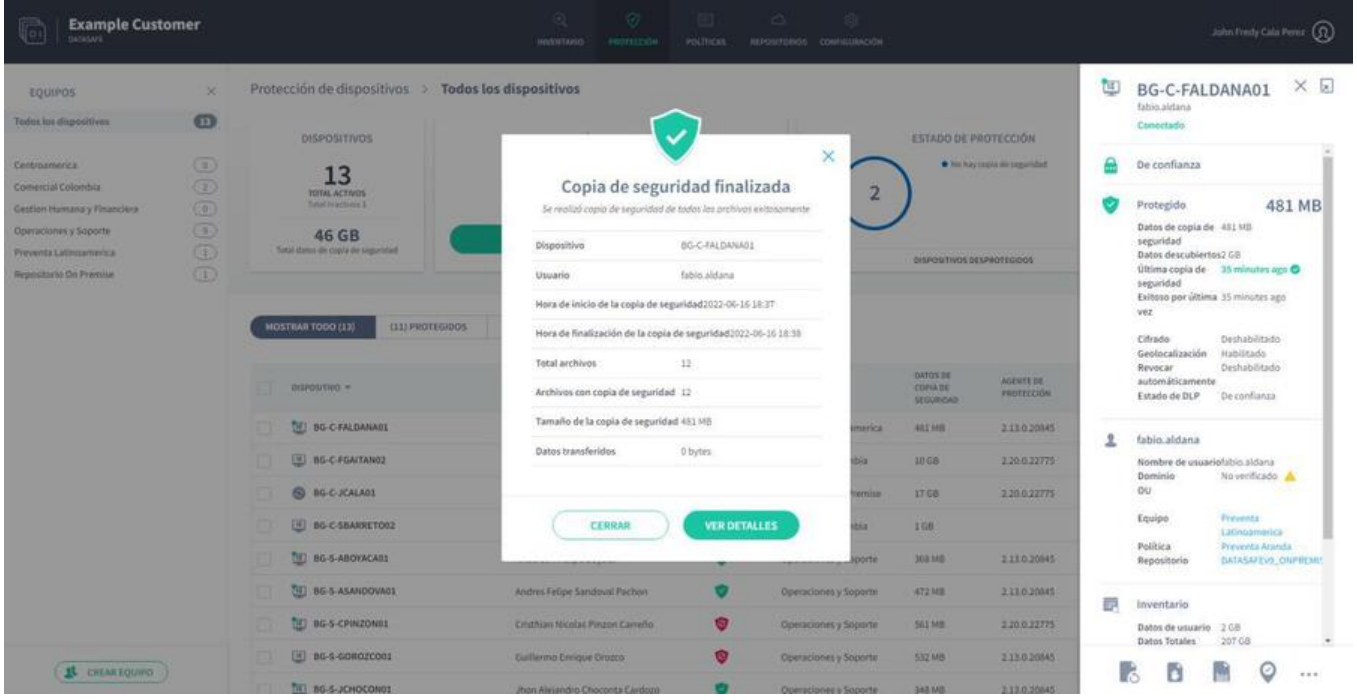
3. Haga clic en el ícono **Hacer copia de seguridad ahora** en la parte inferior del panel.

4. Aparece un mensaje en la parte inferior de la pantalla para informarle que la solicitud de copia de seguridad se realizó correctamente.

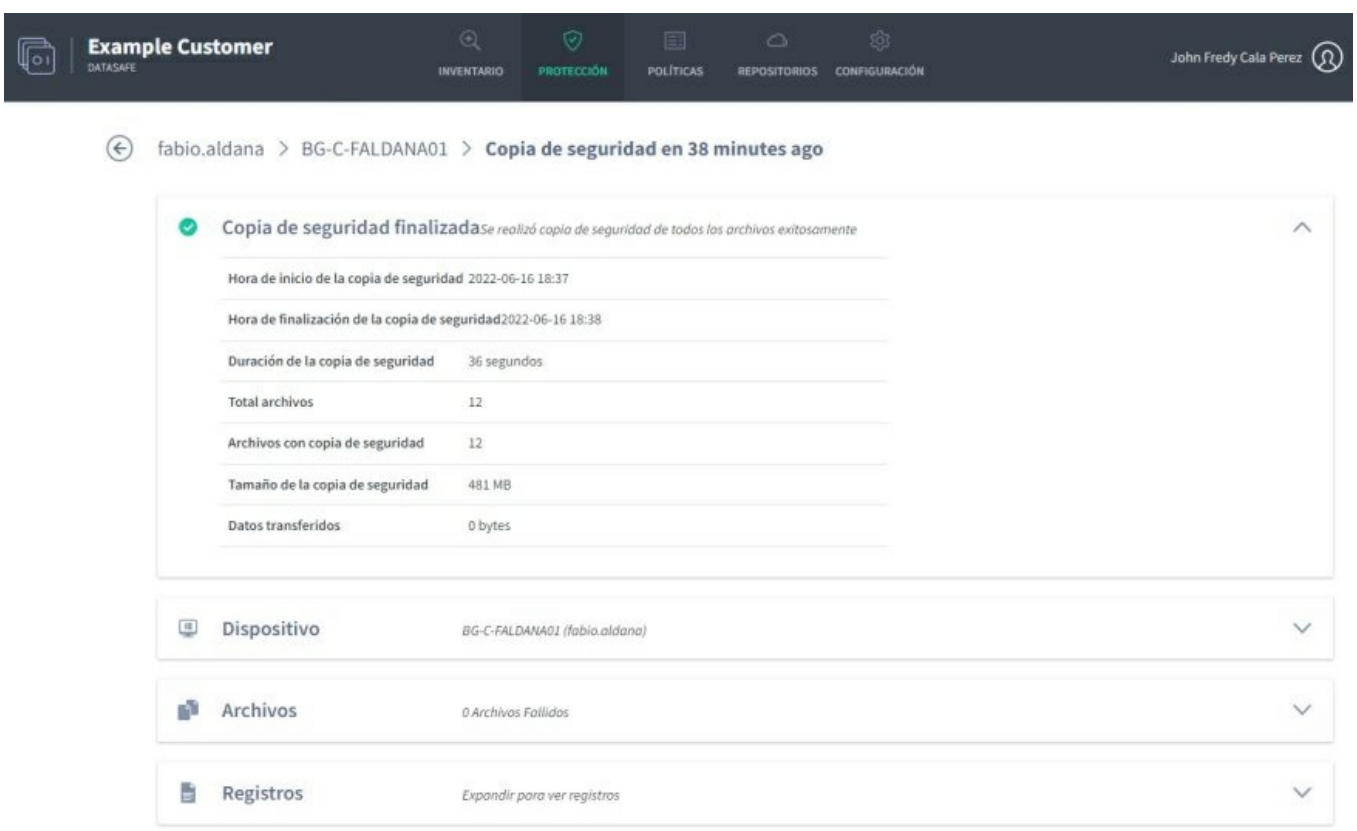


El software Protection Agent (en el dispositivo del usuario) utiliza la deduplicación para asegurarse de que solo se respalden los datos nuevos o modificados en el repositorio. La cantidad de tiempo que se tarda en realizar una copia de seguridad de un dispositivo variará, dependiendo de la cantidad de datos que se deben indexar y realizar una copia de seguridad.

5. En el panel lateral, haga clic en el enlace junto a la entrada **Última copia de seguridad** para mostrar un resumen de la copia de seguridad.



6. Para obtener información más detallada sobre la copia de seguridad, haga clic en **Ver detalles**. A continuación, puede ver los detalles de la copia de seguridad, el dispositivo, los archivos de los que no se pudo hacer una copia de seguridad y los datos de registro.



Ejecute una copia de seguridad remota desde la página de perfil del dispositivo

Para ejecutar una copia de seguridad desde la página de perfil del dispositivo:

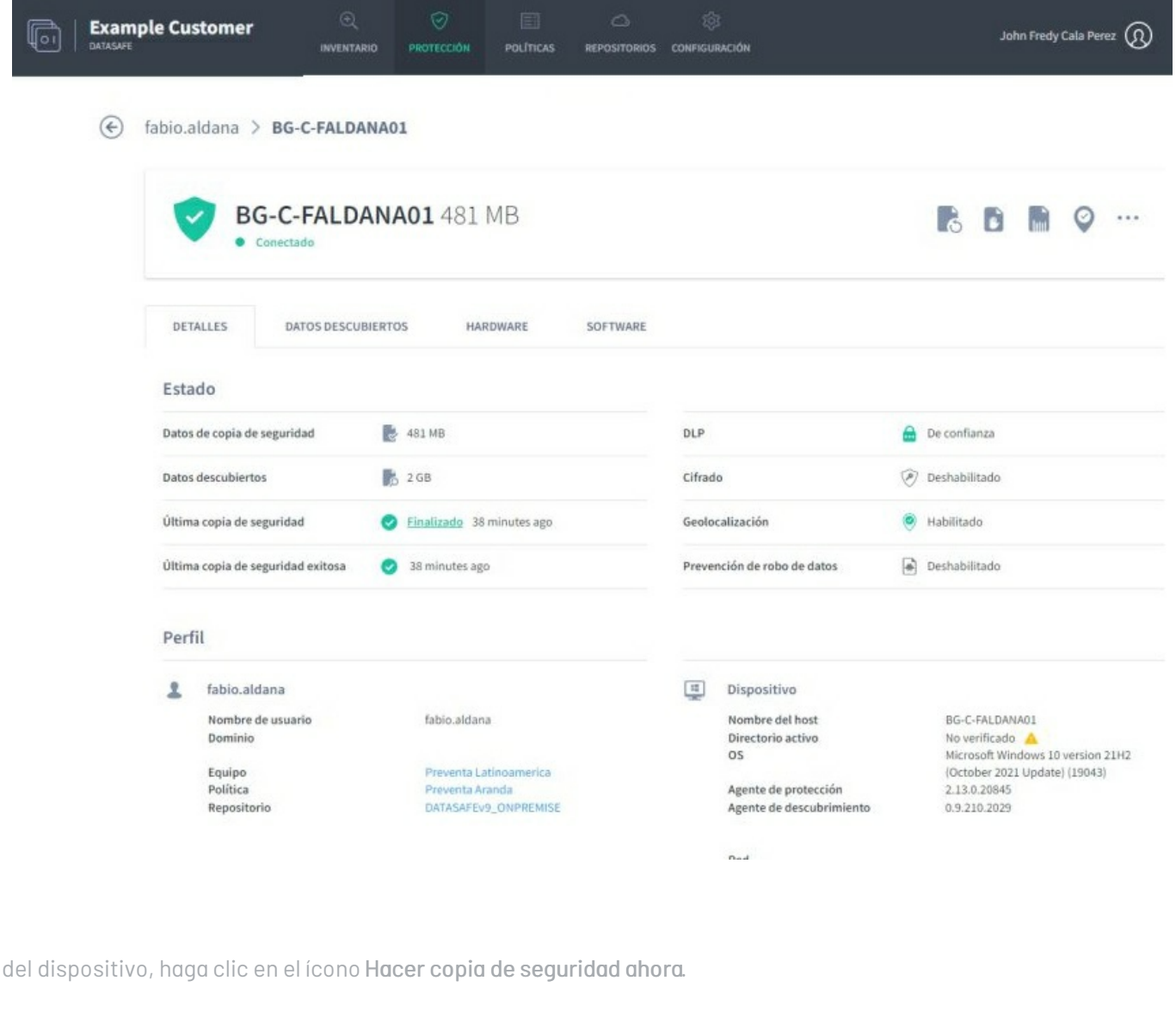
1. El primer paso es acceder a la lista de dispositivos en la página de **Inventario** o en la página de**Protección**.

Haga clic en **Inventario**. O:

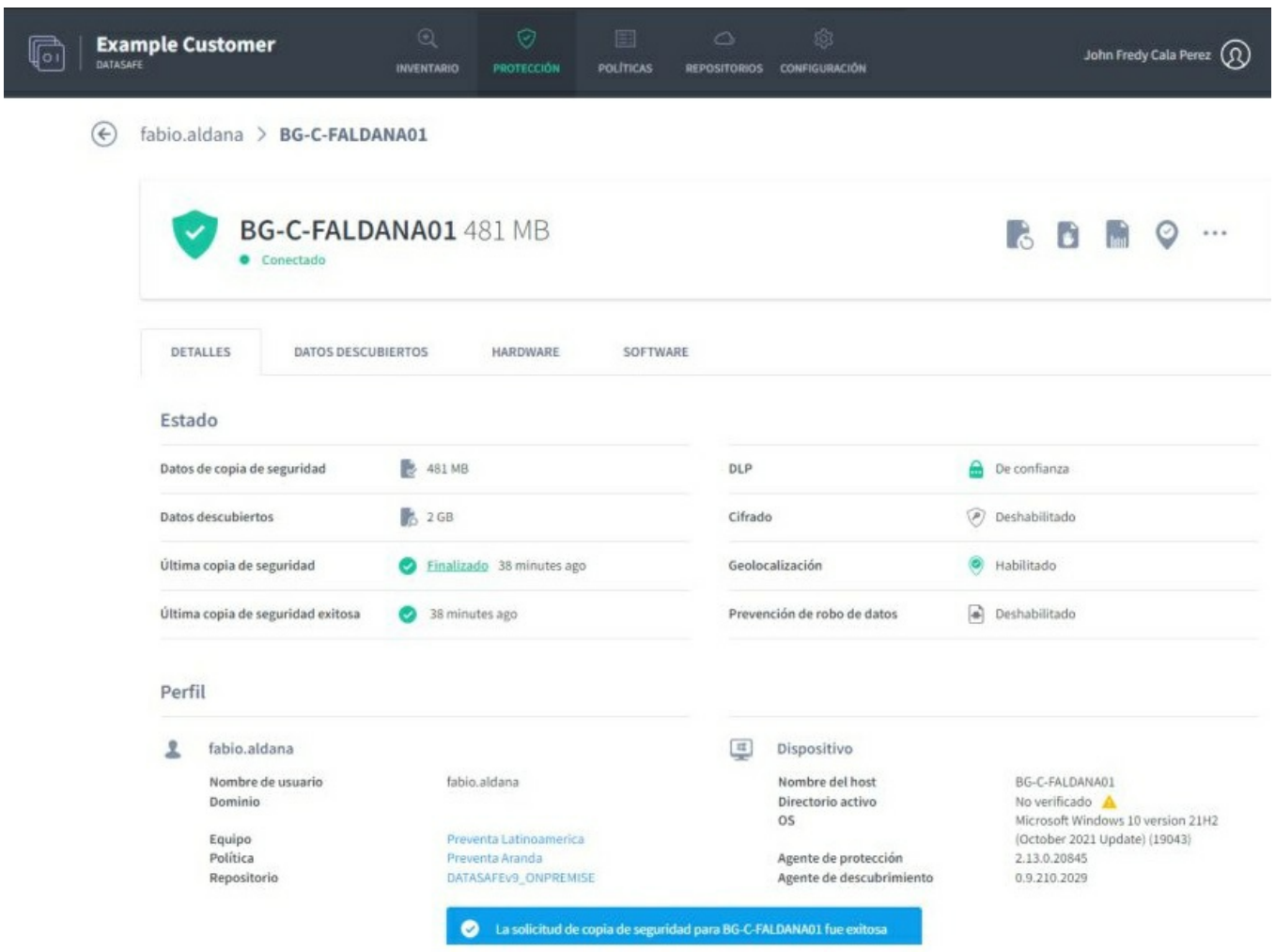
Haz clic en**Protección**.

2. En la lista, haga clic en el dispositivo del que desea realizar una copia de seguridad. Aparece un panel lateral que muestra información sobre el dispositivo que seleccionó.

3. Haga clic en el ícono Detalles en la esquina superior del panel lateral para mostrar la página de perfil del dispositivo.



4. En la página de perfil del dispositivo, haga clic en el ícono **Hacer copia de seguridad ahora**.

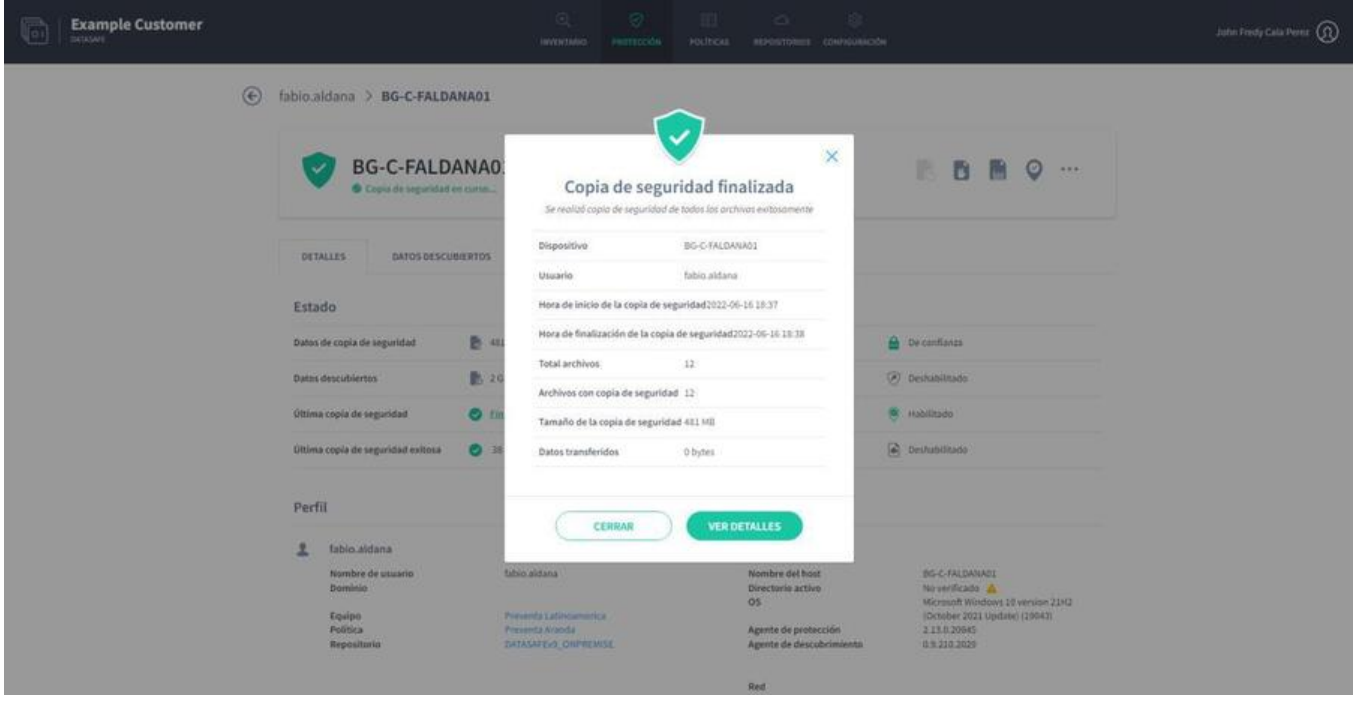


Aparece un mensaje en la parte inferior de la pantalla para informarle que la solicitud de copia de seguridad se realizó correctamente.

El software Protection Agent (en el dispositivo del usuario) utiliza la deduplicación para asegurarse de que solo se respalden los datos nuevos o modificados en el repositorio. La cantidad de tiempo que se tarda en realizar una copia de seguridad de un dispositivo variará, dependiendo de la cantidad de datos que se deben indexar y realizar una copia de seguridad.

5. Cuando se haya realizado la copia de seguridad, haga clic en el enlace de la entrada Última copia de seguridad en la pestaña Detalles de la página de perfil del dispositivo. Aranda Datasafe muestra un resumen de la copia de seguridad.

6. Para obtener información más detallada sobre la copia de seguridad, haga clic en **Ver detalles**. A continuación, puede ver los detalles de la copia de seguridad, el dispositivo, los archivos de los que no se pudo hacer una copia de seguridad y los datos de registro.



Ejecución Copia de Seguridad del Agente

Hay tres formas de hacer una copia de seguridad de sus datos en Aranda Datasafe:

1. Aranda Datasafe realiza una copia de seguridad de sus dispositivos activados automáticamente, en los intervalos definidos en las Políticas para sus dispositivos (consulte Programar las copias de seguridad automáticas).

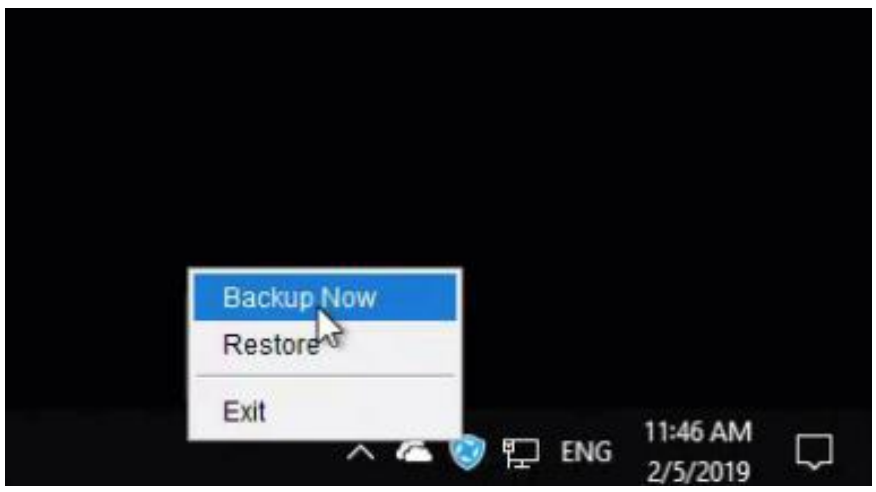
2. Puede iniciar una copia de seguridad manual de forma remota desde Aranda Datasafe (consulte Ejecutar una copia de seguridad remota desde Aranda Datasafe).

3. Puede iniciar una copia de seguridad manual desde un dispositivo local activado (ver más abajo).

Cada dispositivo activado debe tener instalado el software Protection Agent. Este agente es necesario si va a realizar una copia de seguridad manual desde un dispositivo local.

1. Haga clic con el botón derecho en el ícono del Agente de protección en la bandeja del sistema de Windows.

2. Haga clic en Hacer copia de seguridad ahora para iniciar una copia de seguridad.



Detalles y Registros de Copia de Seguridad

Si la página Protección muestra que tiene dispositivos desprotegidos o dispositivos que están protegidos con una advertencia, puede encontrar más información en el último registro de eventos de respaldo del dispositivo. Aranda Datasafe mantiene un registro del último intento de respaldo para cada dispositivo conectado.

Para ver el historial de copias de seguridad y los registros de un dispositivo:

1. Haga clic en **Protección**.

2. En la lista Dispositivos, haga clic en un dispositivo para mostrar los detalles del dispositivo en un panel deslizable.

3. Haga clic en el ícono Ver en la esquina superior del panel deslizante para mostrar la página de perfil del dispositivo.

4. En la página Dispositivo, haga clic en el enlace de la entrada **Última copia de seguridad** (en la pestaña Detalles).

5. En el cuadro de diálogo de resumen de la copia de seguridad, haga clic en **Ver detalles** para mostrar el registro de la copia de seguridad del dispositivo.

6. Expanda las secciones del registro de copia de seguridad para ver los detalles de la última copia de seguridad.

Restaurar Dispositivo

Importante: Solo puede restaurar los datos del usuario y la información del perfil si se ha realizado una copia de seguridad de los datos del usuario en Aranda Datasafe.

Si Aranda Datasafe tiene copias de seguridad de los datos en máquinas protegidas, puede restaurarlas en cualquier momento. Normalmente, utilizaría la función de restauración si:

- Ha eliminado accidentalmente un archivo protegido y desea volver a agregarlo a su dispositivo
- Tiene un dispositivo nuevo y desea descargar los datos protegidos que estaban anteriormente en un dispositivo diferente. Por ejemplo, si está reemplazando una computadora portátil vieja, puede usar **Restaurar** para agregar los archivos protegidos de la computadora portátil vieja a la computadora portátil nueva.

Si la política tiene habilitada la **migración** y la opción **Perfiles de usuario de Microsoft Windows** está seleccionada, también puede restaurar la configuración del perfil de usuario.

Para **restaurar** archivos en un dispositivo:

1. Inicie sesión en el dispositivo que recibirá la copia de seguridad de los datos de Aranda Datasafe.

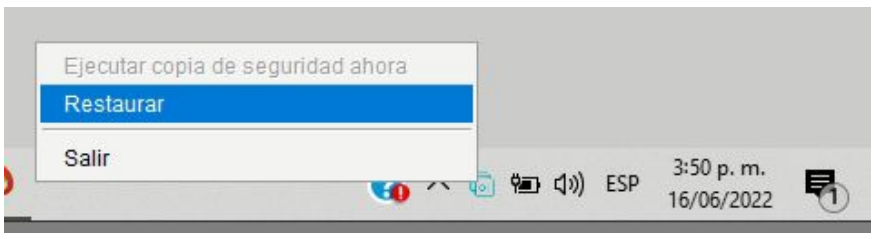
Si el dispositivo ya tiene instalado Discovery Agent, ignore los pasos 2 y 3 y continúe desde el paso 4.

Si necesita restaurar datos a un nuevo dispositivo o un dispositivo que no ha sido protegido por Aranda Datasafe antes, necesita instalar Discovery Agent. Continúe desde el paso 2.

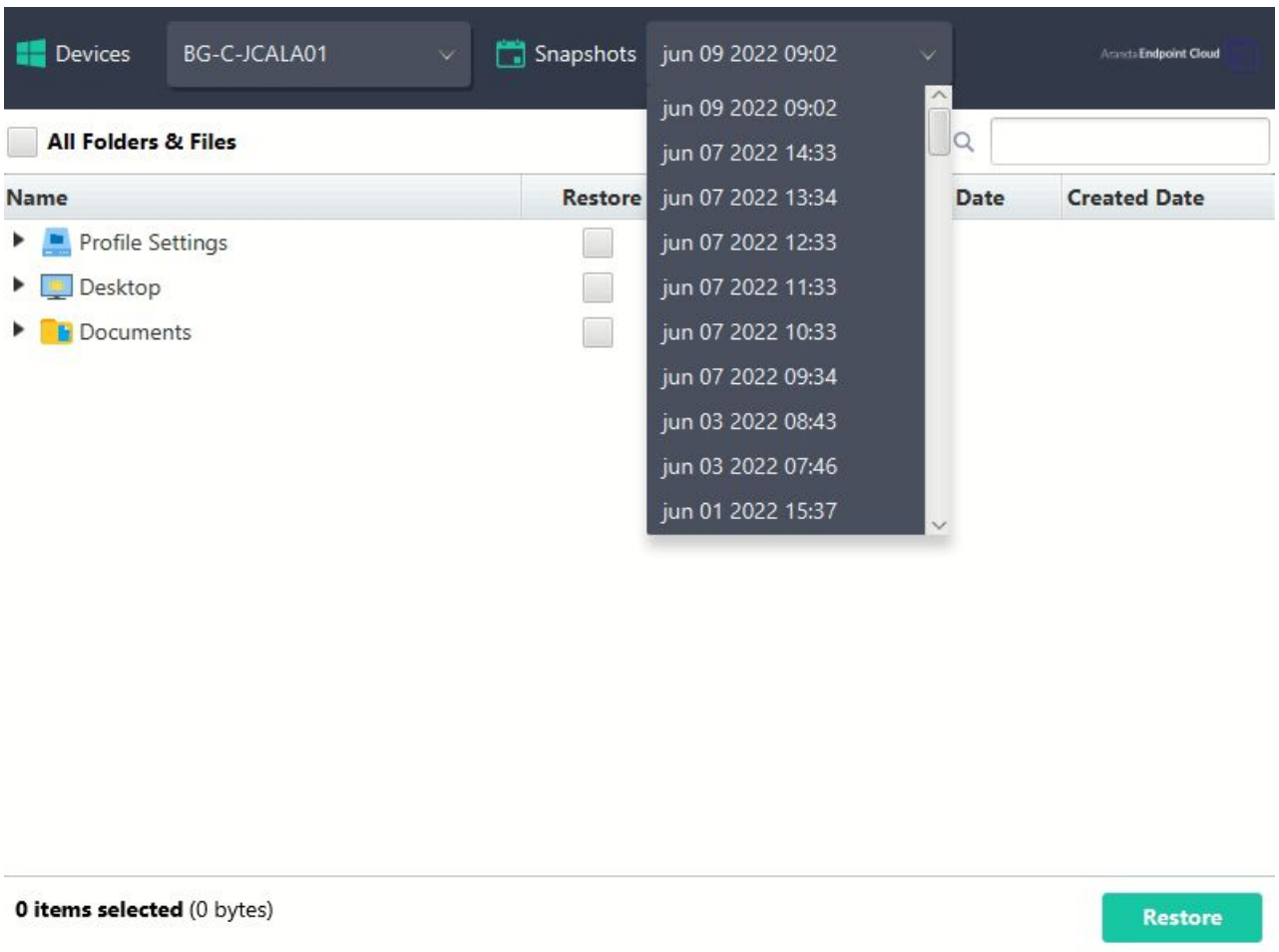
2. Instale Discovery Agent en el dispositivo, para que Aranda Datasafe pueda detectarlo. Si necesita más información, consulte Instalación y despliegue de Discovery Agent.

3. En Aranda Datasafe, active el nuevo dispositivo. Si necesita más información, consulte Activación de sus dispositivos.

4. En la bandeja del sistema de Windows, haga clic con el botón derecho en el ícono del Agente de protección y seleccione **Restaurar**.



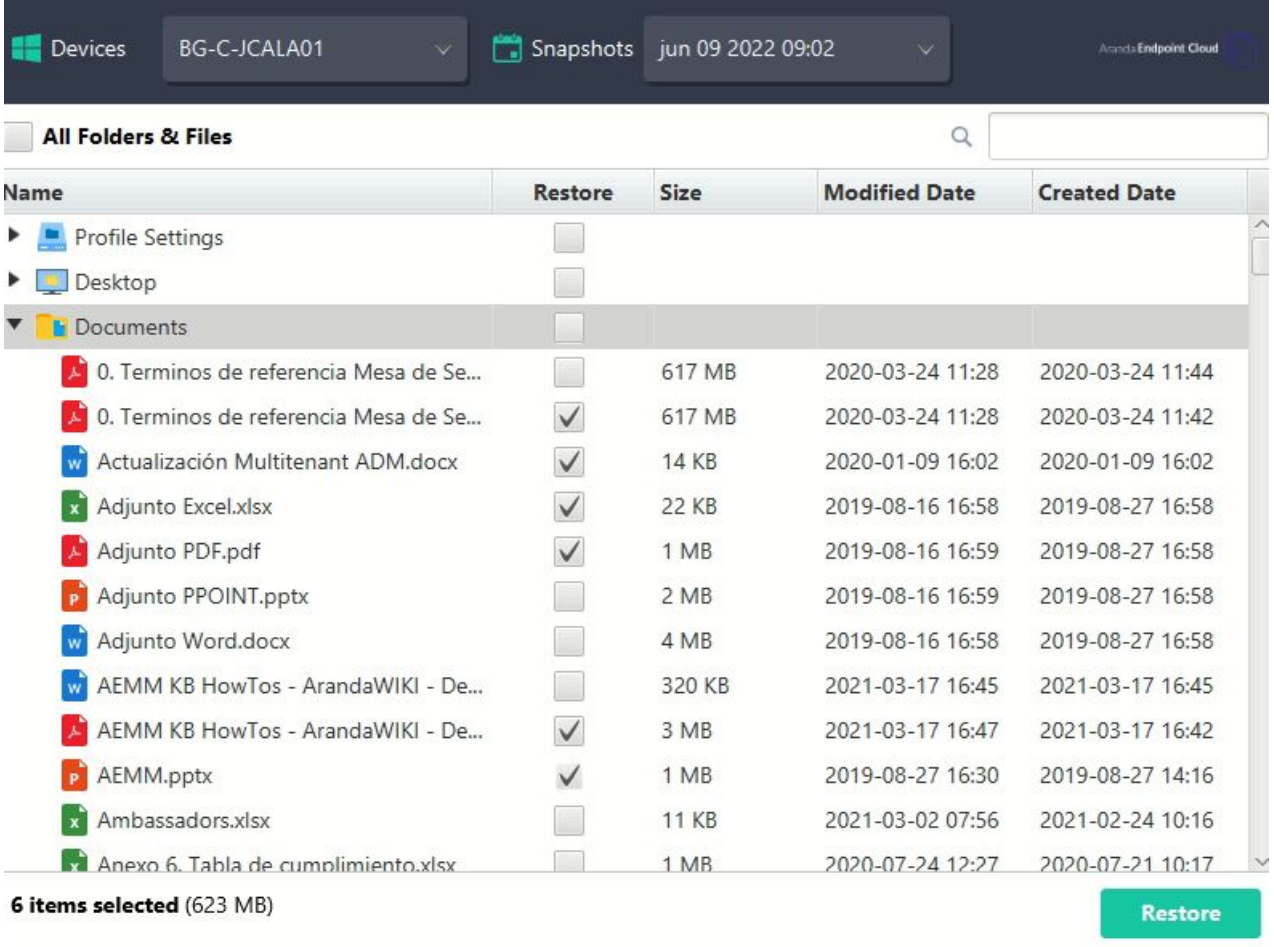
5. En la parte superior del Agente de Aranda, elija el dispositivo y la instantánea asociada que desea migrar al nuevo dispositivo. La instantánea es un registro de los datos de un dispositivo en un momento específico y puede elegir entre cualquiera de los momentos que se muestran en la lista.



6. Elija qué archivos desea restaurar. Puede elegir **Todas las carpetas y archivos**, todos los archivos del **escritorio, todos los documentos** o todos los archivos de los volúmenes (unidades). Alternativamente, puede seleccionar archivos individuales.

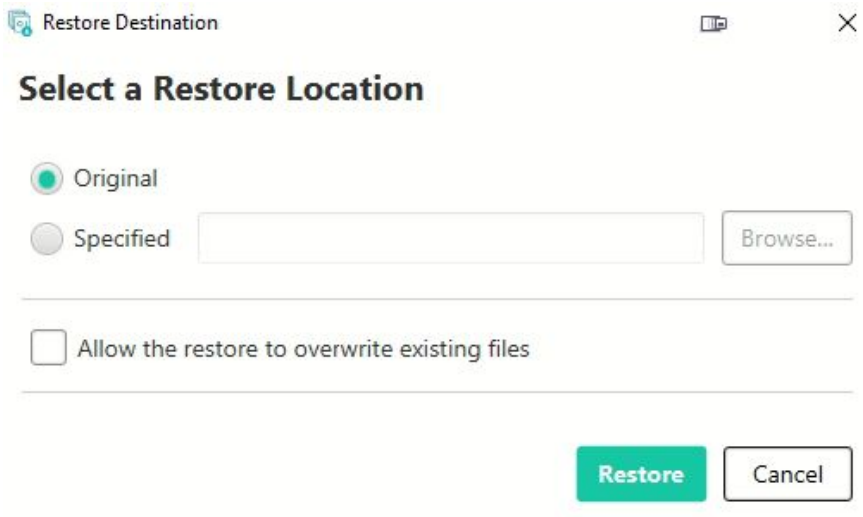
Si la política tiene habilitada la **migración** y la opción **Perfiles de usuario de Microsoft Windows** está seleccionada, también puede restaurar los datos del perfil de usuario. Seleccione la opción **Configuración de perfil** para restaurar esta configuración.

Si la función de **migración** está desactivada o los **perfiles de usuario de Microsoft Windows** no están seleccionados, solo puede optar por restaurar los datos de copia de seguridad.



7. Seleccione **Restaurar**.

8. Elija la ubicación de restauración de los archivos. Si elige **Original**, los archivos se cargarán en la misma ubicación que tenían en el dispositivo anterior. O puede elegir una ubicación **especificada** diferente si lo prefiere.



9. Seleccione **Restaurar**.

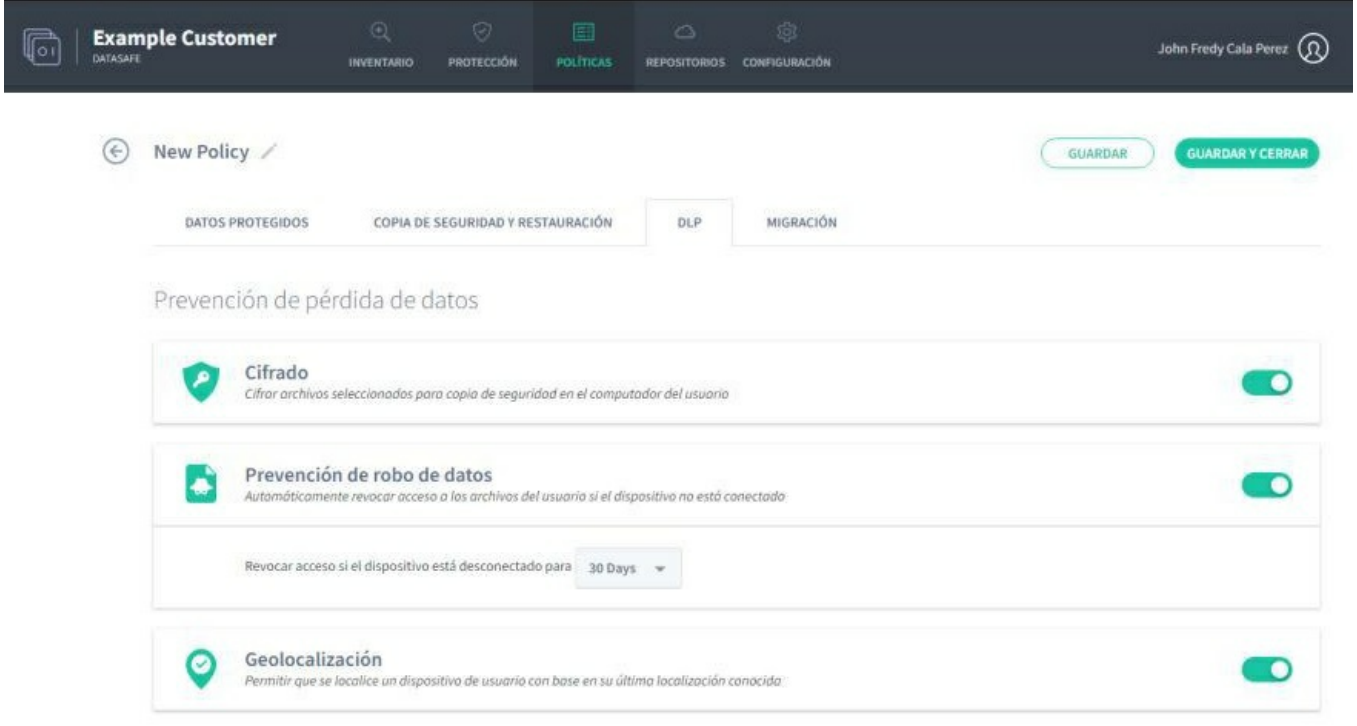
Los datos seleccionados se descargan de Aranda Datasafe a su dispositivo. Si ha elegido archivos de escritorio, los verá aparecer en el escritorio.

Si está restaurando los datos de respaldo y la configuración del perfil de usuario, la restauración se completará en dos fases separadas.

Prevención Pérdida de Datos

Prevención de Pérdida de Datos

Aranda Datasafe tiene muchas funciones de Prevención de pérdida de datos (DLP) que están diseñadas para proteger los datos de su empresa si uno de sus dispositivos se pierde o es robado.



Las funciones de DLP le permiten:

- Habilitar el cifrado de archivos locales. Esto cifra los datos en sus dispositivos de usuario para garantizar que se controle la seguridad y el acceso a los datos. Para obtener más información, consulte Habilitar el cifrado local.
- Tener prevención automática de robo de datos. Si un dispositivo se desconecta de Aranda Datasafe durante un período de tiempo determinado, el Agente de Aranda evitará el acceso a los datos cifrados en el dispositivo. (Esto solo se aplica cuando el cifrado local está habilitado) Para obtener más información, consulte Habilitar la prevención de robo de datos).
- Utilice la geolocalización para encontrar la última ubicación conocida del dispositivo, en función de su señal wi-fi (consulteBuscar dispositivos con geolocalización).
- Utilice Aranda Datasafe para borrar de forma segura un dispositivo para que sus datos ya no existan en el dispositivo.
- Utilice Aranda Datasafe para revocar el acceso a los datos cifrados en el dispositivo en línea (solo se aplica cuando el cifrado local está habilitado). Cuando se revoca un dispositivo, sus datos cifrados no están disponibles, pero puede anularlo si desea que sus datos estén disponibles nuevamente.

Puede activar o desactivar las funciones de DLP para cada política (consulte Activar funciones de prevención de pérdida de datos).

Si uno de sus dispositivos falta o ha sido robado, consulte Si un dispositivo se pierde o es robado.

Pérdida o Robo de Dispositivo

Si un dispositivo protegido por Aranda Datasafe se pierde o es robado, puede:

Encontrar el dispositivo

Si la Política del dispositivo tiene la Geolocalización habilitada, puede usar Aranda Datasafe para encontrar la última ubicación conocida del dispositivo. La ubicación se muestra en Aranda Datasafe en un mapa de Google incrustado. Esta función utiliza las conexiones wi-fi del dispositivo para identificar la última ubicación conocida y, por lo tanto, requiere que el dispositivo esté habilitado para Wi-Fi.

Para obtener más información sobre la geolocalización, consulteBuscar dispositivos con geolocalización.

Revocar el dispositivo*

Si la política del dispositivo tiene habilitado el cifrado local, puede revocar el dispositivo. Esta puede ser una buena opción si sospecha que se ha perdido un dispositivo, en lugar de haber sido robado.

Con una revocación, le dice a Aranda Datasafe que elimine de forma remota el certificado de cifrado del dispositivo. Tan pronto como el agente recibe la instrucción, el certificado se elimina y no se puede acceder ni utilizar los datos cifrados en el dispositivo. Por lo tanto, cualquier persona que use el dispositivo no podrá acceder a sus datos.

Tiene la opción de anular la revocación más tarde. La revocación volverá a colocar el certificado de cifrado en el dispositivo para que los datos cifrados vuelvan a estar disponibles.

Para más información, ver:

- Revocar un dispositivo
- Anular la revocación de un dispositivo

Borrado de dispositivo

Puede utilizar Aranda Datasafe para realizar un “borrado forense” del dispositivo. El borrado elimina de forma segura los datos del dispositivo. Implica una

revocación del certificado de cifrado y una serie de eliminaciones que eliminan los datos y luego se vuelven a borrar para eliminar cualquier rastro de sus datos.

Para obtener más información, consulte Limpiar un dispositivo de forma remota.

> ⚐ **Nota:** Puede configurar Aranda Datasafe para que revoque automáticamente un dispositivo si el dispositivo no se conecta a Aranda Datasafe dentro de un período de tiempo determinado.

Habilitar Funciones de Prevención

Puede editar una política y activar o desactivar cada una de las funciones de DLP (prevención de pérdida de datos) según sea necesario. Pero tenga en cuenta que la configuración de la Política se aplica a todos los equipos que utilizan la Política.

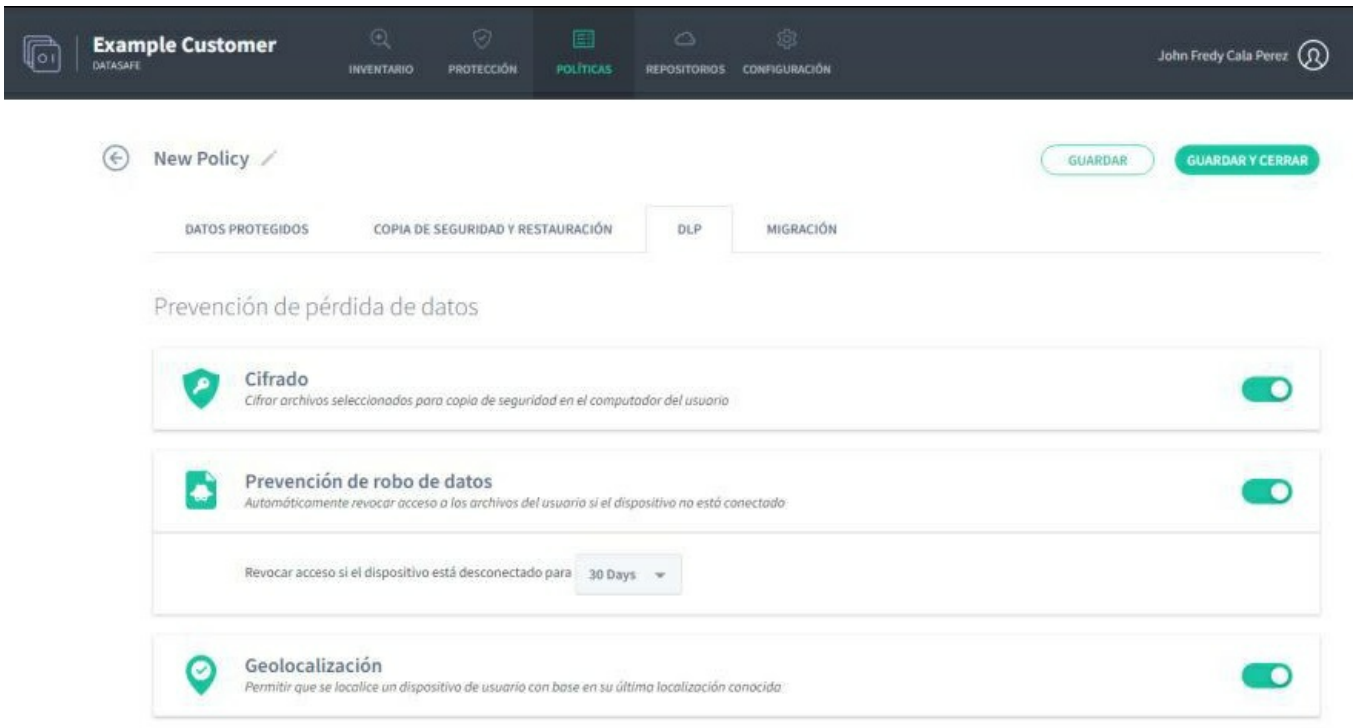
1. Haga clic en **Políticas**.

2. Haga clic en la Política que desea editar.

3. Haga clic en la pestaña **DLP**.

4. Utilice los controles deslizantes para habilitar o deshabilitar cada función de DLP (el verde está habilitado, el gris está deshabilitado).

5. Haga clic en **Guardar** o **Guardar y cerrar**.



Encuentre Dispositivos con Geolocalización

Puede utilizar la **geolocalización** para encontrar la última ubicación conocida de un dispositivo, siempre que:

- El dispositivo tenga WI-FI habilitado
- La función de **geolocalización** está habilitada en la política (utilizada por el equipo del dispositivo).

Para descubrir la última ubicación conocida, Aranda Datasafe se conecta a Google Maps. La ubicación se estima en base a:

- Las coordenadas de los últimos puntos de acceso WI-FI que ubicó su dispositivo
- La intensidad de la señal de su dispositivo al punto de acceso.

La ubicación se estima en función de la señal WI-FI, no se necesita GPS.

Para utilizar la geolocalización de Aranda Datasafe para encontrar un dispositivo:

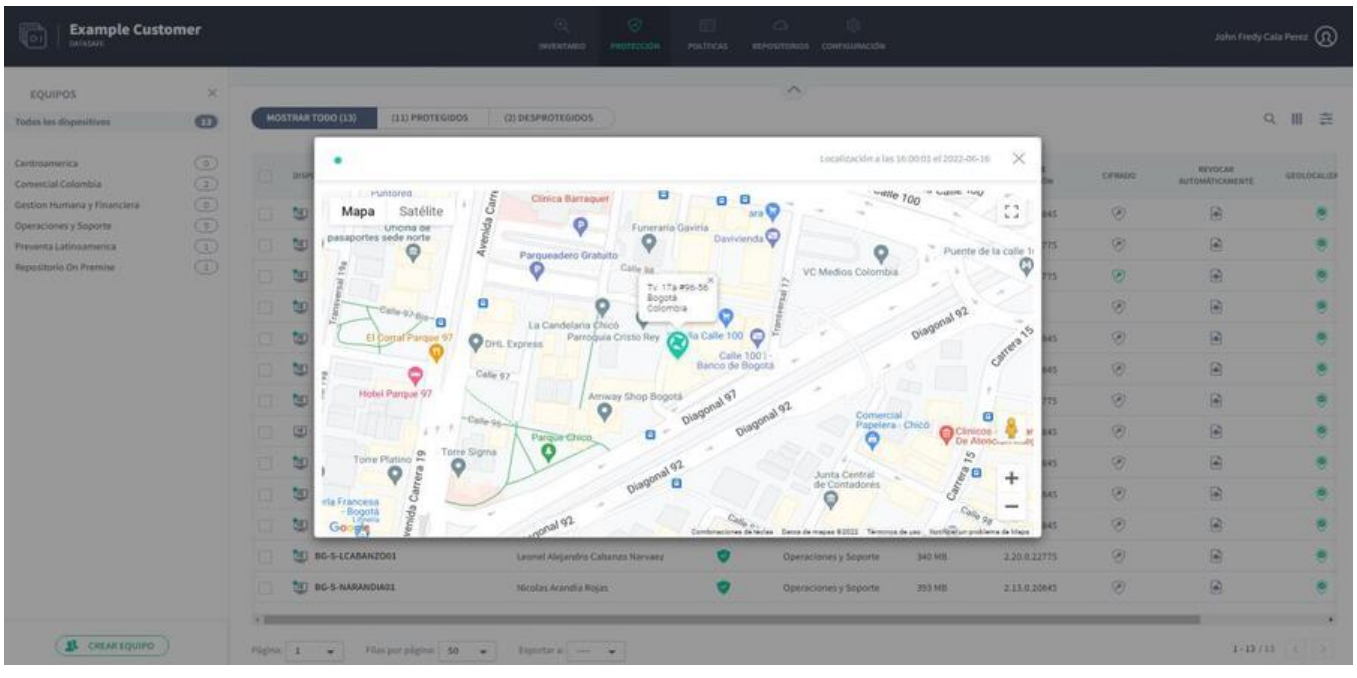
1. Haga clic en **Inventario** o **Protección**.

2. En la lista de dispositivos, haga clic en el dispositivo que desea ubicar. Aparece su panel deslizable.

3. Haga clic en el ícono **Geolocalizar**.

La última ubicación conocida se muestra en un mapa de Google. Puede acercar, alejar y mostrar la vista de satélite.

⚐ **Nota:** El ícono de geolocalización también está disponible en la página de perfil del dispositivo (desde la página de Inventario o Protección, muestre el panel deslizante del dispositivo, luego haga clic en el ícono de ver detalles para mostrar la página de perfil del dispositivo).



Revocar Acceso a dispositivo

Si habilita el cifrado local en una política, cada dispositivo que usa esa política recibe un certificado de cifrado. Cuando un usuario inicia sesión en un dispositivo, solo puede acceder a los datos cifrados si el certificado está en su lugar.

Si un dispositivo se pierde o es robado, puede usar Aranda Datasafe para eliminar de forma remota el certificado del dispositivo. Una vez que se elimina el certificado, cualquier persona, incluido el usuario que inició sesión, no podrá acceder a los datos cifrados en el dispositivo (ya que el certificado no está en el dispositivo).

El uso de Aranda Datasafe para eliminar un certificado se conoce como "revocación de un dispositivo".

Para revocar un dispositivo:

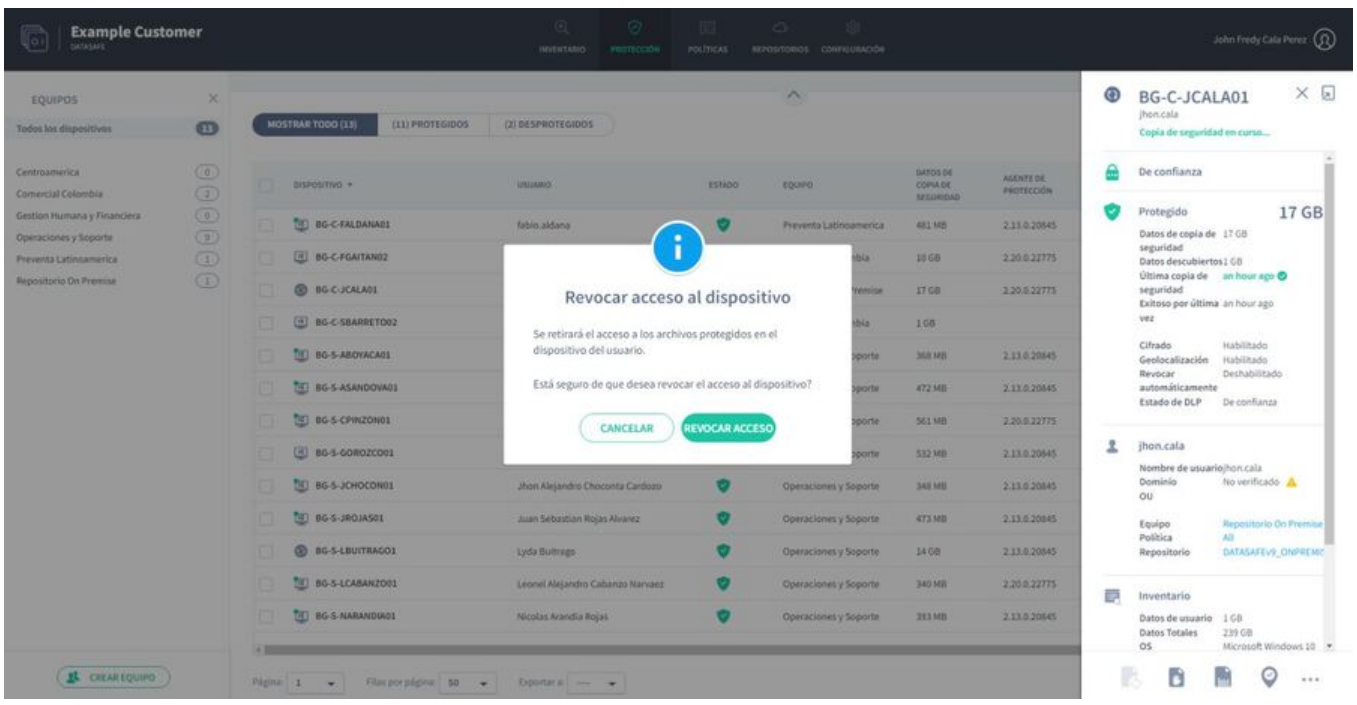
1. Haga clic en **Inventario** o **Protección**.

2. En la lista de dispositivos, haga clic en el dispositivo que desea revocar. Aparece el panel deslizable del dispositivo.

3. Haga clic en el ícono **Revocar dispositivo**.

⚐ **Nota:** El ícono Revocar dispositivo también está disponible en la página de perfil del dispositivo (en la página de Inventario o Protección, muestre el panel lateral del dispositivo y luego haga clic en el ícono de ver detalles para mostrar la página de perfil del dispositivo).

4. Haga clic en Revocar para confirmar. Se realiza la solicitud de revocación del dispositivo. Puede cancelar la solicitud de revocación si es necesario (muestre el panel deslizante del dispositivo o la página del dispositivo y luego haga clic en el ícono Cancelar revocación).



⚐ **Nota:** Si Auto Revocar está habilitado en una Política, Aranda Datasafe automáticamente revocará el certificado de cualquier dispositivo protegido que no se conecte a Aranda Datasafe dentro de un período de 30 días. (Puede cambiar el período de tiempo de revocación automática en la configuración de la política).

Borrado Remoto a Dispositivo

Si desea eliminar los archivos de un dispositivo que falta o es robado, puede usar la funciónBorrado. Esto elimina completamente los archivos protegidos del dispositivo (a diferencia de Revocar, que deja los archivos en su lugar pero los hace inaccesibles).

Con una limpieza, utiliza Aranda Datasafe para realizar un "borrado forense" remoto, que elimina los archivos protegidos en el dispositivo. Como parte del "borrado forense", Aranda Datasafe elimina el certificado de cifrado y realiza una serie de eliminaciones adicionales para eliminar por completo cualquier rastro de los datos protegidos del dispositivo.

Para borrar un dispositivo:

1. Haga clic en **Inventario** o **Protección**.

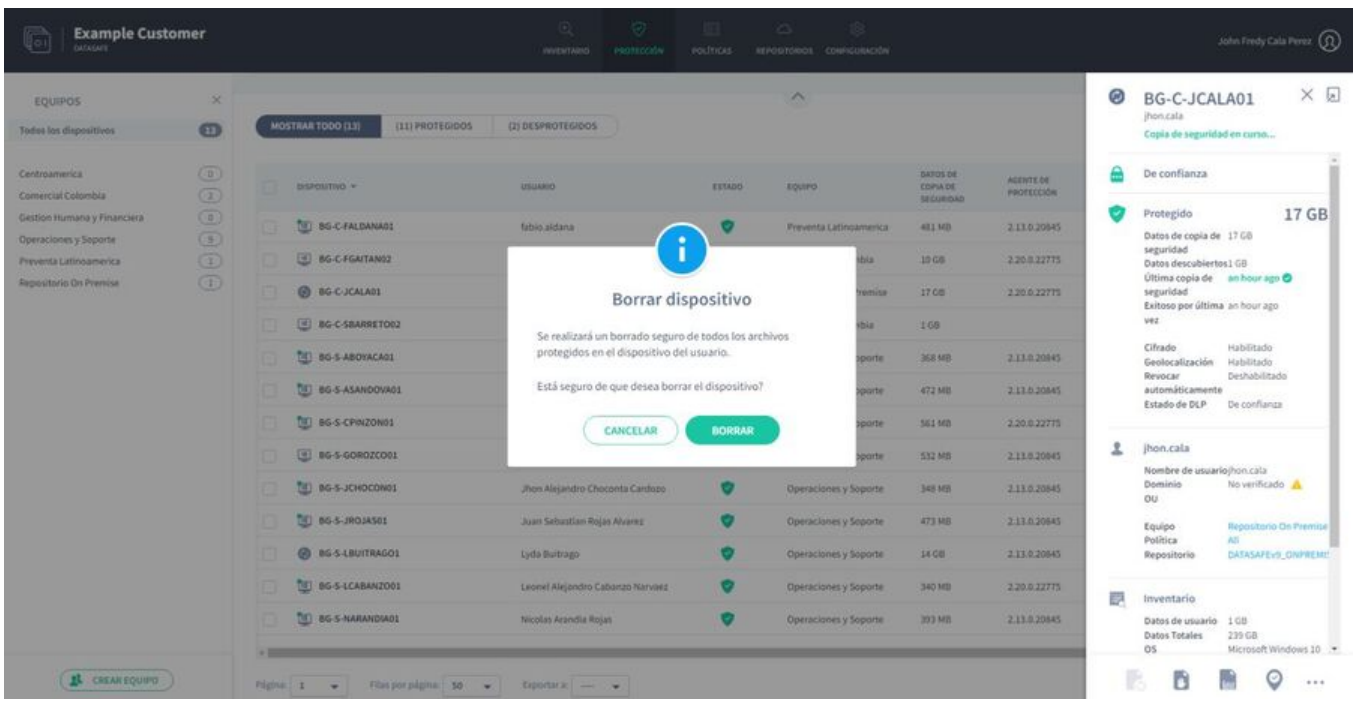
2. En la lista de dispositivos, haga clic en el dispositivo que desea borrar.

3. Haga clic en el ícono **Borrar**.

4. Haga clic en **Borrar** para confirmar. La limpieza se establece como pendiente y, tras un breve retraso, comienza la limpieza. Mientras la limpieza está pendiente, puede cancelarla (haga clic en el ícono **Cancelar Borrarado** en el panel deslizante del dispositivo o en la página Dispositivo). Cuando ha comenzado la limpieza, no se puede cancelar.

La cantidad de tiempo que se tarda en completar el borrado varía, según el tamaño y la velocidad del disco.

⚐ **Nota:** El ícono de borrado también está disponible en la página de perfil del dispositivo (desde la página de **Inventario o Protección**, muestre el panel deslizante del dispositivo y luego haga clic en el ícono de ver detalles para mostrar la página de perfil del dispositivo).



Anular Revocación de Dispositivo

En Aranda Datasafe, puede revocar un dispositivo para que sus archivos protegidos se vuelvan inaccesibles. Esto es para mantener sus datos seguros en caso de pérdida o robo de un dispositivo. Si se encuentra el dispositivo, puede hacer que los datos sean accesibles nuevamente usando **Anular revocación**.

Con una anulación de revocación, Aranda Datasafe vuelve a colocar el certificado de cifrado en el dispositivo revocado. Una vez que el certificado está en el dispositivo, no se puede revocar y se puede acceder a sus datos protegidos.

Para anular la revocación de un dispositivo:

1. Haga clic en **Inventario** o **Protección**.

2. En la lista de dispositivos, haga clic en el dispositivo que desea anular la revocación. Aparece el panel deslizable del dispositivo.

3. Haga clic en el ícono **Anular revocación de dispositivo**.

4. Haga clic en **Anular revocación** para confirmar. Se realiza la solicitud para anular la revocación del dispositivo y la anulación está pendiente. Cuando Aranda Datasafe completa la solicitud, se completa la revocación.

Mientras la anulación de revocación está pendiente, puede cancelar la solicitud de anulación de revocación si es necesario (muestre el panel deslizante del dispositivo o la página del dispositivo y luego haga clic en el ícono **Cancelar anular revocación**).

Estado de Prevención de Pérdida de Datos

Puede ver el estado de **DLP** en la sección **Protección**. Muestra la cantidad de dispositivos que tienen habilitadas las funciones de encriptación local, revocación automática y geolocalización (en la Política).

El estado de DLP también se muestra en la lista de dispositivos en la parte inferior de la sección **Protección**.

Migración Remota

Migración Remota

Nuestra solución de migración de dispositivos remotos transfiere todos los datos del usuario y la configuración de su perfil a la nueva máquina, mientras el usuario trabaja. La transferencia de datos es completamente segura y no corre el riesgo de perder ningún archivo de usuario.

El personal de TI puede administrarlo de forma remota y los usuarios pueden simplemente comenzar a usar la nueva máquina con todas sus configuraciones y

archivos exactamente como estaban en su computadora anterior.

- Activa y supervisa de forma remota varias migraciones desde Aranda Datasafe
- Migración de dispositivo a dispositivo (sin necesidad de almacenamiento de repositorio adicional)
- Mejor descubrimiento de rutas de red
- Abrir / cerrar automáticamente el firewall de Windows
- Migraciones en vivo (inicial completa y actualizaciones para las siguientes)
- Capacidad de reintento de conexión
- Compresión y cifrado
- Migrar todos los datos (incluidos los comerciales y personales)
- Migración de acceso directo a nuevas ubicaciones
- Migrar ubicaciones de unidades en la nube (no de configuración)

- Migración de perfiles
    - Configuración de la barra de tareas, opciones de carpeta de Windows, unidades de red
    - Microsoft Outlook: todas las cuentas de correo electrónico, archivos PST, firma de correo electrónico.

Preparación para Migración Remota

Antes de que pueda migrar, se necesitan las siguientes comprobaciones:

Las máquinas de origen y destino deben estar preparadas

- Ambas máquinas deben estar en estado **Activo** y visibles en la ventana **Protección** en Aranda Datasafe.
- El usuario relevante debe iniciar sesión en ambas máquinas.
- La máquina de destino debe tener Windows y las aplicaciones instaladas antes de la migración. Muchos clientes utilizan una imagen de empresa estándar para sus máquinas.

Preparando el dispositivo de destino

- Debe haber suficiente tamaño de disco en el dispositivo de destino.
- Es importante que la configuración o la partición del disco sea la misma en ambos dispositivos. Si el dispositivo de origen tiene un volumen C: \ & D: \, por ejemplo, y el dispositivo de destino solo tiene un volumen C: \, la migración de los datos en D: \ fallará.
- Asegúrese de que las aplicaciones como MS Office, Antivirus y otras aplicaciones de la empresa estén instaladas antes de ejecutar la migración. La información de **Inventario** en Aranda Datasafe mostrará todas las aplicaciones que están instaladas en el dispositivo de **Origen**.
- Descubrir y activar el dispositivo de destino en Aranda Datasafe si aún no está activo y visible en la ventana de Protección.

¿Qué puedo esperar de la migración?

La función de migración remota completa copiará todos los datos del usuario y la configuración del perfil en el dispositivo de destino.

¿Qué se incluirá en la configuración del perfil?

- Perfil de correo electrónico para Microsoft Outlook
- Firmas de correo electrónico
- Archivos de almacenamiento de correo electrónico (archivos PST)
- Ubicaciones de unidades mapeadas
- Impresoras de red
- Vistas de carpeta personalizadas
- Preferencias de la barra de tareas

¿Qué quedará excluido de la migración?

- Aplicaciones
- El archivo incorporado excluye como ejecutables, archivos de sistema y archivos temporales
- Se excluirán los archivos bloqueados
- Discos y volúmenes que no existen en el dispositivo de destino
- La migración fallará si el tamaño del disco de destino es menor
- No se incluirán las impresoras conectadas localmente
- El fondo del escritorio no se migrará

Realización de Migración Remota

Iniciar una migración desde Aranda Datasafe

1. Navegue a Protección en Aranda Datasafe.

2. Utilice la función de búsqueda en el panel de la lista de dispositivos y busque el usuario que le gustaría migrar.

3. La búsqueda debe dar como resultado al menos dos dispositivos para el usuario. El dispositivo actual y el nuevo dispositivo

4. Haga clic en el dispositivo de destino para abrir el panel lateral.

5. Haga clic en los 3 puntos en la parte inferior derecha del panel lateral y seleccione Migrar.

6. Seleccione el dispositivo desde el que migrar en el menú desplegable y continúe.

7. La migración comenzará y mostrará el progreso.

Monitoreo

Después de iniciar la migración, el administrador puede continuar monitoreando el progreso desde Aranda Datasafe. Es posible que la ventana se cierre mientras se realizan otras tareas de gestión.

El administrador puede verificar en cualquier momento el progreso de la migración, haciendo clic en cualquiera de los dispositivos involucrados en la migración y abriendo los detalles del evento desde el panel lateral.

Realizar una migración de actualización

Una vez que se ha completado la migración remota completa inicial, hay algunos pasos más antes de entregar el dispositivo de destino al usuario:

- En el caso de que un usuario estuviera trabajando en la máquina de origen mientras se estaba ejecutando la migración, es posible que algunos archivos estén bloqueados. Esto será visible en los detalles del evento de migración.
- Es importante que el usuario cierre todas las aplicaciones durante la migración de actualización (posterior).
- En Aranda Datasafe puede iniciar otra migración. Esto migrará cualquier dato que estuviera en uso por el usuario en el momento de la ejecución de la migración inicial.
- Una vez que la migración de la actualización se haya completado con éxito, puede realizar un cierre de sesión / inicio de sesión para aplicar la configuración del perfil al nuevo dispositivo.
- Asegúrese de aplicar otras configuraciones que no estén cubiertas por la función de migración remota completa.
- Entregue el nuevo dispositivo al usuario y confirme con él que se ha migrado todo.

Detalles del evento

Cuando se haya completado la migración remota completa, podrá ver los resultados y los detalles del evento de migración. Seleccione el dispositivo de destino en Aranda Datasafe y haga clic en el nombre del dispositivo junto a Migrado desde.

Se mostrará la siguiente información:

- Horas de inicio y finalización
- Número de archivos migrados
- Tamaño de la migración
- Archivos exitosos vs fallidos con motivos de falla

Migración

Migración

La función de migración de Aranda Datasafe facilita la transferencia de la configuración del perfil de usuario de un dispositivo a otro. El uso de la función de migración puede ahorrarle mucho tiempo y esfuerzo cuando necesite actualizar o reemplazar sus dispositivos.

Migración de la configuración del perfil

Con la función de migración de la configuración del perfil, puede hacer una copia de seguridad de los datos del usuario y la configuración del perfil en un dispositivo en Aranda Datasafe. Luego, puede restaurarlos en otro dispositivo. Esto hace que sea más fácil y rápido transferir datos de usuario comunes, como accesos directos de escritorio, archivos de escritorio, documentos, etc.

Para usar la función de migración, debe [habilitarla en la Política] que usa el dispositivo que desea reemplazar.

Cuando la migración está habilitada, Aranda Datasafe hará una copia de seguridad de los datos del usuario y la configuración del perfil. Esto tiene lugar al mismo tiempo que la próxima copia de seguridad de datos comerciales (como se define en la Política).

Cuando se haya realizado una copia de seguridad de los datos del usuario y la configuración del perfil, puede restaurarlos en un nuevo dispositivo.

Ejemplo: Digamos que tiene una computadora portátil respaldada y protegida por Aranda Datasafe. La computadora portátil será reemplazada por un modelo más nuevo.
Utiliza la función de migración para hacer una copia de seguridad de los datos de usuario y la configuración del perfil de la computadora portátil actual.

Cuando llegue la nueva computadora portátil, descubrirás y activarás el dispositivo en Aranda Datasafe. Luego, usa la función Restaurar para transferir los datos de usuario y la configuración del perfil de la computadora portátil antigua desde Aranda Datasafe a la nueva computadora portátil.

Su nueva computadora portátil se actualiza con los datos de usuario y la configuración del perfil (perfil y firmas de Outlook, unidades de red asignadas y varias configuraciones de carpeta y barra de tareas, etc.).

Habilitar función de migración de perfil de usuario

Puede utilizar la función de migración de perfil de usuario de Aranda Datasafe para hacer una copia de seguridad de la información del perfil de usuario de Windows en un dispositivo. Luego, puede transferir la información a un dispositivo diferente realizando una restauración.

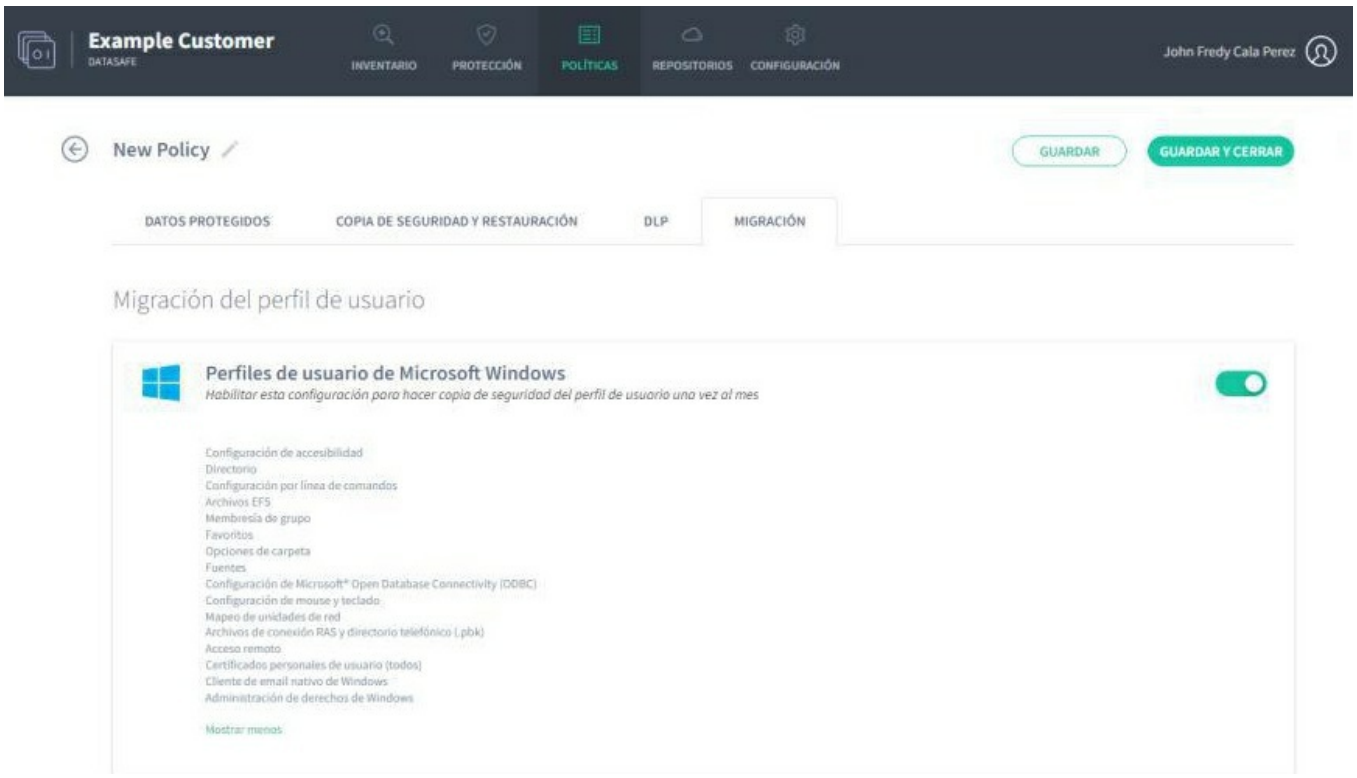
Para usar la migración de perfil, habilítela en la Política utilizada por el dispositivo que desea respaldar:

1. Haga clic en **Políticas**.

2. Edite la Política asociada con el Equipo al que pertenece el dispositivo.

3. Haga clic en **Migración**.

4. Utilice el control deslizante para habilitar la migración de**perfiles para los perfiles de usuario de Microsoft** Windows. (El verde está habilitado, el gris está deshabilitado).



4. Haga clic en el enlace **Mostrar más** para ver una lista completa de la información del perfil de usuario de Windows que se respaldará. Incluye el diseño de la barra de tareas, unidades de red asignadas, opciones de carpeta, cuentas de correo electrónico, archivos pst adjuntos anteriormente y firmas de correo electrónico.

5. Haga clic en **Guardar y cerrar**.

Aranda Datasafe respaldará los datos del usuario y la configuración del perfil en todos los dispositivos asociados con esta Política. La copia de seguridad del perfil se realizará cuando se realice la siguiente copia de seguridad de los datos comerciales (según lo programado en la Política). Se ejecutará una vez cada 30 días para garantizar que se actualice periódicamente.

Cuando se ha realizado una copia de seguridad, puede migrar la[configuración a un nuevo dispositivo](#) .

Deshabilitar función de migraciónde perfil de usuario

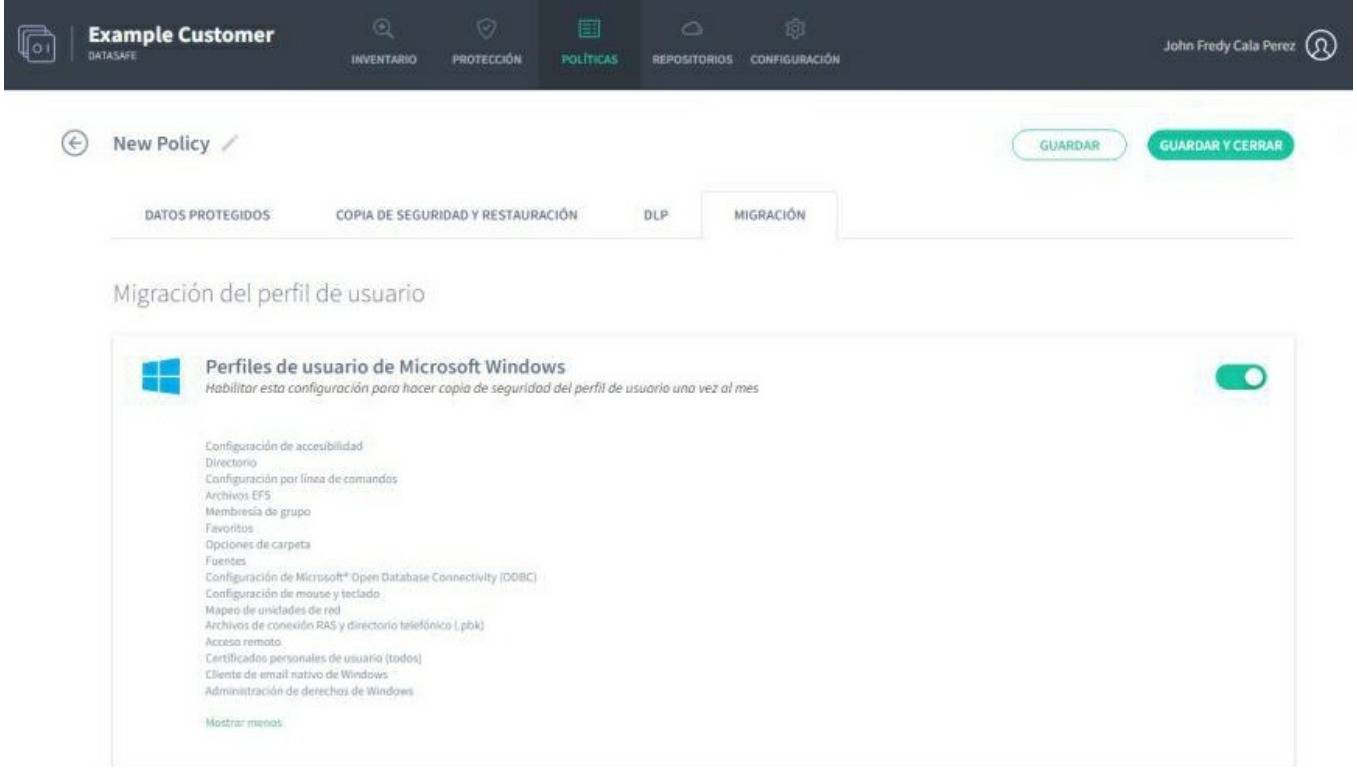
Para deshabilitar la función de migración del perfil de usuario para que Aranda Datasafe no haga copias de seguridad de los datos del perfil de usuario de Windows:

1. Haga clic en **Políticas**.

2. Edite la Política asociada con el Equipo al que pertenece el dispositivo.

3. Haga clic en **Migración**.

4. Utilice el control deslizante para deshabilitar la migración de perfiles para los**perfiles de usuario de Microsoft Windows**. (El gris está desactivado, el verde está desactivado).



5. Haga clic en **Guardar y cerrar**.

Aranda Datasafe **no** realizará una copia de seguridad de los datos y perfiles del usuario en todos los dispositivos asociados con esta Política.

Migrar datos de perfil de Usuario a dispositivo

Si ha habilitado la migración en una Política, puede usar Restaurar para transferir los datos del perfil de usuario de Windows (y los datos de respaldo) desde un dispositivo antiguo a un dispositivo nuevo (a través de Aranda Datasafe).

> ⚐ **Nota:** Solo puede restaurar los datos del perfil de usuario desde otro dispositivo si la migración está habilitada y se ha realizado una copia de seguridad del dispositivo "antiguo". Para saber cómo habilitar la función de migración, consulte Habilitar la función de migración.

Para **restaurar** archivos en un dispositivo:

1. Inicie sesión en el nuevo dispositivo.

Si el dispositivo ya tiene instalado Discovery Agent, ignore los pasos 2 y 3 y continúe desde el paso 4.

Si necesita restaurar datos a un nuevo dispositivo o un dispositivo que no ha sido protegido por Aranda Datasafe antes, necesita instalar Discovery Agent. Continúe desde el paso 2.

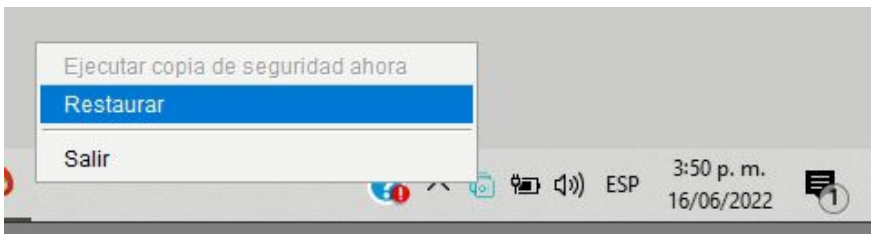
2. Instale Discovery Agent en el dispositivo, para que Aranda Datasafe pueda detectarlo. Si necesita más información, consulte Instalación y despliegue de Discovery Agent.

3. En Aranda Datasafe, active el nuevo dispositivo.

Si necesita más información, consulte Activación de sus dispositivos.

> ⚐ **Nota:** Aranda Datasafe utiliza la cuenta de usuario de Windows en el nuevo dispositivo para identificar qué dispositivo antiguo se está reemplazando. Asigna automáticamente el nuevo dispositivo al mismo equipo y perfil que el dispositivo anterior.

4. En la barra de tareas de Windows, haga clic con el botón derecho en el ícono del Agente de protección y seleccione Restaurar.

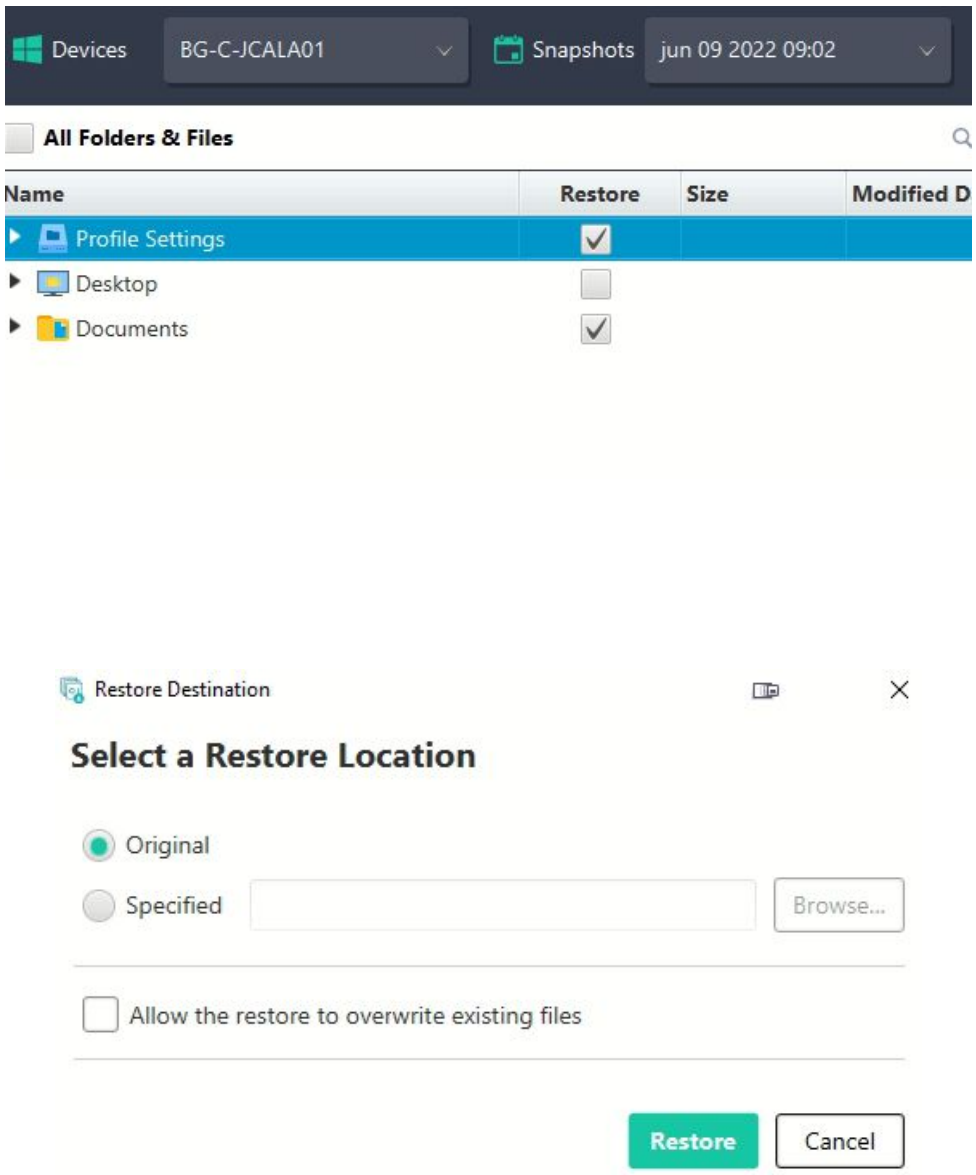


> ⚐ **Nota:** Si no se muestra el ícono del Agente de protección, busque la aplicación Agente de Aranda en su dispositivo y luego ejecútela.

5. Elija los datos que desea migrar y la ubicación de los datos migrados.

- Utilice la opción Dispositivos para elegir el dispositivo "antiguo" que tiene los datos que desea migrar al dispositivo "nuevo".
- Utilice la opción Instantáneas para elegir la instantánea que desea migrar al nuevo dispositivo. La instantánea es un registro de los datos de un dispositivo en un momento específico. En la mayoría de los casos, querrá seleccionar la instantánea más reciente.
- Utilice las casillas de verificación Restaurar para elegir los datos que se migrarán. Seleccione todos los datos que desea restaurar y también la Configuración del perfil (perfil de usuario de Windows).
- Haga clic en Restaurar.
- Elija Restaurar ubicación para los datos migrados en el nuevo dispositivo. Puede elegir Original para migrar los datos a la misma ubicación que tenía en el

dispositivo anterior o elegir Especificado para establecer una ubicación diferente.



1. Haga clic en Restaurar.

Los datos de usuario seleccionados y la información del perfil se descargan de Aranda Datasafe a su nuevo dispositivo. Si ha elegido archivos de escritorio, los verá aparecer en el escritorio.