
Aranda Data Safe

Bem-vindo ao Tutorial Introdutório do Aranda Datasafe. Se você é novo no Aranda Datasafe, este é o lugar perfeito para aprender a:

- Descubra seus dispositivos e dados.
- Configure seus computadores, repositórios e conectores do Active Directory.
- Crie políticas para configurar as opções de Backup e Prevenção de Perda de Dados.
- Execute backups e restaurações.
- Saiba como usar os recursos de prevenção contra perda de dados, como criptografia local, limpeza remota e geolocalização.
- Saiba como usar o recurso de migração remota completa.

O tutorial é dividido em uma série de etapas. Você precisa completá-los em sequência, começando com a Etapa 1 - Ativação da conta de administrador

Iniciando dados com segurança

Requisitos do sistema

Requisitos de hardware

Requisitos de hardware para Storage Vault

Os requisitos de hardware para o Storage Vault podem variar dependendo do número de dispositivos que você precisa proteger. As tabelas a seguir mostram nossas recomendações.

Especificação	1-250 Usuários	251-500 Usuários	500-800 Usuários
Sistema operacional	- Windows Server 2016 - 2019 - CentOS 6.x - 9.x - Debian 6.x - 11.x - Ubuntu 22.04 ou posterior	- Windows Server 2016 - 2019 - CentOS 6.x - 9.x - Debian 6.x - 11.x - Ubuntu 22.04 ou posterior	- Windows Server 2016 - 2019 - CentOS 6.x - 9.x - Debian 6.x - 11.x - Ubuntu 22.04 ou posterior
CPU	CPU 4 Núcleos	6 Núcleos / vCPUs	8 Núcleos / vCPUs
Memória	6 GB	8 GB	16 GB
Armazenamento - Vault(~20 GB por usuário)	5 TB	10 TB	16 TB +
Armazenamento – Índice do Vault	N/A	SSD de 50 GB	SSD de 50 GB

Requisitos do agente

Aqui estão os requisitos de sistema recomendados para que os dispositivos executem com êxito o Aranda Agent:

Especificação	Descrição
Sistema operacional	Windows 10/11 Pro ou Enterprise
CPU	Intel i3, i5, i7 ou equivalente AMD
Memória RAM	384 MB disponíveis para o agente
Armazenamento	500 MB livres *Unidade de estado sólido para melhor desempenho.

Requisitos de rede

Solicitação	Descrição
Resolver o nome DNS do locatário EPC	nslookup endpointcloud.com
Permitir acesso à Internet ao locatário	O firewall e o proxy devem permitir a comunicação com: .endpointcloud.com Permitir comunicação de saída na porta 443.
O Firewall deve permitir a comunicação dos dispositivos cliente com o servidor de cofre de armazenamento.	Entrada e saída pela porta 9000 no servidor do cofre de armazenamento.

Requisitos do Active Directory Connector

O AD Connector poderá ser instalado no mesmo hardware que o Storage Vault. Se você não tiver um cofre local/local, precisará das seguintes especificações mínimas de hardware para a instalação do AD Connector:

Solicitação	Descrição
Sistema operacional	Windows Server 2016 - 2019
CPU	4 Núcleos / vCPUs
Memória RAM	4 GB (requisito de sistema operacional incluído)
Armazenamento	500MB livres.

Active Directory e requisitos de acesso

Os seguintes requisitos devem ser atendidos para fornecer acesso:

Requisitos	Descrição
Domínio do AD para autenticação de usuário	Domínio do AD para autenticação de usuário Para integração do AD, é necessário um domínio do AD. O domínio não é necessário para a implantação do grupo de trabalho.
O AD Connector deve ser instalado em um servidor ingressado no domínio do Active Directory.	Deve ser o mesmo domínio do AD usado para autenticar o usuário.
A conta de administrador do Windows Server deve ter permissões suficientes.	Você deve ter permissões para: Instalar software e serviços. Registre um registro SPN no domínio. Acesse https://endpointcloud.com
Os firewalls devem permitir que os dispositivos do cliente se comuniquem com o Storage Vault.	Porta 9000 de entrada e saída.

Ative sua conta de administrador

Para começar, ative sua conta de administrador para que você possa fazer login e configurar o Aranda Datasafe.

⚐ > Observação: quando sua organização se registrar no Aranda Datasafe, um administrador de conta enviará um convite por e-mail. Se você não receber o e-mail, verifique suas pastas de spam. Se você ainda não conseguir encontrar o e-mail, entre em contato com a Aranda reportedecasos@arandasoft.com atendimento ao cliente. Depois de receber o e-mail, clique em **Ativar conta**. Seu navegador abre a página da web de ativação. Na primeira vez que você acessar o Aranda Datasafe, precisará inserir uma senha e digitá-la novamente para confirmar. Clique em **Ativar** para fazer login. Se você for o primeiro administrador a fazer login, receberá automaticamente a função de **Oficial de Segurança**. Se não for o primeiro, ele receberá uma função de**administrador**. (Isso pode ser alterado posteriormente, se necessário.)A função de Responsável pela Segurança é a função de classificação mais alta e permite que você baixe e registre o conector do AD usado para autenticação do usuário.

Instalar o Discovery Agent

Você pode usar o aplicativo gratuito Discovery Agent para que o Aranda Datasafe detecte os dispositivos de seus usuários automaticamente.

Para configurar o Discovery Agent, baixe-o e instale-o em cada dispositivo do usuário final. Não o instale em seu servidor.

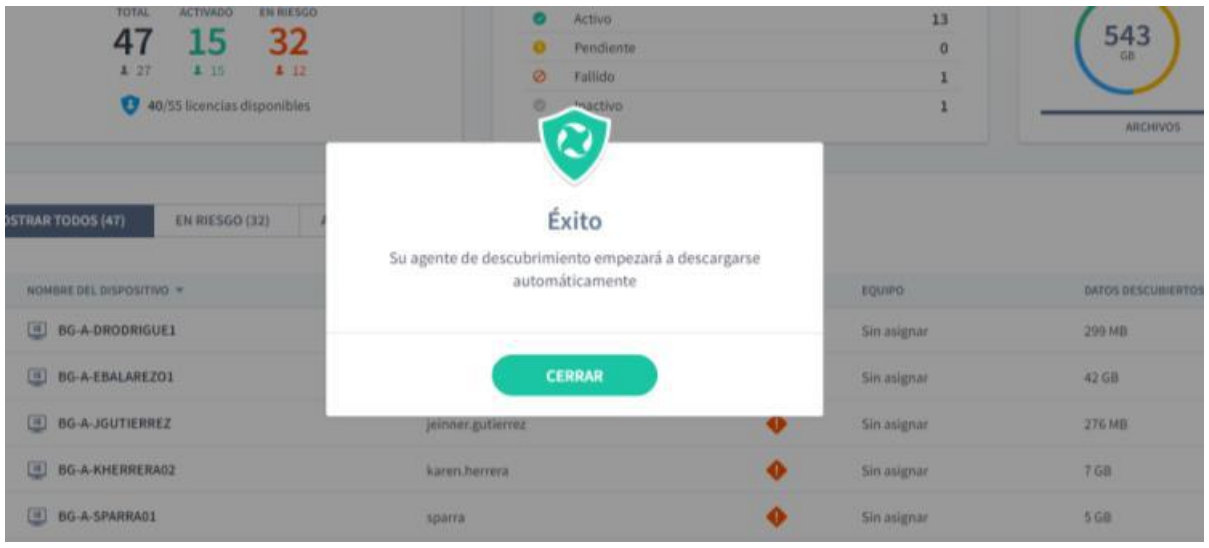
Baixe o Discovery Agent

Você pode baixar o Discovery Agent no console do Aranda Datasafe:

1. Faça login como administrador. Quando você efetua login como administrador pela primeira vez, o Inventário é selecionado por padrão. Nesta fase, o Aranda Datasafe não descobriu nenhum dispositivo.

2. Clique em Baixar Discovery Agent. O pacote MSI do Discovery Agent é baixado para o navegador. O Discovery Agent é específico para sua instância do Aranda

Datasafe.



Instale o Discovery Agent em seus dispositivos de usuário

Instale o pacote do MSI Discovery Agent em cada dispositivo de usuário (desktop, laptop etc.). O agente de descoberta executará um inventário de dispositivos e dados e, em seguida, carregará com segurança as informações no Aranda Datasafe.

Pré-requisitos

- Os dispositivos do usuário devem ter acesso à Internet, pois o Discovery Agent precisa se conectar ao Aranda Datasafe.
- Os dispositivos do usuário devem usar um sistema operacional Windows, Windows 7 ou posterior. Uma versão para Mac estará disponível em breve.
- Firewalls e servidores proxy devem permitir conexões. Talvez seja necessário colocar endpointcloud.com na lista de permissões e o caminho completo para a URL do locatário do Aranda Datasafe. Exemplo: https://arandasoftware.endpointcloud.com em que "arandasoftware" é substituído pelo nome da sua organização.

Você pode instalar o Discovery Agent manual ou remotamente em cada dispositivo.

Instalação manual do agente

O Discovery Agent pode ser instalado executando o pacote MSI em cada dispositivo de usuário.

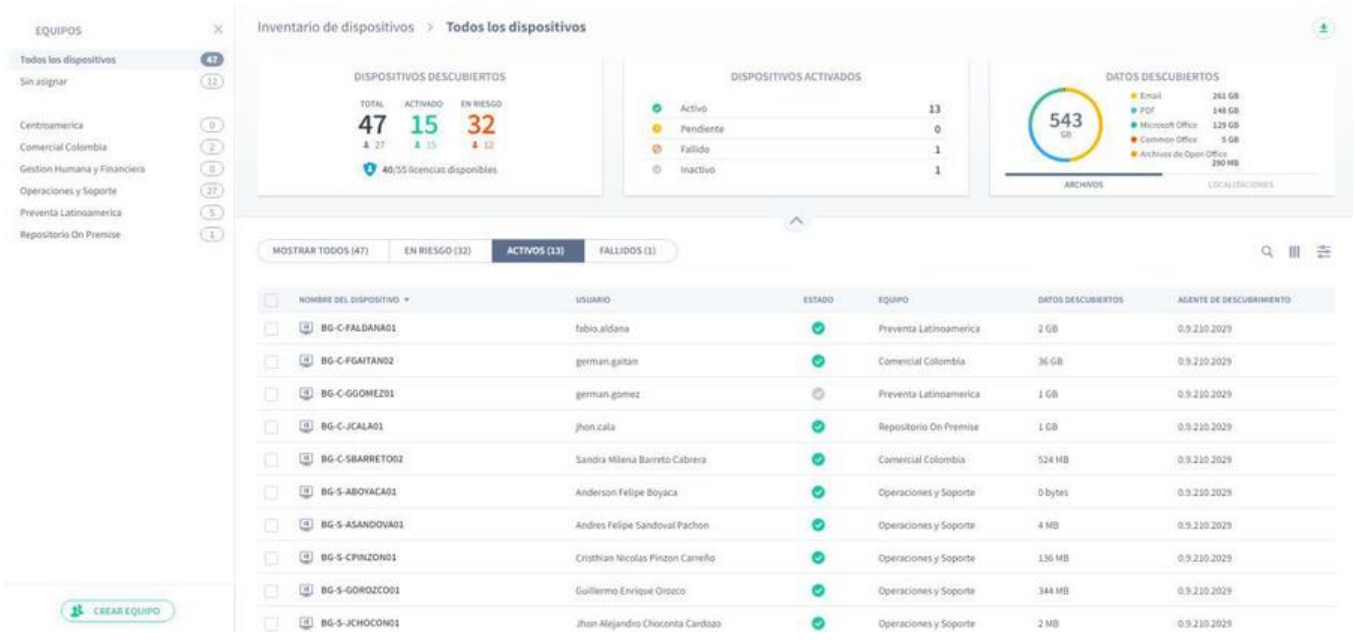
Talvez você queira mover o pacote MSI para uma pasta compartilhada que possa ser acessada por todos os dispositivos. Como alternativa, você pode colocar o pacote MSI em um cartão de memória e transferi-lo entre dispositivos dessa maneira.

Instalação do Agente Remoto

Você pode instalar o pacote MSI em dispositivos remotamente, usando o recurso Política de Grupo do Active Directory ou um aplicativo de terceiros. Para obter mais detalhes, entre em contato com o Suporte da Aranda (reportedecasos@arandasoft.com).

Inventário

Quando seus dispositivos tiverem o Discovery Agent instalado, eles se reportarão ao locatário do Aranda Datasafe. Você verá os dispositivos aparecerem na lista Inventário e o painel será preenchido com dados.



Visualize as informações de cada uma das seções.

1. **Dispositivos descobertos**: quantos dispositivos foram descobertos, quantos foram ativados para proteção e quantos ainda estão em risco.

2. **Dispositivos ativados**: Útil quando começamos a ativar os dispositivos. Ele nos mostra quantos dispositivos estão pendentes de ativação e quantos falharam.

3. **Dados descobertos**: a quantidade de dados descobertos. Você pode ver o valor com base nos tipos de arquivo ou locais de arquivo.

Há também uma lista de dispositivos que mostra todos os dispositivos que o Discovery Agent descobriu. Há um breve resumo do dispositivo, incluindo a conta de usuário do dispositivo e a quantidade de dados descobertos.

Você pode acessar informações mais detalhadas para cada dispositivo.

1. Clique em um dispositivo na lista de dispositivos. É exibido um painel deslizante que contém um resumo mais detalhado do dispositivo e da conta de usuário associada a ele.

2. Clique no ícone do perfil para exibir todos os detalhes do dispositivo.

3. Clique na seta para trás ao lado do nome de usuário na parte superior da tela para retornar ao Inventário.

Você deve ter notado que no lado esquerdo do Inventário há uma lista de **Equipamentos**. Você o usará para criar novas equipes e organizar seus dispositivos na próxima etapa.

Organizando dispositivos em equipes

Quando seus dispositivos se conectam ao Aranda Datasafe pela primeira vez, eles são "não atribuídos". Isso significa que eles não estão em uma equipe. Você pode criar equipes e usá-las para organizar seus dispositivos em grupos significativos.

Com o Teams, você pode:

- Atribua uma política para controlar as configurações de backup e proteção para um grupo de dispositivos.
- Atribua um repositório onde a equipe fará backups.
- Filtre as informações por uma equipe para que você possa ver informações sobre os dispositivos que são usados na mesma área do seu negócio, por exemplo, você pode ter uma equipe que mostre todos os dispositivos usados para marketing.

Mostraremos como funciona. Crie sua própria equipe ele Atribuir dispositivos e então você pode Visualize as informações nos dispositivos desse computador.

Criar uma equipe

Para criar uma equipe:

1. Clique em **Inventário**.

2. Clique em **Criar equipe** (canto inferior esquerdo da tela Inventário).

3. Insira um nome para a nova equipe.

4. Ignore as configurações Atribuir uma política e Atribuir um repositório por enquanto. Você retornará a eles depois de criar uma Política e um repositório.

5. Clique em Salvar computador.

Atribuir um dispositivo a uma equipe

Depois de configurar suas equipes, você pode usá-las para organizar seus dispositivos descobertos:

1. Passe o mouse sobre um dispositivo na lista de dispositivos.

2. Clique no botão de opção no dispositivo (...).

3. Clique em Atribuir equipe.

4. Atribua o dispositivo a uma equipe na lista.

5. Clique em Atribuir.

A página será atualizada automaticamente e o dispositivo será atribuído à equipe selecionada. Agora você pode usar o Inventário para exibir informações sobre todos os dispositivos, dispositivos não atribuídos ou dispositivos em cada um dos seus computadores.

Ver os dispositivos de uma equipe

Quando você organiza seus dispositivos em computadores, pode filtrar o inventário para que ele mostre apenas informações sobre os dispositivos em um computador específico.

1. Clique em Inventário.

2. Na seção Equipes, clique em:

- **Todos os dispositivos** para exibir informações sobre todos os dispositivos em todos os dispositivos

- **Não atribuído** para exibir informações apenas para os dispositivos que ainda não estão atribuídos a uma equipe
- **** para exibir informações sobre dispositivos em uma equipe específica. Selecione vários dispositivos mantendo pressionada a tecla CTRL e clicando nos computadores.

Instalar repositório

Você precisa configurar um repositório no qual seus dispositivos serão copiados.

Um repositório é uma área de armazenamento que pode ser instalada em um servidor local ou em um servidor remoto em um data center. Armazena com segurança os dados de backup de seus dispositivos ativados.

Observação: o software Private Cloud Vault está disponível para Windows Server 2019 de 64 bits.

Baixe e instale o pacote Private Cloud Vault – Windows

Para registrar um repositório, você precisará ter o endereço de e-mail e a senha de uma conta de usuário do Aranda Datasafe com a função de administrador ou oficial de segurança.

Para baixar e instalar o pacote Private Cloud Vault:

1. Clique em Repositório.

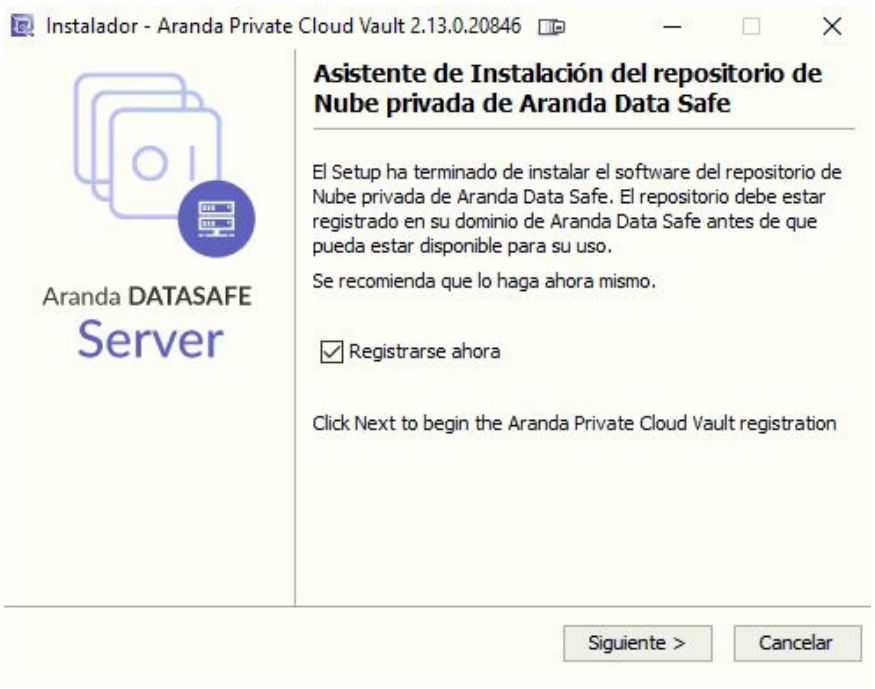
2. Clique em Baixar cofre de nuvem privada.

3. Quando o pacote Private Cloud Vault for baixado, procure-o em seu computador e copie-o para o servidor.

4. No servidor, instale o software Private Cloud Vault. Você pode instalá-lo no local padrão ou escolher outro local, se preferir.

Siga as etapas do assistente de instalação.

Depois de instalar o software, certifique-se de que a opção**Registrar agora** esteja marcada e clique em**Avançar**.



5. Insira os detalhes de registro:

-

Campo	Descrição
Domínio	O nome do seu locatário do Aranda Datasafe. Este é geralmente o nome da sua organização e é a primeira parte do seu endereço Aranda Datasafe.
Nome de usuário	Insira o endereço de e-mail de uma conta do Aranda Datasafe que tenha a função de Administrador ou Oficial de Segurança. Somente essas contas de usuário têm permissão para registrar um repositório.
Senha	Digite a senha da conta Aranda Datasafe.
Nome do host / IP	Insira o nome ou endereço IP do servidor que tem o software do repositório instalado. Se o servidor estiver em um endereço da Internet, insira o URL.
Porta	9000. (Você pode selecionar a porta de sua escolha, mas recomendamos usar 9000.)
Pseudônimo	Digite o nome do repositório como ele aparecerá no Aranda Datasafe.

⚠ > **Importante:** Os agentes de descoberta e os agentes de proteção devem ser capazes de se comunicar na porta 9000.

6. Clique em Inscrever-se e concluir.

Instalar o Active Directory Connector

O Active Directory Connector (AD Connector) é um aplicativo que o Aranda Datasafe usa para autenticar suas contas de usuário, de modo que seus dados criptografados estejam disponíveis apenas para usuários autorizados.

Você deve instalar o AD Connector em um servidor Windows ingressado no domínio que esteja local em sua empresa.

Para baixar, instalar e registrar o software AD Connector:

1. Clique em **Configurações**.

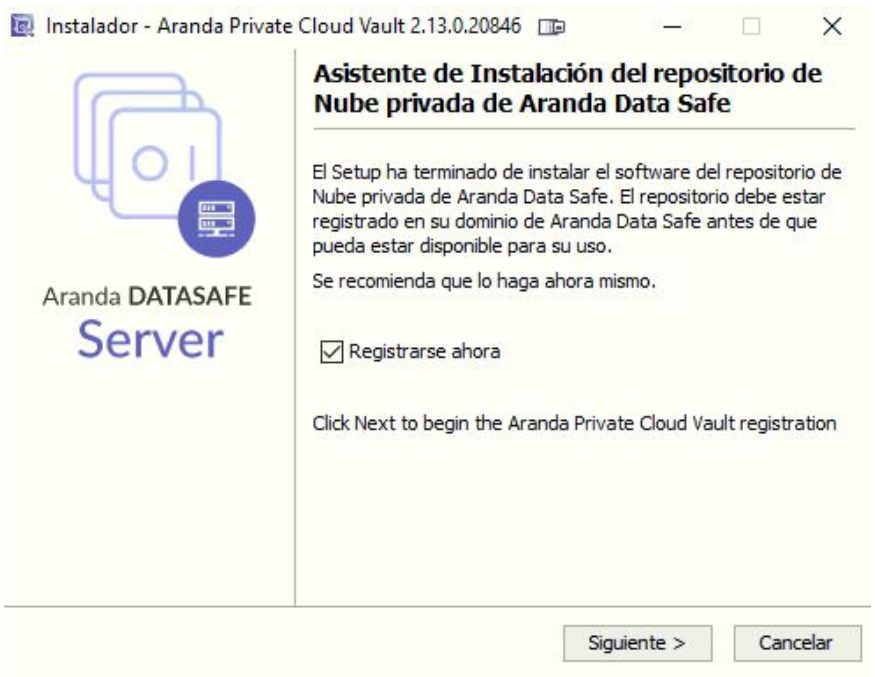
2. Clique em **Active Directory**.

3. Clique em Conectar **Anúncio** para baixar o arquivo executável do adconector. Você precisará copiar este arquivo para o servidor local.

4. Faça login no servidor no qual o AD Connector será executado. Você deve fazer logon por meio de uma conta de usuário administrador de domínio que tenha permissão para registrar um SPN (nome da entidade de serviço) para autenticação Kerberos.

5. Copie o arquivo executável do adconnector para o servidor e execute-o.

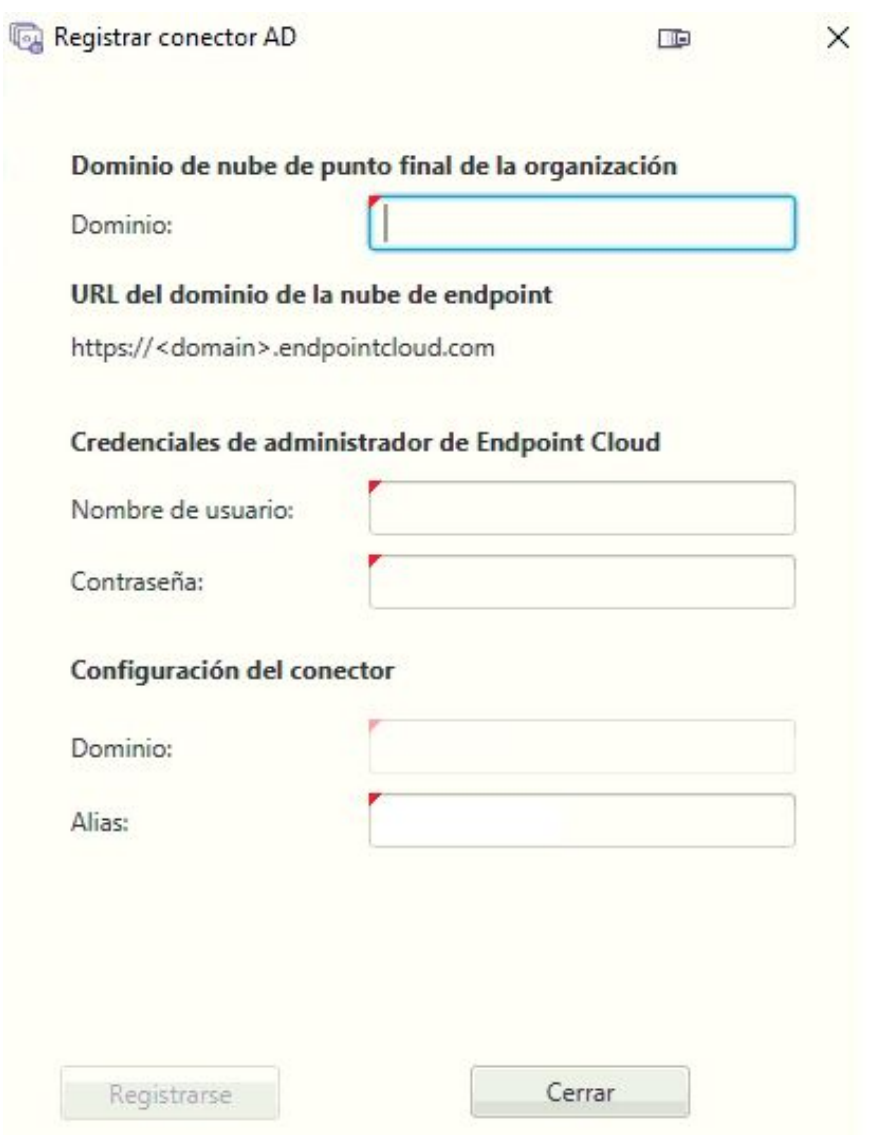
6. Siga as instruções na tela para instalá-lo.



Você pode instalá-lo em qualquer diretório (o local padrão é a unidade C).

Quando você concluir as etapas de instalação, os arquivos começarão a ser extraídos e instalados. Quando os arquivos são instalados, o assistente de instalação pergunta se você deseja se registrar.

7. Certifique-se de que a opção Registrar esteja marcada e clique em Avançar.



8. Insira os detalhes do registro:

Campo	Descrição
Domínio	O nome do seu locatário do Aranda Datasafe. Este é geralmente o nome da sua organização e é a primeira parte do seu endereço Aranda Datasafe.
Nome de usuário	Insira o endereço de e-mail de uma conta do Aranda Datasafe que tenha a função de Responsável de Segurança. Somente contas de usuário do Security Officer têm permissão para registrar um AD Connector.
Domínio	Digite o nome de domínio da organização
Senha	Digite a senha da conta Aranda Datasafe.
Pseudônimo	Insira o nome do conector do AD como ele aparecerá no Aranda Datasafe.

9. . Clique em **Registrar** e **concluir**.

Criar uma política

Uma política é um conjunto de regras que definem:

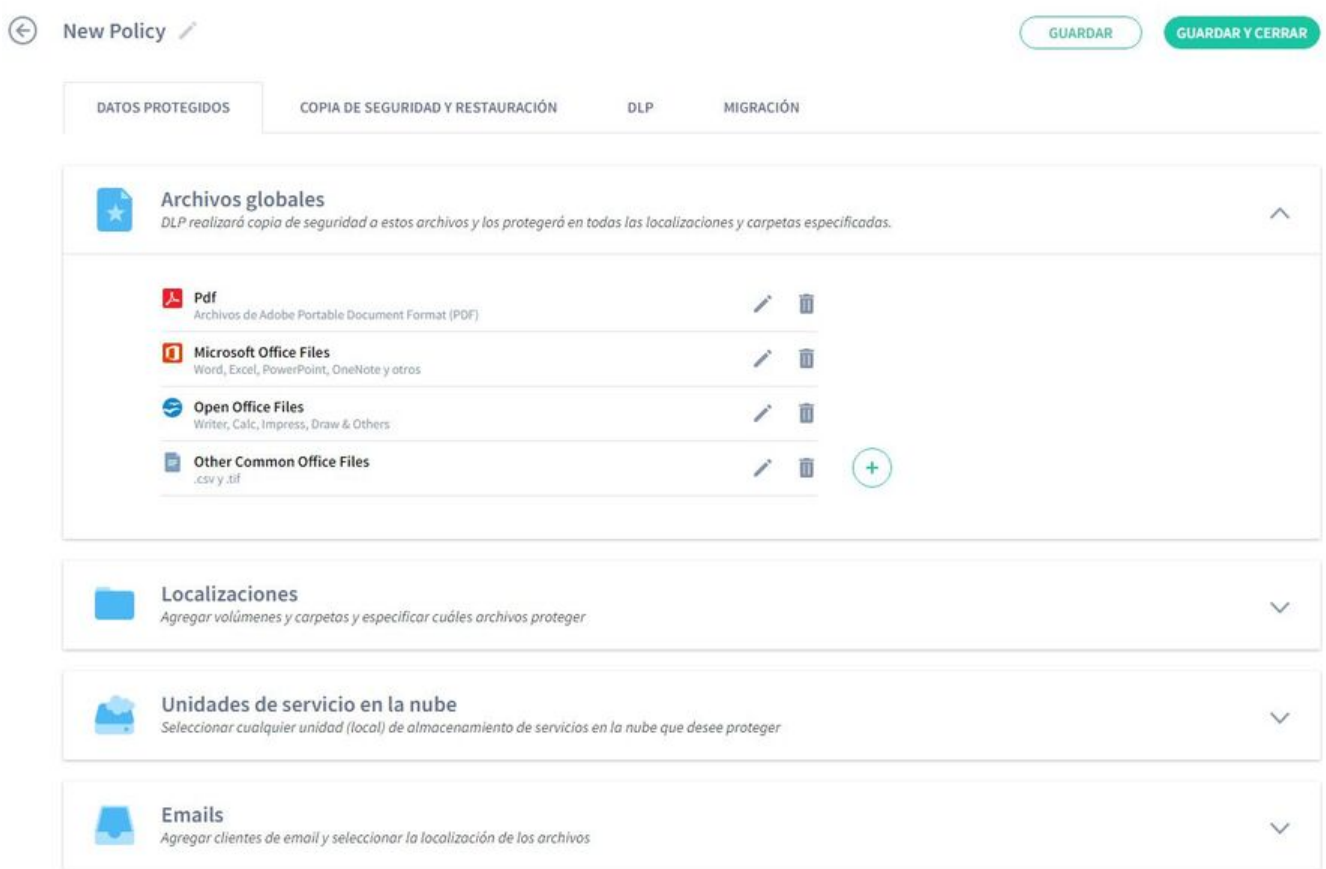
- Quais dados são protegidos e armazenados em backup
- Com que frequência os backups ocorrem
- Se algum recurso de prevenção contra perda de dados for usado para proteger seus dados em caso de perda ou roubo de um dispositivo
- Se for feito backup das configurações de perfil de usuário do Windows.

Você pode criar quantas políticas precisar. Você pode ter uma Política para todos ou pode ter Políticas diferentes para cada equipe.

Crie uma nova política

1. Clique em Políticas.

Se você não tiver uma política no Aranda Datasafe, clique em Adicionar uma política. O Aranda Datasafe cria uma nova Política e a abre, pronta para você definir sua configuração.



2. Insira um nome para a política. Clique no ícone de edição ao lado do nome padrão e insira o novo nome.

Sua nova política tem configurações padrão, e muitos administradores do Aranda Datasafe consideram essas configurações adequadas às suas necessidades. Se você tiver requisitos diferentes, poderá alterar as configurações nas seguintes seções:

Campo	Descrição
Dados protegidos	Ele é usado para definir quais dados são selecionados para proteção.
Backup & Restauração	É usado para escolher com que frequência os backups são realizados.
DLP	É usado para escolher medidas de prevenção de perda de dados para a política.
Migração	Ele é usado para escolher se deseja fazer backup das configurações relacionadas aos perfis de usuário do Windows.

Visualize as escolhas que você pode fazer nas seçõesDados protegidos, Backup e restauração , DLP e Migração.

Dados protegidos

Use as configurações de Dados Protegidos para escolher quais arquivos serão protegidos e copiados (de acordo com as regras definidas na política). As configurações de política definem:

- Quais dados são armazenados em backup e protegidos
- Se a criptografia é aplicada a arquivos no dispositivo local.
- Se o acesso aos dados pode ser revogado automaticamente.
- Se os dados protegidos podem ser apagados de um dispositivo remotamente

Visualize as diferentes seções.

Arquivos Globais

Os arquivos globais são coleções de tipos de arquivo. Por exemplo, há uma coleção de arquivos do Microsoft Office, para arquivos salvos no Word, Excel, PowerPoint, etc. Por padrão, o Aranda Datasafe fará backup desses arquivos 'globais', independentemente de onde eles estejam armazenados nos dispositivos que usam a política.

Você pode usar as configurações de Arquivos Globais para:

- Adicionar ou remover tipos de arquivos de diferentes coleções
- Crie uma nova coleção para diferentes tipos de arquivo. Por exemplo, talvez você queira criar uma nova coleção que contenha os tipos de arquivo para seu software proprietário.

Localizações

Você pode configurar o Aranda Datasafe para fazer backup e proteger arquivos em locais específicos em um computador (somente unidades locais, por padrão). Alguns locais comuns são incluídos por padrão, incluindo Todos os Volumes, Área de Trabalho e Documentos, e você pode adicionar outros locais, se necessário.

Para cada local, você pode escolher quais arquivos serão copiados e protegidos: todos os arquivos, apenas arquivos globais ou um conjunto de arquivos que você escolhe manualmente.

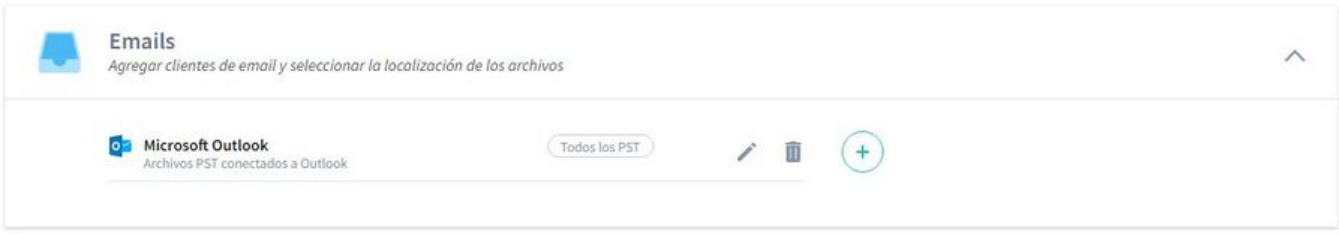
Unidades de nuvem

A seção Cloud Drives funciona da mesma maneira que Locations, exceto que se aplica a locais de armazenamento em nuvem, como One Drive.

Escolha a unidade de nuvem da qual deseja que o Aranda Datasafe faça backup e proteja e, em seguida, opte por incluir todos os arquivos, arquivos globais e/ou uma seleção de arquivos personalizada.

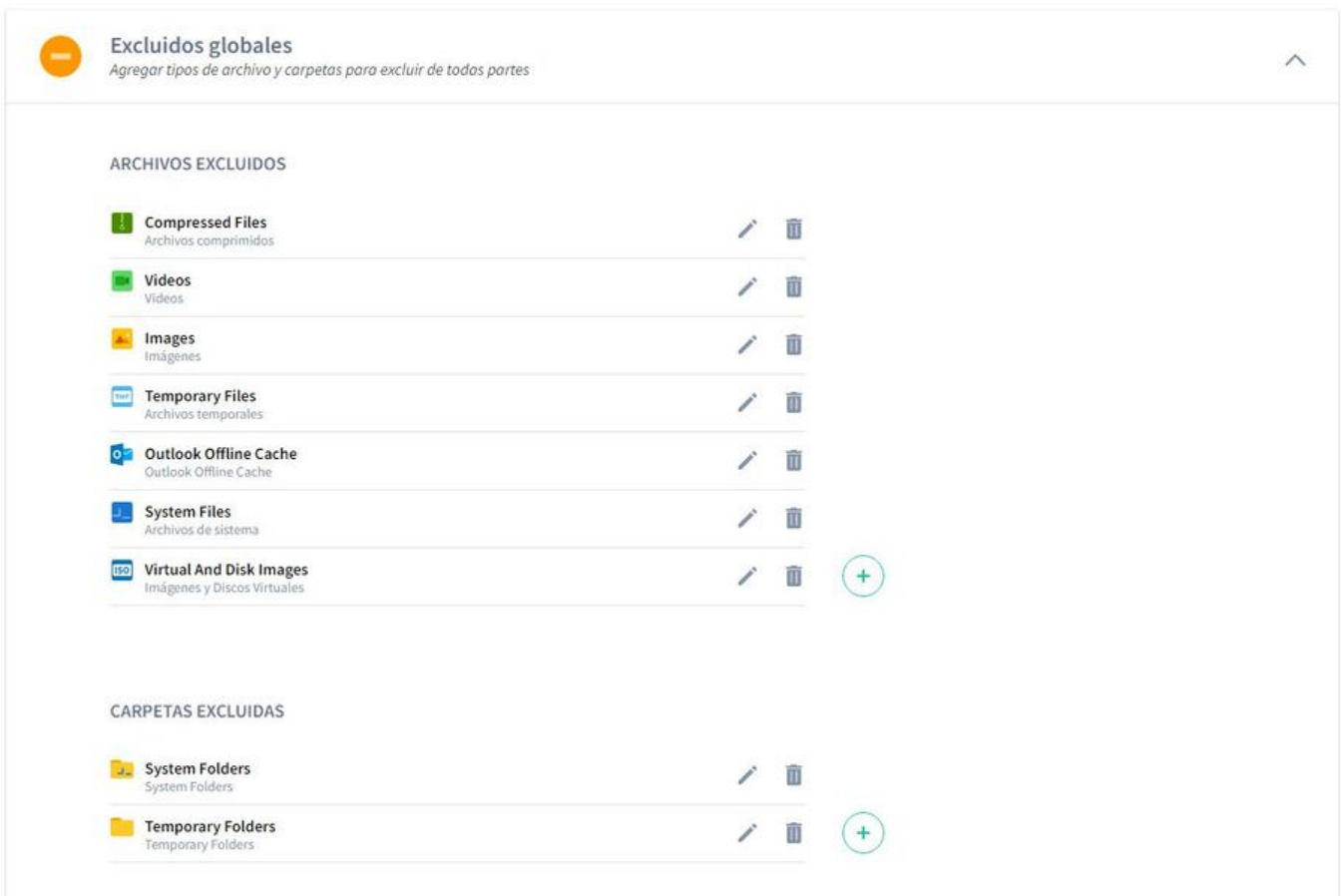
E-mails

Use a seção E-mails para configurar o Aranda Datasafe para fazer backup e proteger seus arquivos de cliente de e-mail. Por exemplo, você pode adicionar o Microsoft Outlook como um cliente de e-mail e, em seguida, configurar o Aranda Datasafe para fazer backup e proteger todos os arquivos PST do Outlook ou apenas os arquivos PST que estão ativos no perfil do Outlook.



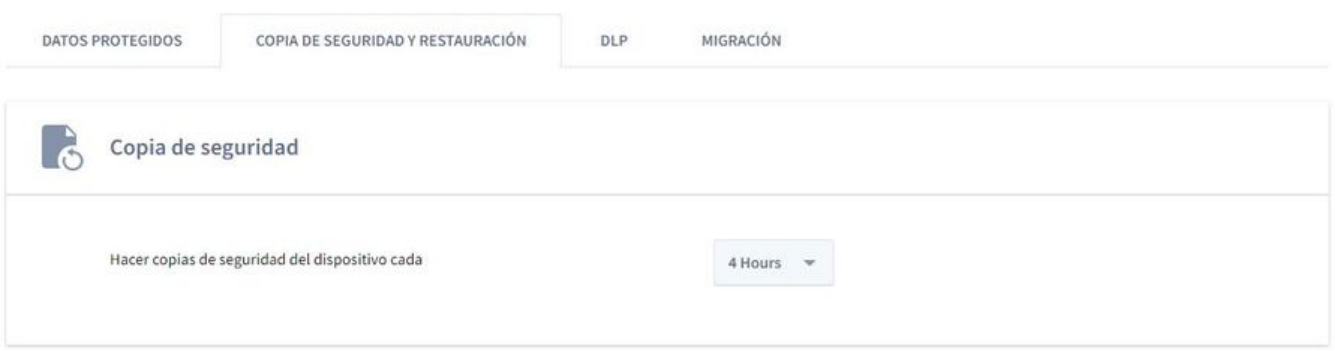
Exclusões globais

Use a seção Exclusões globais para especificar quais tipos de arquivos e pastas não devem ser copiados ou protegidos. Observe que, se uma pasta ou tipo de arquivo estiver incluído em Arquivos Globais e Arquivos Globais Excluídos, não será feito backup ou protegido (os arquivos globais excluídos têm precedência sobre os arquivos globais).



Backup & Restore

Use a guia Backup e restauração para definir o agendamento de backup de dispositivos (que usam a política) regularmente.



DLP

A guia Prevenção contra perda de dados (DLP) é onde você controla as configurações para proteger os dados localmente nos dispositivos. Essas configurações são projetadas para proteger seus dados quando um dispositivo (que usa essa política) é perdido ou roubado.

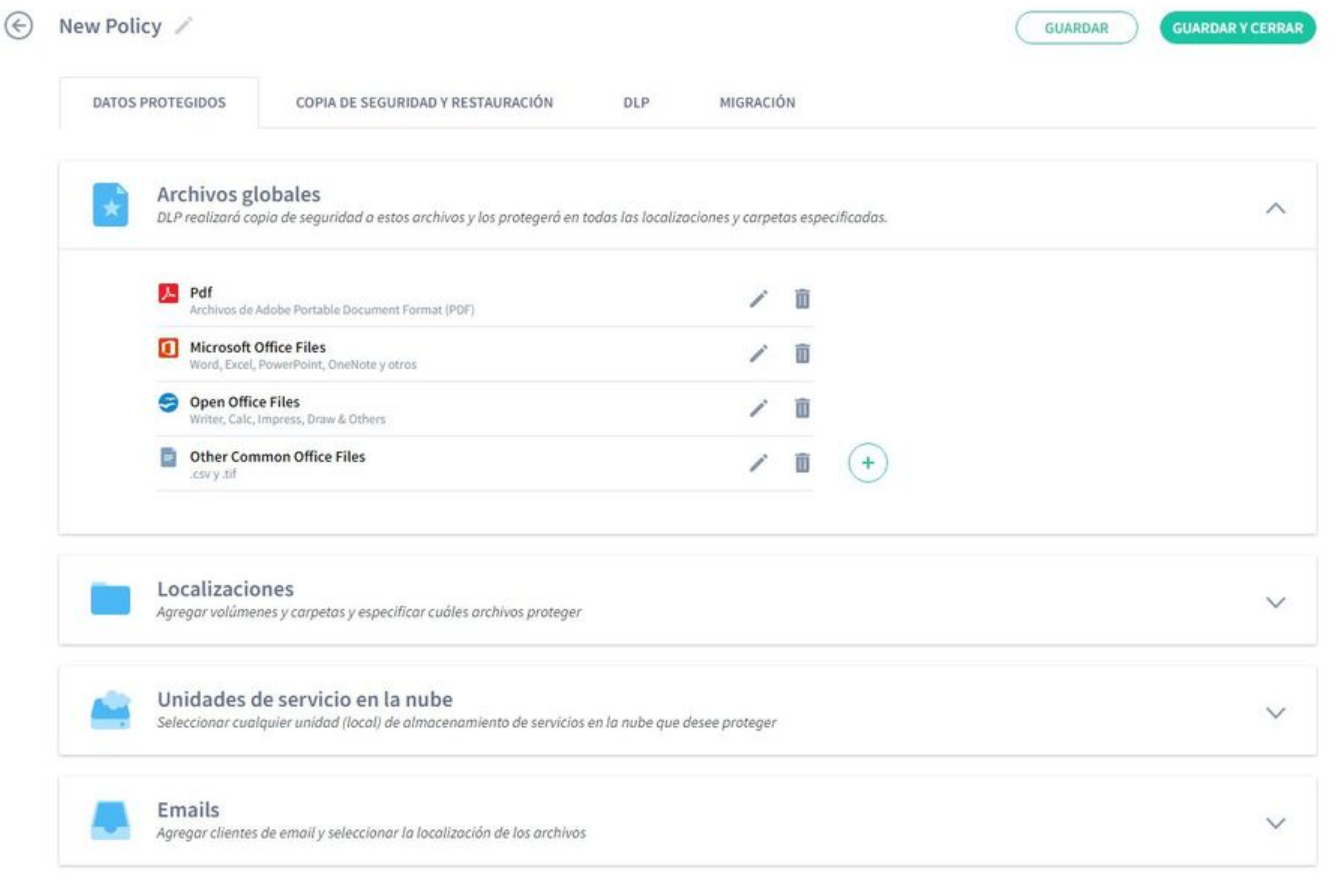
Você pode escolher:

1. Ative a criptografia de arquivo local na máquina. Isso funciona carregando um certificado de criptografia do usuário no dispositivo. Os arquivos só podem ser acessados se o certificado estiver disponível.
2. Impeça o acesso aos arquivos se o dispositivo não se conectar ao Aranda Datasafe dentro de um determinado período de tempo. O agente revoga automaticamente o certificado de criptografia do usuário, para que os arquivos não possam ser acessados.
3. Use a geolocalização para encontrar a última localização conhecida do dispositivo.

Migração

Use as configurações de migração para controlar se o Aranda Datasafe faz backup das configurações de perfil de usuário do Windows. Esse tipo de dados inclui configurações de acessibilidade, configurações de mouse e teclado, favoritos e muitas outras configurações específicas do usuário.

Você pode habilitar ou desabilitar a migração conforme necessário.



Atribuir políticas e repositórios às suas equipes

Você pode atribuir uma política e um repositório a cada uma de suas equipes. Eles informam ao Aranda Datasafe quais dispositivos devem ser copiados e protegidos, com que frequência os backups devem ser feitos e onde os dados devem ser armazenados.

Para atribuir uma política e um repositório, você deve editar a equipe.

1. Clique em **Inventário**.

2. Na barra **Equipes**, passe o mouse sobre a equipe à qual você atribuirá um repositório e/ou Política.

3. Clique no botão de opção Equipe (...).

4. Clique em **Editar**.

5. Escolha uma política na lista.

6. Escolha um repositório na lista.

7. Clique em Salvar computador.

A equipe agora está associada à política e ao repositório selecionados. Cada dispositivo atribuído a essa equipe será copiado e protegido de acordo com os detalhes da Política selecionada. Os dados dos dispositivos da equipe serão criptografados e armazenados no repositório selecionado.

Ativar dispositivos

Depois de configurar suas equipes, repositórios e políticas, você pode **ativar** seus dispositivos.

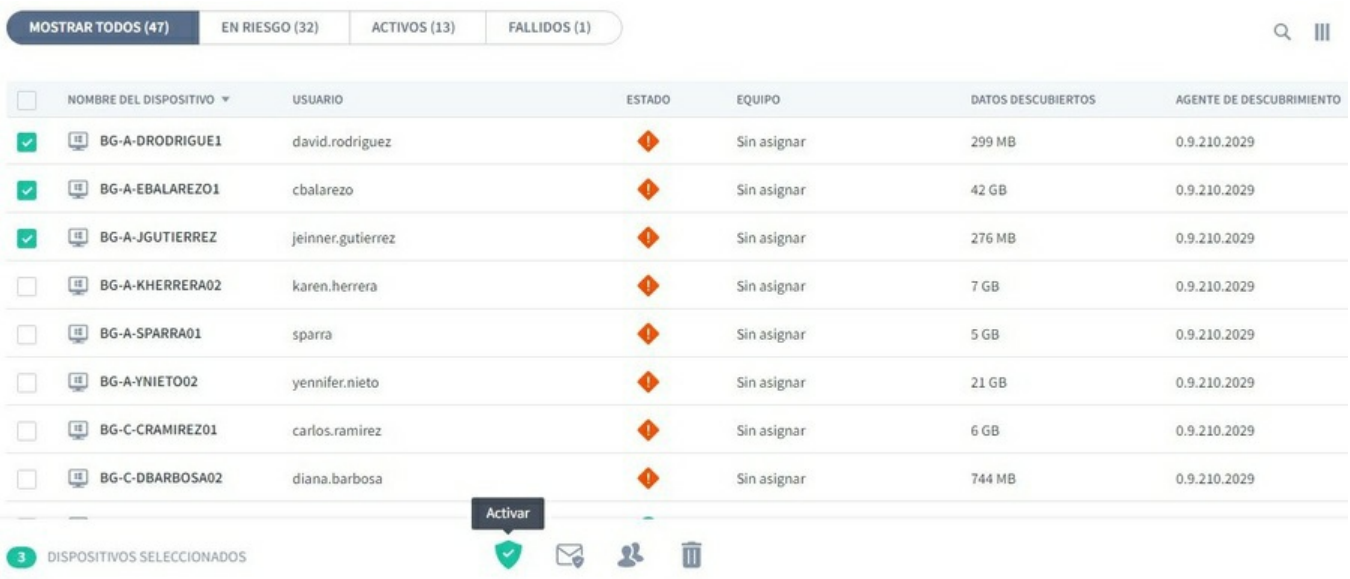
Ao ativar um dispositivo, você cria uma solicitação para que esse dispositivo seja protegido e copiado. Se a solicitação de ativação for bem-sucedida, o dispositivo será protegido **quando o próximo backup for agendado** (conforme definido nas configurações de política).

Para ativar um dispositivo:

Clique em **Inventário**. Encontre o dispositivo que deseja ativar na lista de dispositivos.

Para ativar um único dispositivo, você pode clicar no botão de opção (...) e, em seguida, clicar em **Ativar**.

Para ativar vários dispositivos, marque as caixas de seleção dos dispositivos que deseja ativar. Em seguida, clique no ícone **Ativar** na barra pop-up na parte inferior.



Quando você ativa um dispositivo, seu status muda de **Em risco** para **Pendente**. Após um pequeno atraso (cerca de 10 minutos se esta for a primeira vez que o dispositivo é ativado), o dispositivo realizará um backup; se for bem-sucedido, o status do dispositivo muda para **Protegido** e uma marca verde é exibida.

Se o dispositivo não puder ser protegido, um ícone de escudo vermelho será exibido. Você precisará investigar por que a ativação falhou. Pode ser porque o usuário

não está conectado ao dispositivo ou houve um problema relacionado à conexão.

Backup

Quando você ativa dispositivos no Aranda Datasafe, seus dados são copiados automaticamente:

- Aproximadamente 10 minutos após a ativação inicial ou após o agente ser iniciado
- Regularmente, de acordo com o agendamento de backup (definido na Política).

Após a conclusão do backup automático inicial, você também pode fazer backup de um dispositivo manualmente. O backup é iniciado a partir do Aranda Datasafe ou usando o Agente de Proteção localmente no dispositivo.

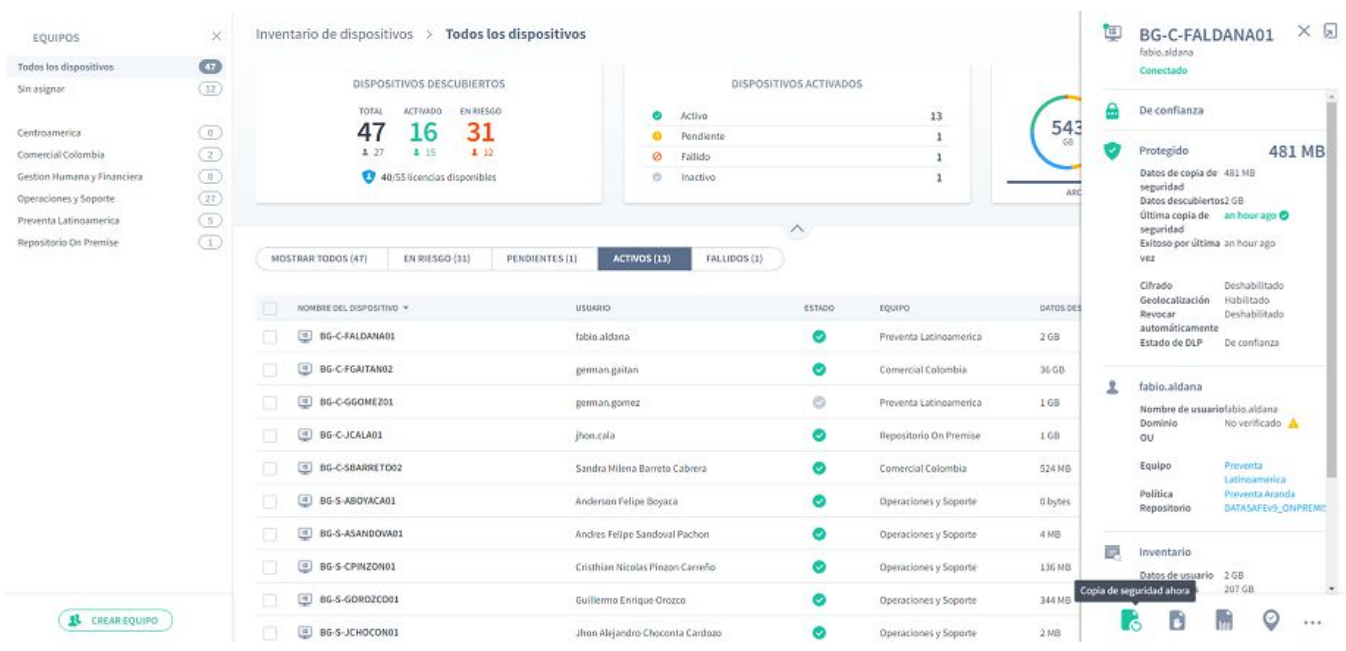
Nesta etapa, você aprenderá como iniciar um backup do Aranda Datasafe e, em seguida, verá informações detalhadas sobre o backup.

1. Clique em Inventário.

2. Na lista de dispositivos, clique no dispositivo que deseja fazer backup. Seus detalhes aparecem em um painel deslizante.

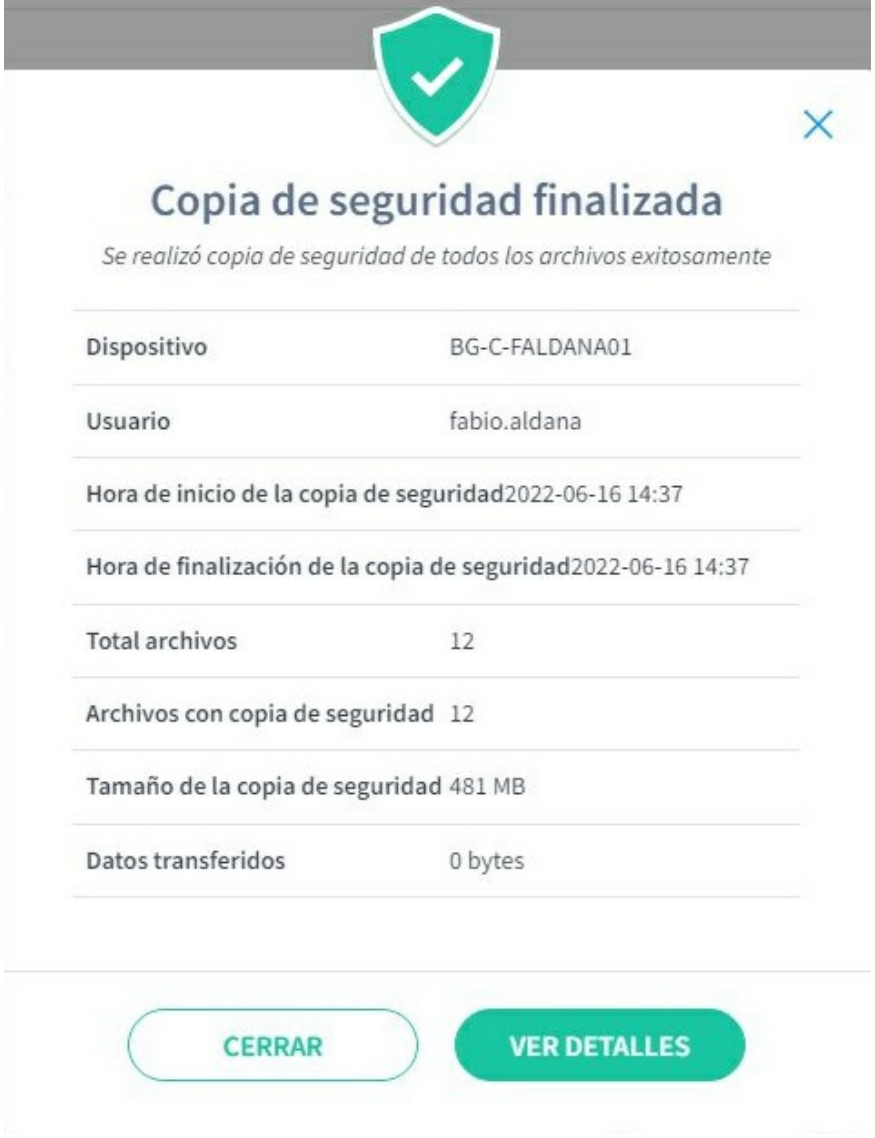
3. Clique no ícone Fazer backup agora na parte inferior do painel deslizante.

Uma mensagem de confirmação aparece na parte inferior da tela para informar que a solicitação de backup foi bem-sucedida.



O software do Agente de Proteção (no dispositivo do usuário) usa a eliminação de duplicação para garantir que apenas dados individuais sejam copiados para o repositório. A quantidade de tempo necessária para fazer backup de um dispositivo varia, dependendo da quantidade de dados que precisam ser indexados e copiados.

4. No painel deslizante, clique no link ao lado da entrada Último backup para exibir um resumo do backup.



5. Para obter informações mais detalhadas sobre o backup, clique em Exibir detalhes. Em seguida, você pode visualizar os detalhes do backup, o dispositivo, os arquivos que não puderam ser copiados e os logs de erros.

Restaurar no dispositivo

O Aranda Datasafe armazena backups de dados protegidos em seus dispositivos ativados. Se os dados forem excluídos acidentalmente do dispositivo, você poderá restaurá-los baixando-os do Aranda Datasafe. Você também pode restaurar backups de um dispositivo antigo para um novo dispositivo.

Para **restaurar** arquivos em um dispositivo:

1. Faça login no dispositivo que receberá o backup dos dados do Aranda Datasafe.

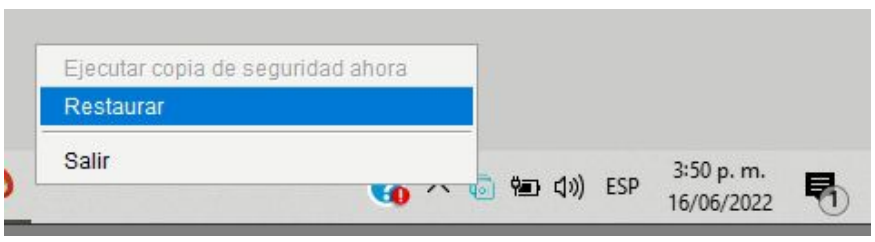
2. Se o seu dispositivo já tiver o Discovery Agent instalado, ignore as etapas 2 e 3 e continue a partir da etapa 4.

3. Se você precisar restaurar dados para um novo dispositivo ou um dispositivo que não tenha sido protegido pelo Aranda Datasafe antes, será necessário instalar o Discovery Agent. Continue a partir da etapa 2.

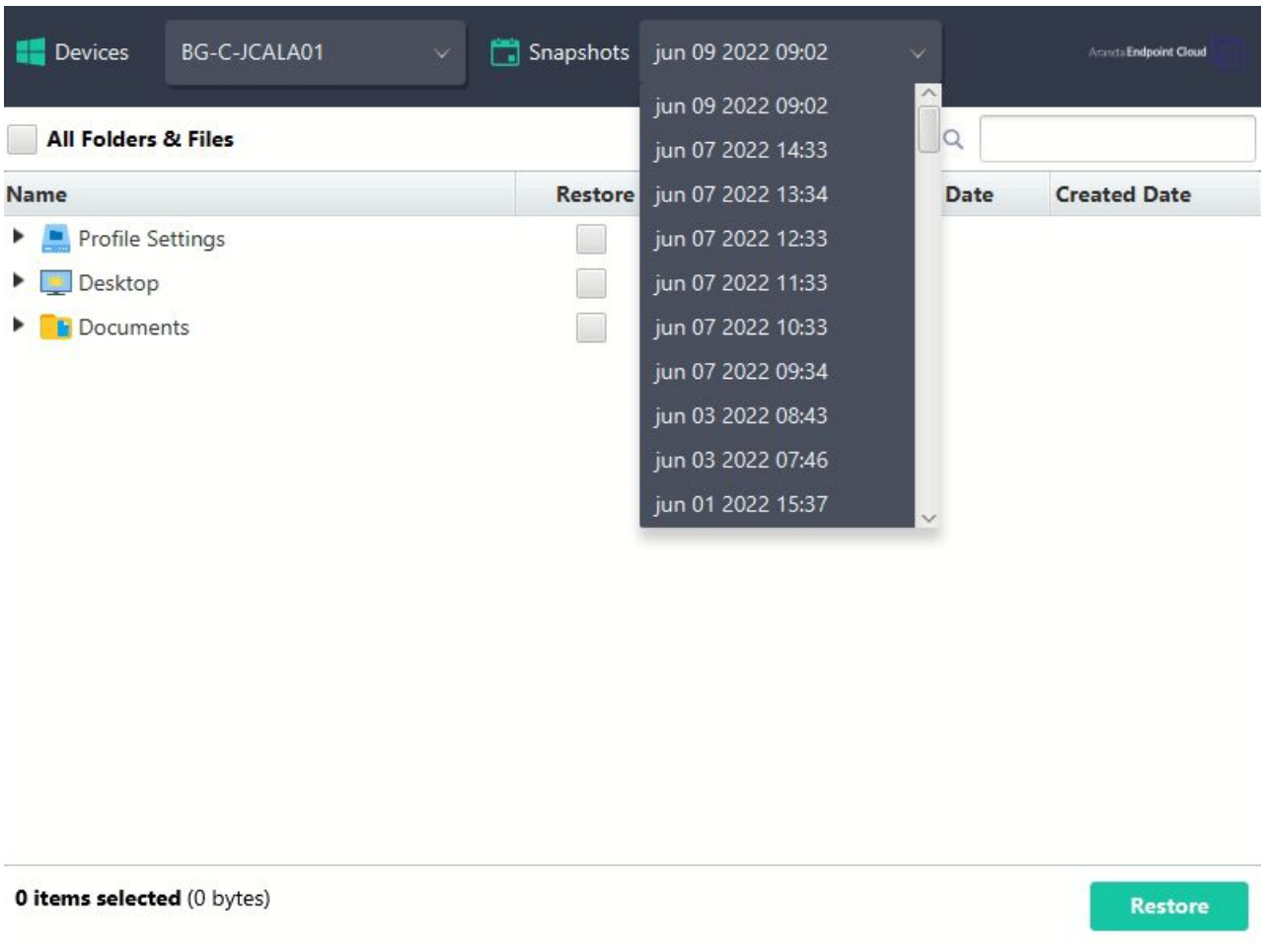
4. Instale o Discovery Agent no dispositivo, para que o Aranda Datasafe possa detectá-lo.

5. No Aranda Datasafe, ative o novo dispositivo.

6. Na barra de tarefas do Windows, clique com o botão direito do mouse no ícone do Agente de Proteção e selecione Restaurar.



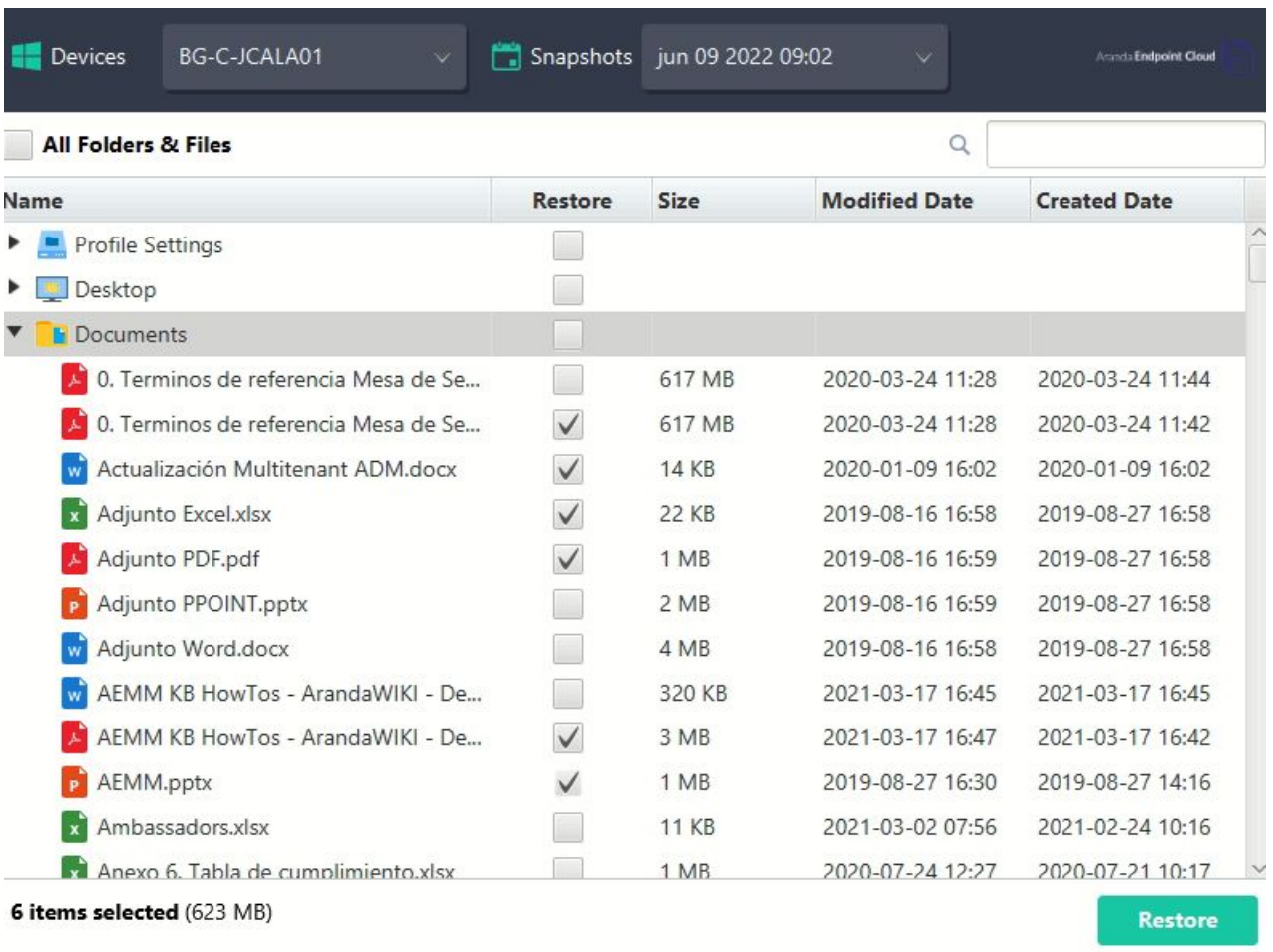
7. Na parte superior do Datasafe Aranda Agent, escolha o dispositivo que continha os dados que deseja restaurar. Em seguida, escolha o instantâneo apropriado. Um instantâneo é um registro dos dados de um dispositivo em um ponto específico no tempo, e você pode escolher qualquer um dos horários mostrados na lista.



8. Escolha quais arquivos deseja restaurar. Selecione os arquivos nos locais disponíveis (Área de trabalho, C:\, etc.).

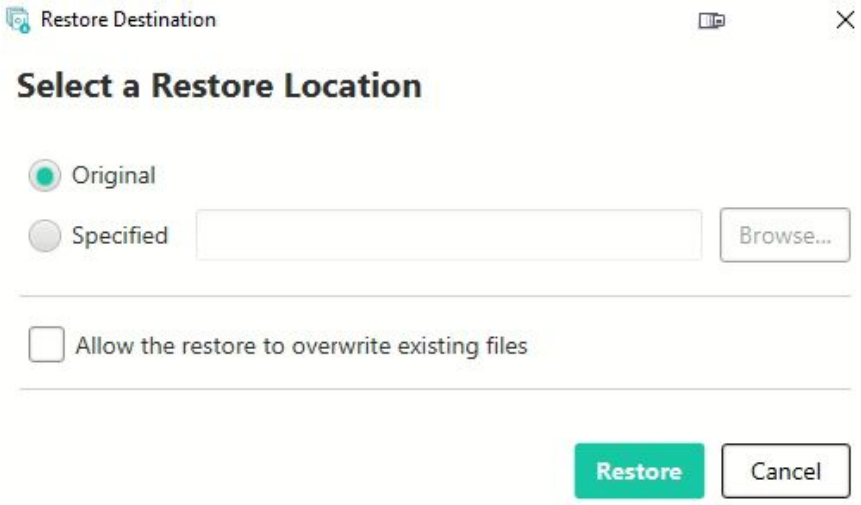
Se a política tiver a migração habilitada e a opção Perfis de usuário do Microsoft Windows estiver selecionada, você também poderá restaurar os dados do perfil do usuário. Selecione a opção **Configurações de perfil** para restaurar essas configurações.

Se o recurso de migração estiver desativado ou os perfis de usuário do Microsoft Windows não estiverem selecionados, você só poderá optar por restaurar os dados de backup.



9. Selecione **Restaurar**.

10. . Escolha o local para os arquivos de restauração. É aqui que eles serão restaurados para o seu novo dispositivo. Se você escolher **Original**, os arquivos serão recuperados para o mesmo local que tinham no dispositivo anterior. Ou você pode escolher um local **especificado** diferente, se preferir.



Selecione **Restaurar**.

Os dados selecionados são restaurados do repositório para o seu dispositivo. Se você escolheu arquivos da área de trabalho, eles aparecerão na área de trabalho.

Se você estiver restaurando dados de backup e configurações de perfil de usuário, a restauração será concluída em duas fases separadas.

Prevenção contra perda de dados

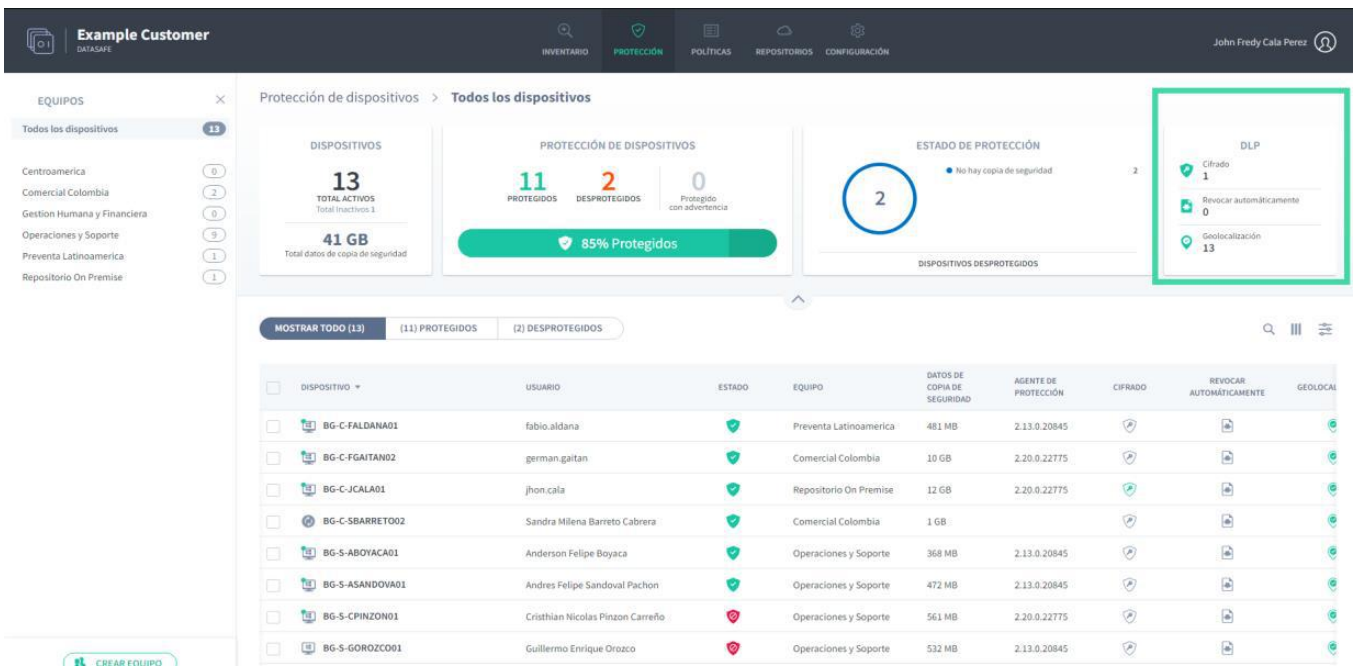
O Aranda Datasafe possui recursos de prevenção contra perda de dados (DLP) que reduzem o risco em caso de perda ou roubo de um dispositivo protegido. Os recursos estão habilitados na Política consulte Criar uma política e eles podem proteger seus dados com:

- Criptografia de dados locais em seus dispositivos
- Prevenção automática de acesso a dados protegidos se um dispositivo não se conectar dentro de um número específico de dias (revogação automática)
- Fornecer a última localização conhecida do dispositivo (geolocalização)
- Permitir que você limpe remotamente os dados de backup em um dispositivo

Vejamos como você pode exibir e usar os recursos DLP.

Exibir status do DLP

Você pode exibir o status do DLP na página Proteção. Mostra o número de dispositivos que têm recursos de criptografia local, revogação automática e geolocalização habilitados (na política).



O status da DLP também é exibido na lista de dispositivos na parte inferior da seção Proteção.

Revogar um dispositivo

Se uma política tiver a criptografia local habilitada, cada dispositivo receberá um certificado de criptografia armazenado localmente em cada máquina. Os dados criptografados só podem ser acessados pelo usuário registrado se o certificado estiver em vigor.

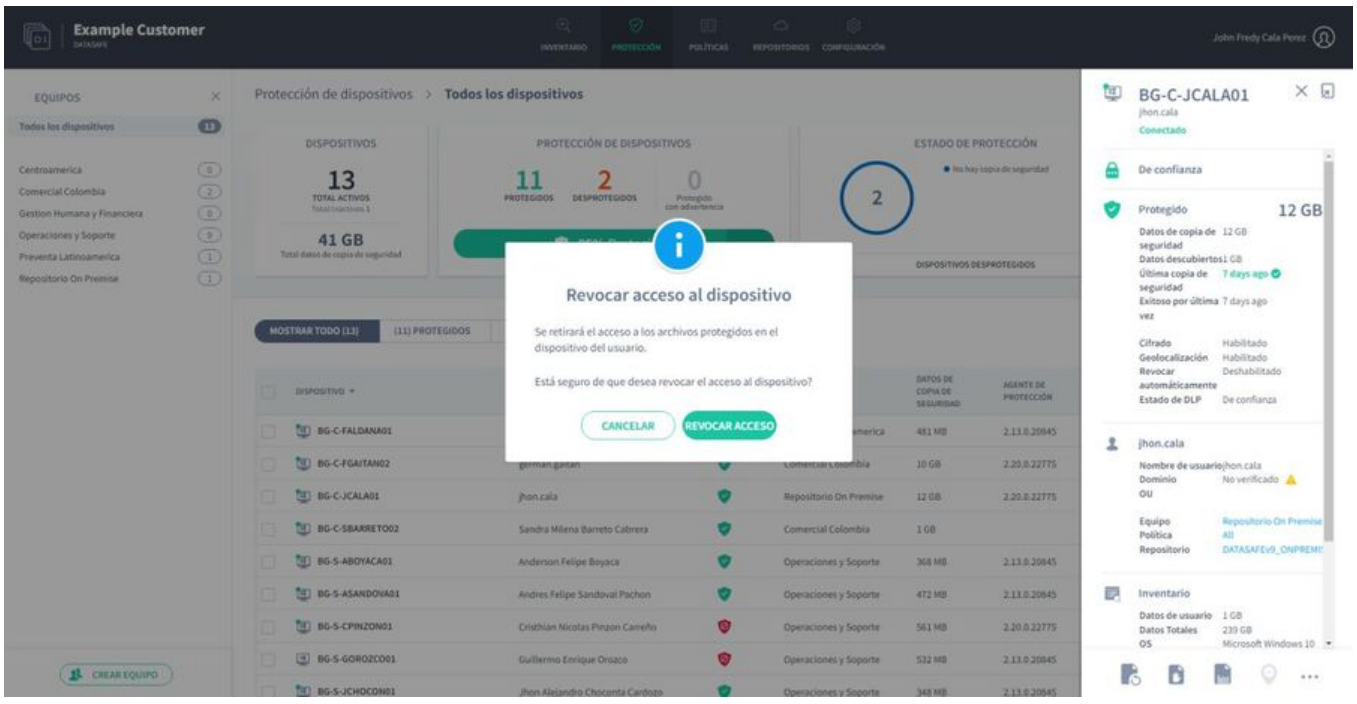
Ao revogar um dispositivo, você remove o certificado para que os dados criptografados não possam ser acessados.

1. Clique em **Proteção**.

2. Clique no dispositivo que deseja revogar.

3. Clique no ícone **Revogar dispositivo**.

4. Clique em **Revogar** para confirmar.



⚐ > Observação: Se a revogação automática estiver habilitada em uma política, o Aranda Datasafe revogará automaticamente o certificado de qualquer dispositivo protegido que não se conecte ao Aranda Datasafe dentro de um número especificado de dias. (Você pode alterar o período de revogação automática nas configurações de política.)

Apagar um dispositivo

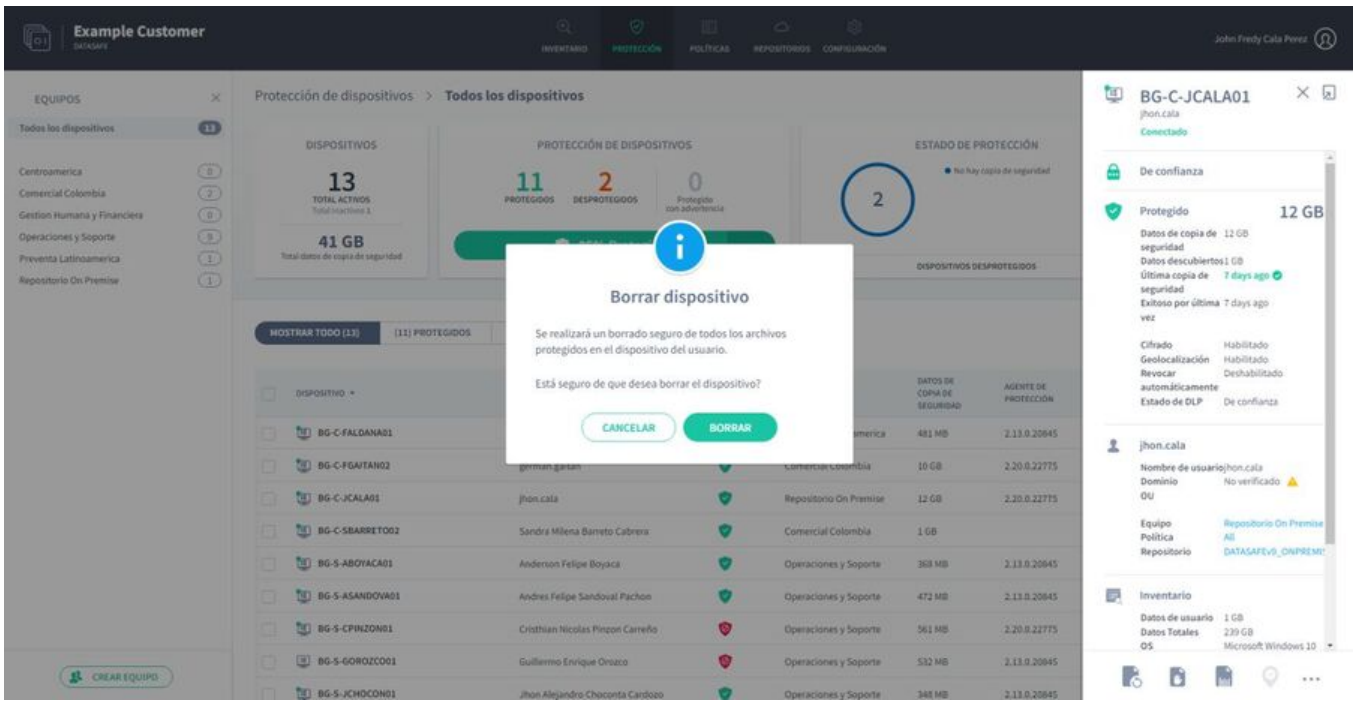
Você pode limpar remotamente os arquivos protegidos em seus dispositivos. Com uma limpeza, os arquivos protegidos são excluídos e o Aranda Datasafe também executa um "apagamento forense" para remover quaisquer vestígios dos arquivos no dispositivo.

1. Clique em **Proteção**.

2. Clique no dispositivo que deseja apagar.

3. Clique no ícone **excluir**.

4. . Clique em Limpar para confirmar.



Localize um dispositivo

Se uma política tiver a geolocalização habilitada, ela poderá ver a última localização conhecida de um dispositivo protegido (o dispositivo deve ter o Wi-Fi habilitado).

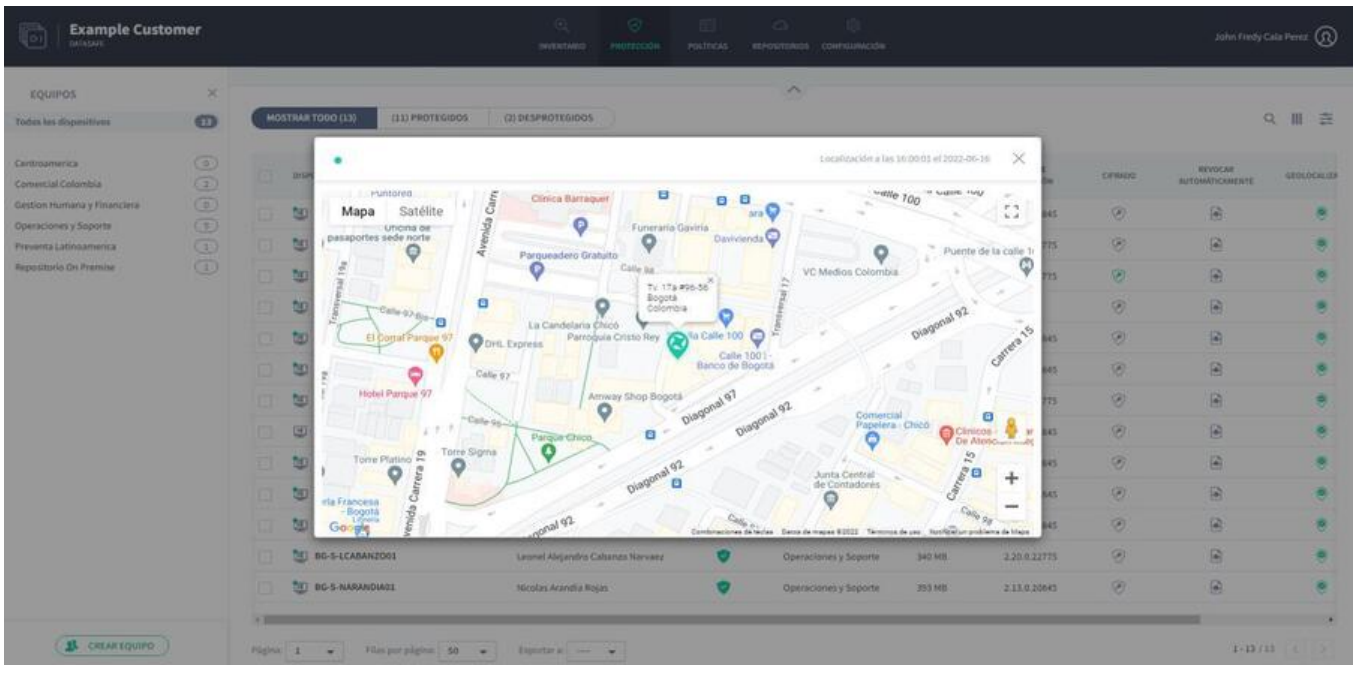
Para usar a geolocalização para encontrar um dispositivo:

1. Clique em **Proteção**.

2. Clique no dispositivo que deseja localizar.

3. Clique no ícone Geolocalizar.

O último local conhecido é mostrado em um mapa do Google. Você pode ampliar, diminuir o zoom e mostrar a visualização de satélite.



Migração de configuração

Em algum momento, você provavelmente precisará substituir um de seus dispositivos protegidos. Por exemplo, um dispositivo mais antigo pode precisar ser atualizado para um modelo mais novo ou um dispositivo protegido pode ser perdido ou roubado. Para facilitar e agilizar a configuração de um novo dispositivo, o Aranda Datasafe possui um recurso de migração.

Com o recurso de migração, você pode configurar o Aranda Datasafe para realizar backups mensais das configurações de perfil de usuário do Windows em dispositivos protegidos. Em seguida, quando precisar substituir um dispositivo protegido, você poderá migrar a configuração do Aranda Datasafe para o novo dispositivo de substituição.

Para usar o recurso de migração, você deve habilitá-lo nas políticas relevantes.

Habilitar migração de perfil de usuário

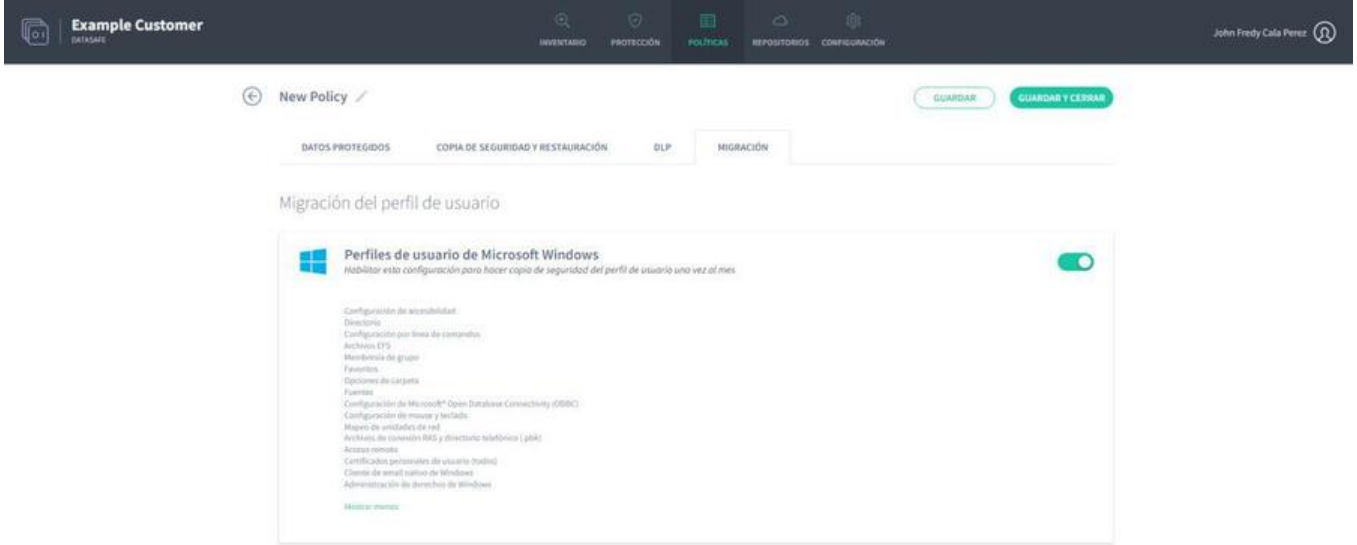
Para ativar o recurso de migração das configurações de perfil do usuário:

1. No Aranda Datasafe, clique em **Políticas**.

2. Edite a Política associada ao equipamento do dispositivo.

3. Clique em **Migração**.

4. Ative a migração de perfil para perfis de usuário do Microsoft Windows.



5. Clique no link **Mostrar mais** para ver uma lista completa das informações do perfil de usuário do Windows que serão copiadas. Inclui layout da barra de tarefas, unidades de rede mapeadas, opções de pasta, contas de e-mail, arquivos pst anexados anteriormente e assinaturas de e-mail.

6. Clique em Salvar e Fechar.

Os dados e perfis do usuário serão copiados para os dispositivos protegidos quando o próximo backup de dados for feito (conforme agendado na política).

Quando um backup for feito, você poderá migrar as configurações para um novo dispositivo.

Migrar configurações para um novo dispositivo

Se você tiver habilitado a migração em uma política, poderá usar a Restauração para transferir dados de perfil de usuário do Windows (e dados de backup) de um dispositivo antigo para um novo dispositivo (via Aranda Datasafe).

Para restaurar arquivos em um dispositivo:

1. Faça login no novo dispositivo.

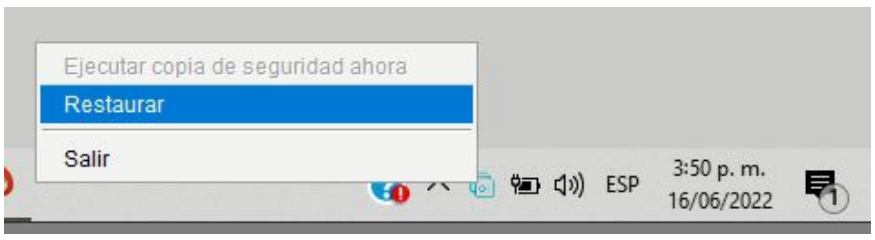
Se o seu dispositivo já tiver o Discovery Agent instalado, ignore as etapas 2 e 3 e continue a partir da etapa 4.

Se você precisar restaurar dados para um novo dispositivo ou um dispositivo que não tenha sido protegido pelo Aranda Datasafe antes, será necessário instalar o Discovery Agent. Continue a partir da etapa 2.

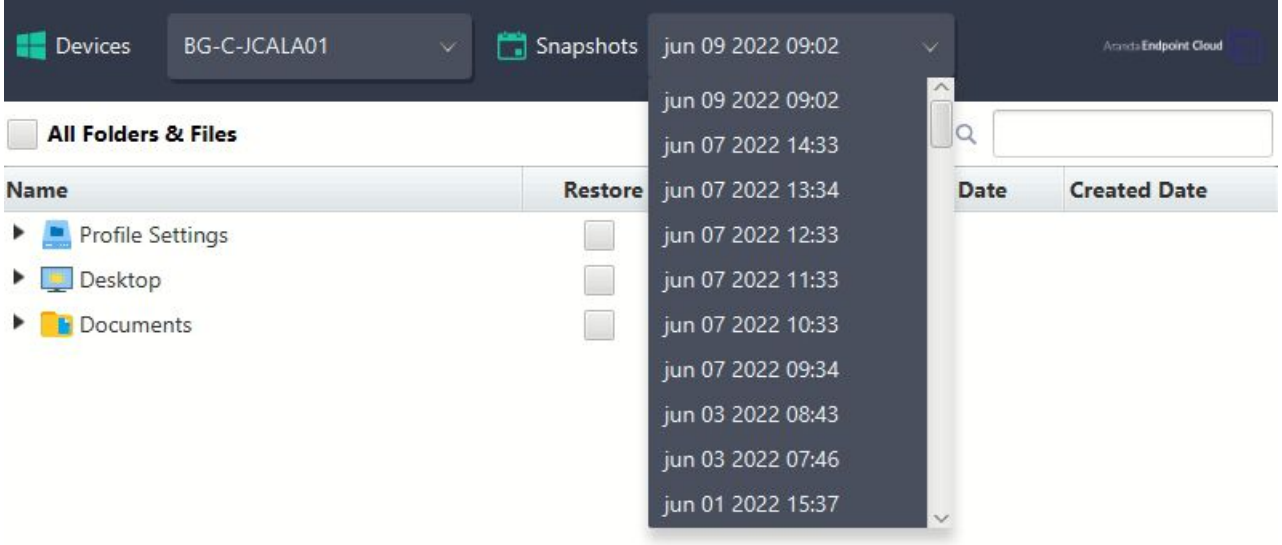
2. Instale o Discovery Agent no dispositivo, para que o Aranda Datasafe possa detectá-lo.

3. No Aranda Datasafe, ative o novo dispositivo.

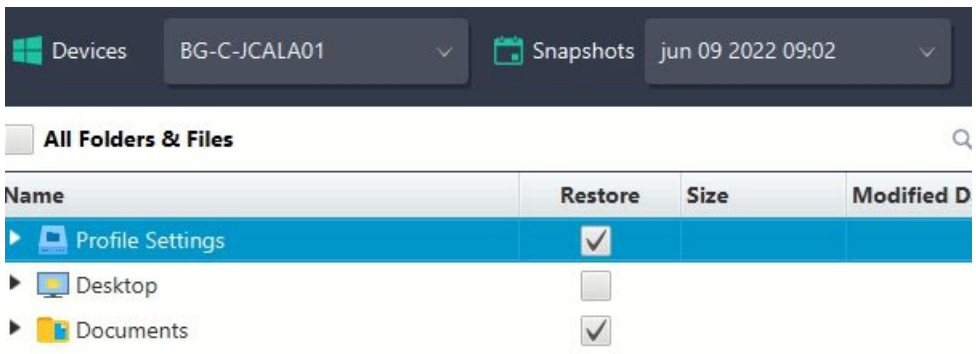
4. Na bandeja do sistema do Windows, clique com o botão direito do mouse no ícone do Agente de Proteção e selecione **Restaurar**.



5. Na parte superior do Aranda Datasafe Agent, escolha o dispositivo e, em seguida, o instantâneo que deseja migrar para o novo dispositivo. O instantâneo é um registro dos dados de um dispositivo em um ponto específico no tempo, e você pode escolher qualquer um dos horários mostrados na lista.

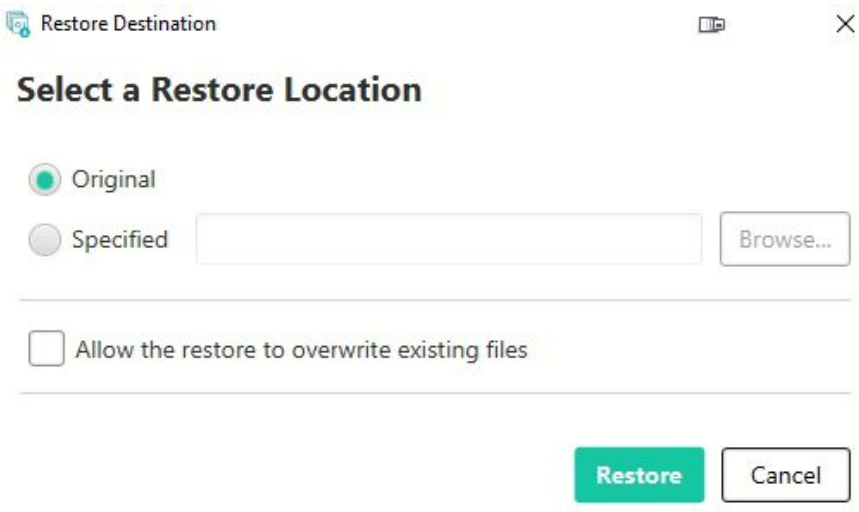


6. Escolha quais arquivos deseja restaurar. Você pode escolher **Todas as pastas e arquivos**, todos os arquivos da área de trabalho, todos os documentos ou todos os arquivos em volumes (unidades). Como alternativa, você pode selecionar arquivos individuais.



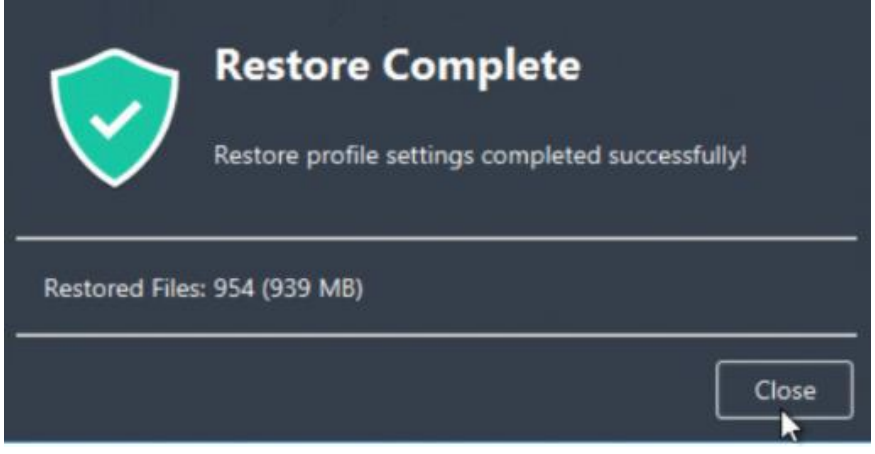
7. Selecione **Restaurar**.

8. Escolha o local dos arquivos migrados. Se você escolher **Original**, os arquivos serão enviados para o mesmo local que tinham no dispositivo anterior. Ou você pode escolher um local **específico** diferente, se preferir.



9. Selecione **Restaurar**.

Os dados do usuário selecionados e as informações do perfil são baixados do Aranda Datasafe para o seu novo dispositivo. Se você escolheu arquivos da área de trabalho, eles aparecerão na área de trabalho.



Descoberta e inventário

Descoberta e inventário

O Aranda Datasafe pode fornecer uma visão geral de seus dispositivos e dados em escala global. Você pode usar essas informações para determinar quais tipos de dados sua organização possui, quais dados estão em risco e quanto espaço de armazenamento é necessário para fazer backup no Aranda Datasafe.

Para obter uma visão geral, instale o aplicativo Discovery Agent em cada um dos seus dispositivos empresariais (mas não o instale no servidor).

O Discovery Agent permite que o Aranda Datasafe detecte os dispositivos de seus usuários automaticamente.

O que é o Discovery Agent?

O Discovery Agent é um aplicativo leve e gratuito que você pode implantar em um número ilimitado de dispositivos em sua organização. Ele oferece uma visão instantânea de seus dispositivos e dados de endpoint, para que você possa planejar seu armazenamento e começar a proteger seus dispositivos, tudo de dentro do Aranda Datasafe.

Quando você executa o Discovery Agent, ele analisa seus dispositivos e dados e cria um inventário. O Aranda Datasafe usa o inventário para fornecer uma grande quantidade de informações sobre seus dispositivos e dados, incluindo detalhes de:

- Os componentes de hardware que compõem o dispositivo
- Aplicativos, drivers, serviços e atualizações instalados
- Dados do dispositivo, categorizados automaticamente em dados comerciais e não comerciais
- Status de ativação. Você pode ver quais dispositivos estão em risco e quais estão ativados para proteção.

Você pode acessar todas essas informações na página Aranda Datasafe Inventory.

Instalação e implantação do Discovery Agent

Você pode usar o Discovery Agent do Aranda Datasafe para identificar:

- A quantidade de dados da sua empresa que está em risco.
- Quanto espaço de armazenamento você precisará para fazer backup e proteger seus dispositivos.

O Discovery Agent é gratuito e oferece uma visão geral de seus dispositivos e dados. Você precisa instalá-lo em todos os dispositivos que deseja fazer backup e proteger com o Aranda Datasafe.

Baixe o Discovery Agent

Você pode baixar e instalar o Discovery Agent em todos os dispositivos que deseja incluir no inventário do Aranda Datasafe**Não instale o Discovery Agent em seus servidores locais ou servidores em nuvem**.

Em um dispositivo que você deseja ser descoberto:

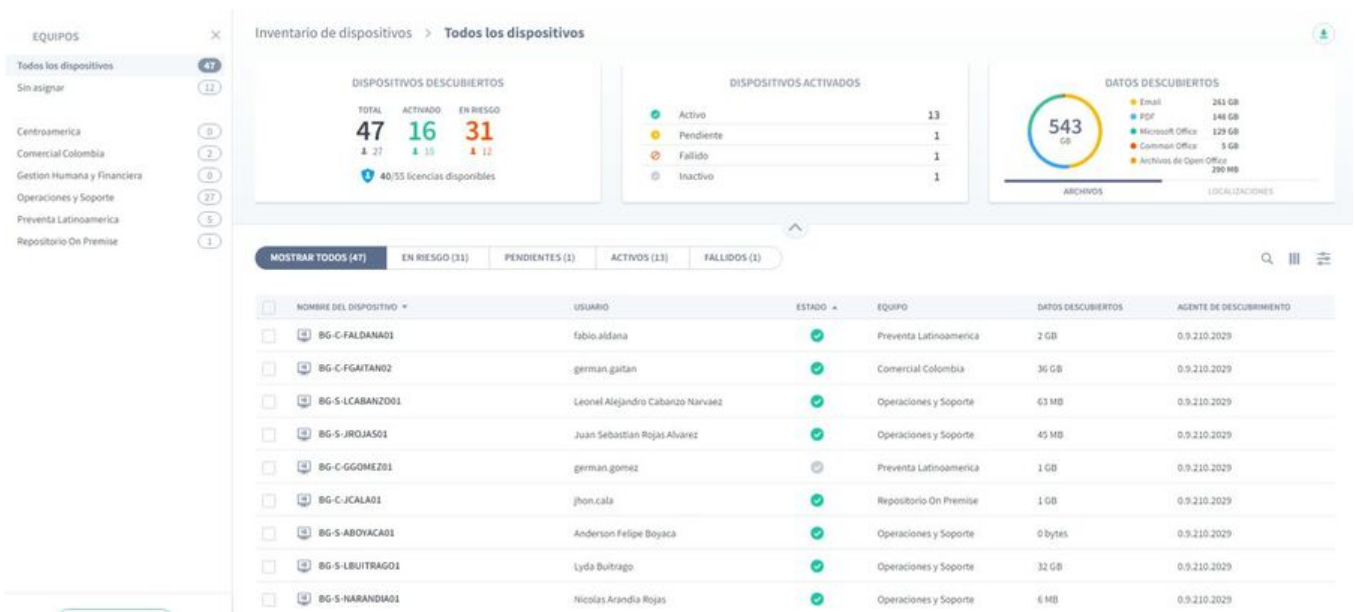
1. Faça login no Aranda Datasafe como administrador.

Se o Aranda Datasafe ainda não tiver descoberto nenhum dispositivo, a página Inventário não contém informações sobre o dispositivo e aconselha você a baixar o agente de descoberta.

Se o Aranda Datasafe tiver descoberto dispositivos, a página Inventário exibirá informações sobre esses dispositivos.

2. Se o Aranda Datasafe não tiver descoberto nenhum dispositivo, clique em Baixar Discovery Agent para começar a baixar um Discovery Agent específico para seu Aranda Datasafe Tenant. (O pacote do MSI Discovery Agent é baixado para o navegador.)

Se o Aranda Datasafe já descobriu dispositivos, clique no ícone de download no canto superior direito, acima do paine**Dados descobertos**##. O Discovery Agent começará a ser baixado para o seu navegador.



Instale o Discovery Agent em seus dispositivos de usuário final

Instale o pacote do MSI Discovery Agent em cada dispositivo de usuário (desktop, laptop etc.). O agente de descoberta executará um inventário de dispositivos e dados e, em seguida, carregará com segurança as informações no Aranda Datasafe.

Pré-requisitos

- Os dispositivos do usuário devem ter**acesso à Internet**, pois o Discovery Agent precisa se conectar ao Aranda Datasafe.
- Os dispositivos do usuário devem usar um**sistema operacional Windows**, Windows 7 ou posterior. Uma versão para Mac estará disponível em breve.
- **Firewalls e servidores proxy devem permitir conexões**. Talvez seja necessário colocar endpointcloud.com na lista de permissões e o caminho completo para a URL do locatário do Aranda Datasafe. Exemplo: https://arandasoftware.endpointcloud.com em que **"arandasoftware"** é substituído pelo nome da sua organização.

Você pode instalar o Discovery Agent manual ou remotamente em cada dispositivo.

Instalação manual do agente

O Discovery Agent pode ser instalado executando o pacote MSI em cada dispositivo de usuário.

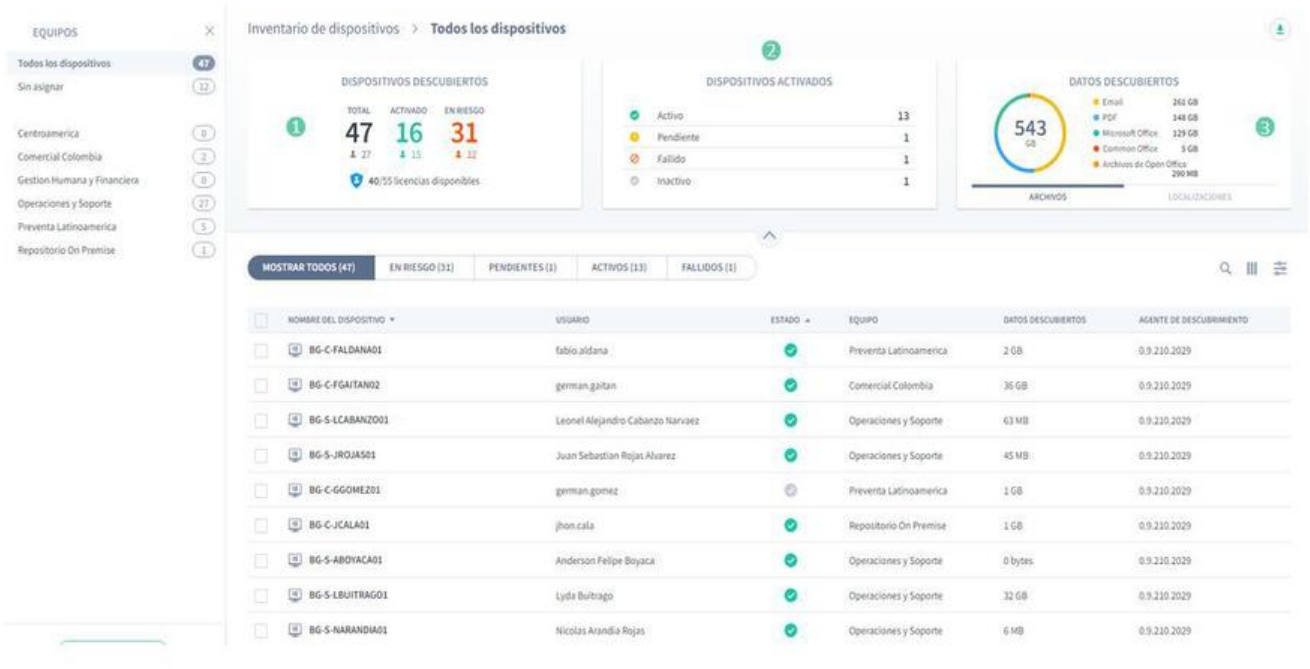
Talvez você queira mover o pacote MSI para uma pasta compartilhada que possa ser acessada por todos os dispositivos. Como alternativa, você pode colocar o pacote MSI em um cartão de memória e transferi-lo entre dispositivos dessa maneira.

Instalação do Agente Remoto

Você pode instalar o pacote MSI em dispositivos remotamente, usando o recurso Política de Grupo do Active Directory ou um aplicativo de terceiros. Para obter mais detalhes, entre em contato com o Suporte da Aranda (reportedecasos@arandasoft.com).

Inventário de dispositivos

A página Inventário exibe informações sobre os dispositivos que o Aranda Datasafe descobriu. Essas informações incluem detalhes sobre cada dispositivo, a quantidade de dados descobertos e o status de proteção de cada dispositivo.



Dispositivos descobertos

O painel Dispositivos Descobertos fornece um resumo dos dispositivos que foram descobertos.

Campo	Descrição
Total	O número total de dispositivos que foram descobertos (dispositivos ativados + dispositivos comprometidos). Abaixo do número total está o número de usuários. Na imagem acima, o Aranda Datasafe descobriu 47 dispositivos e 27 usuários.
Ativos	O número de dispositivos descobertos que foram ativados. Os dispositivos ativados estão sendo copiados e protegidos ou aguardando backup e proteção. Quando você ativa um dispositivo pela primeira vez, seu status é definido como Ativado, mas a ativação não é iniciada até que o próximo backup seja feito. Abaixo do número ativado está o número de usuários que ativaram seus dispositivos.
Em risco	O número de dispositivos descobertos que não foram ativados e, portanto, não são protegidos ou suportados pelo Aranda Datasafe.
Licenças disponíveis	O número de licenças que estão atualmente em uso e o número total de licenças que estão disponíveis para você.

Dispositivos ativados

O painel Dispositivos Ativados fornece informações sobre os dispositivos que foram ativados (configurados para serem copiados e protegidos).

Campo	Descrição
Ativos	O número total de dispositivos que foram ativados e estão atualmente com backup e protegidos pelo Aranda Datasafe.
Pendente	O número de dispositivos descobertos que foram ativados, mas ainda não foram copiados e protegidos pelo Aranda Datasafe. Eles serão ativados quando o agente de proteção for autenticado com sucesso.
Reprovado	O número de dispositivos descobertos que não puderam ser ativados. Uma ativação pode falhar se o Agente de Proteção não tiver sido baixado e instalado ou se o usuário não estiver autenticado no Active Directory.
Inativo	O número de dispositivos descobertos que não se conectaram ao Aranda Datasafe nos últimos 30 dias.

Dados descobertos

O painel Dados descobertos fornece um resumo dos tipos de dados corporativos que o Aranda Datasafe encontrou em seus dispositivos. Por padrão, ele exibe arquivos com um resumo dos tipos de arquivo e a quantidade de espaço de armazenamento necessária para fazer backup.

Se você clicar em Locais, o painel fornecerá um resumo dos vários locais onde os dados estão localizados em seus dispositivos. Ele também fornece detalhes do espaço de armazenamento necessário para fazer backup de cada local.

Barra lateral do Teams

No lado esquerdo da página Inventário está a barra lateral do Equipamento. Isso exibe uma lista dos dispositivos configurados no Aranda Datasafe (mais Todos os dispositivos e Não atribuídos, que estão integrados).

Se você clicar em um computador, os painéis e a lista de inventário serão atualizados para que ele mostre apenas as informações dos dispositivos no computador selecionado. Você pode clicar em Todos os dispositivos para configurar o inventário para exibir dados de cada dispositivo.

Lista de dispositivos

A seção inferior do Inventário exibe a lista de dispositivos, que contém um resumo dos dispositivos que o Aranda Datasafe descobriu.

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

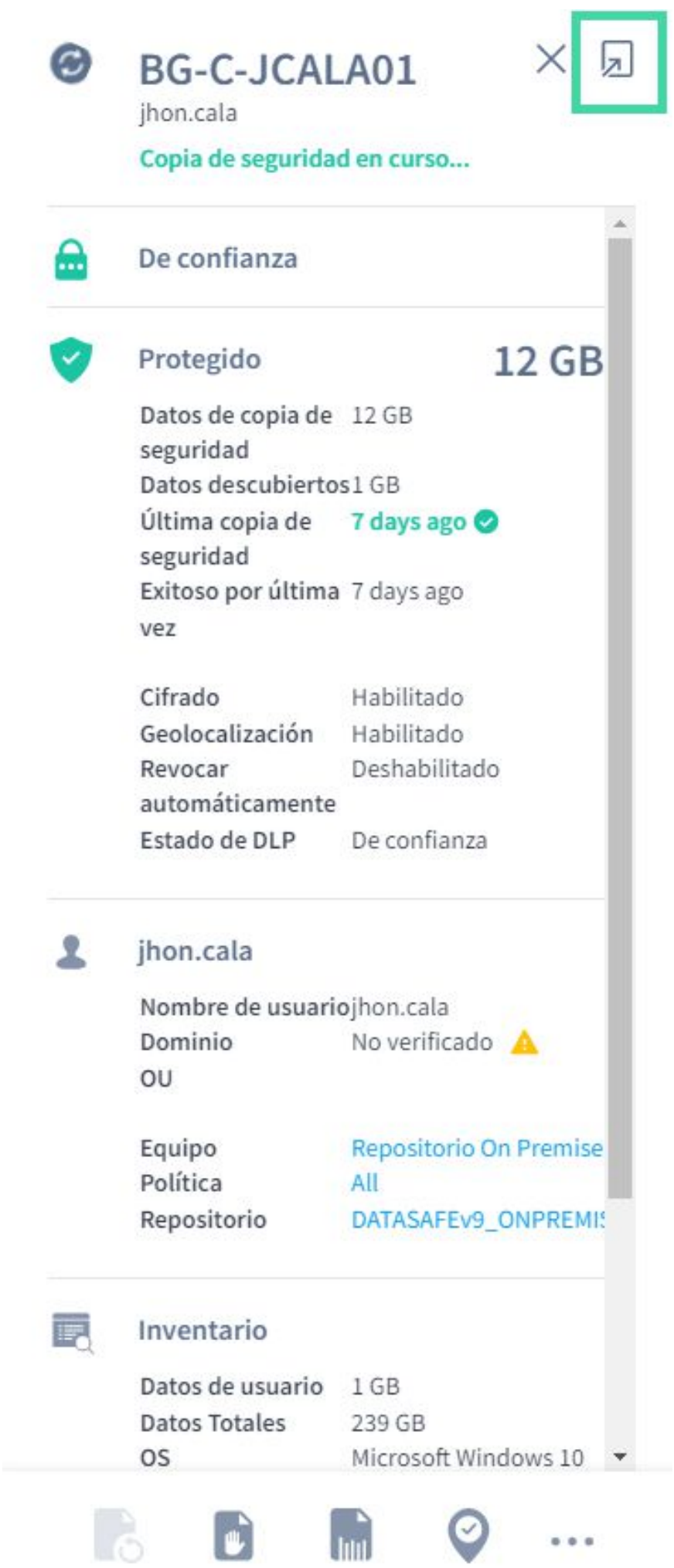
Campo	Descrição
Nome	O nome do dispositivo Device
Usuário	O nome de usuário associado ao dispositivo
Status	Exibe o status do dispositivo: - Ativo (ícone de verificação verde) - Ativação pendente (ícone de relógio amarelo) - Em risco (ícone de aviso vermelho) - Falha (ícone vermelho de falha)
Equipe	O computador ao qual o dispositivo está atribuído
Dados descobertos	A quantidade de dados de negócios descobertos
Agente de descoberta	O número da versão do software Discovery Agent que foi usado para descobrir o dispositivo.

Se você realçar um dispositivo na lista, um botão de opção (...) aparecerá à direita do nome do dispositivo. Clique no botão de opção para exibir um menu de contexto com estas opções:

Campo	Descrição
Visualizar	Exibe a página Dispositivo, que contém detalhes sobre o dispositivo, incluindo seu hardware e software.
Ativar	Use-o para ativar o dispositivo para que o Aranda Datasafe comece a fazer backup e protegê-lo. Você só poderá ativar um dispositivo se ele estiver atribuído a uma equipe e a equipe estiver atribuída a um repositório e a uma política.
Atribuir equipe	Use-o para atribuir o dispositivo a uma equipe. O Aranda Datasafe só pode fazer backup e proteger dispositivos atribuídos a computadores, pois os computadores devem estar associados a um repositório e a uma política.
Excluir	Use-o para remover um dispositivo.

Barra lateral do dispositivo

Se você clicar em um dispositivo na lista de dispositivos, a barra lateral do dispositivo será exibida. Exibe informações adicionais sobre o dispositivo selecionado. Se você clicar no ícone Exibir no canto superior, o Aranda Datasafe exibirá a página Dispositivo, que contém uma visão mais detalhada do dispositivo, incluindo seu hardware e software.



Na parte inferior da barra lateral do dispositivo, há ícones para fazer backup manual do dispositivo, revogá-lo, apagá-lo e usar a geolocalização para descobri-lo.

Ações de vários dispositivos

Você pode usar a lista de dispositivos para aplicar uma única ação a vários dispositivos. Por exemplo, você pode atribuir vários dispositivos ao mesmo computador.

Use a caixa de seleção à esquerda de cada linha de dispositivos para selecionar um dispositivo. Quando você marca as caixas de seleção, as opções de ação aparecem na parte inferior da lista. Eles funcionam da mesma maneira que para dispositivos individuais, exceto que a ação será aplicada a todos os dispositivos selecionados.

Dispositivos

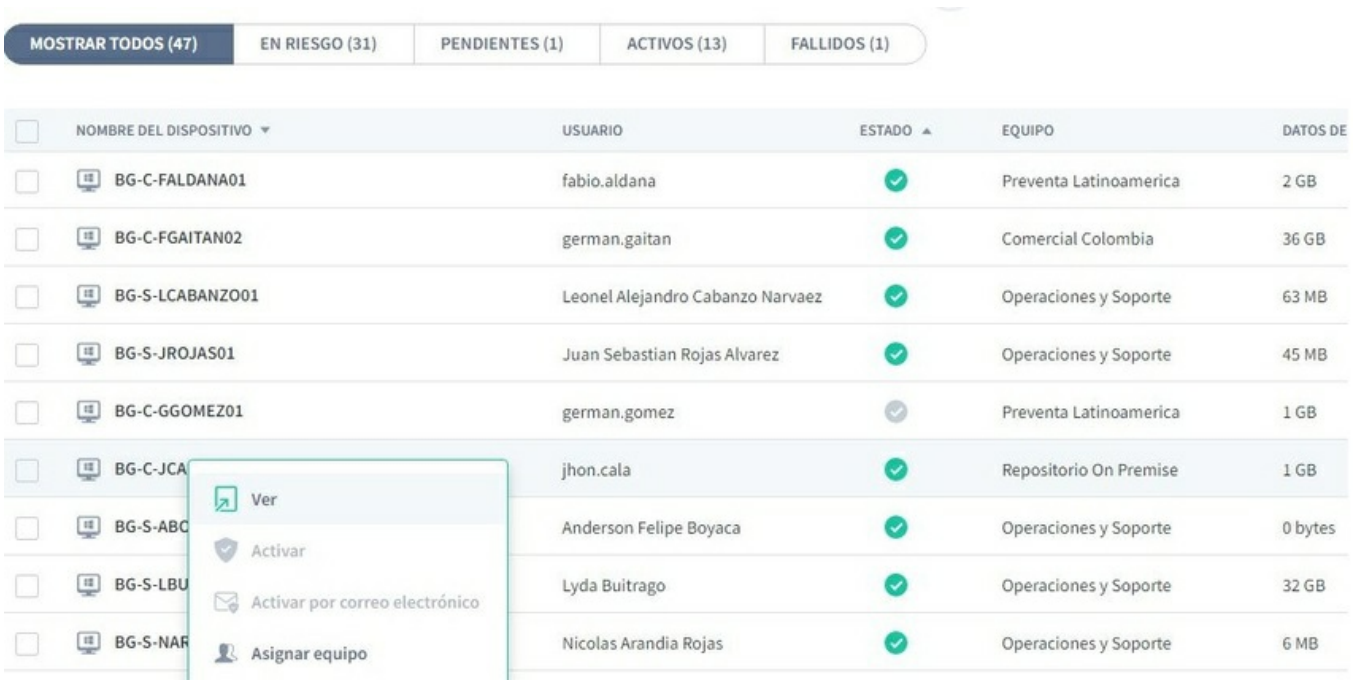
O Aranda Datasafe fornece uma página de dispositivo para cada dispositivo descoberto. A página Dispositivo fornece informações detalhadas sobre a integridade, os dados, o hardware e o software do dispositivo.

Para acessar a página **Dispositivo** de um dispositivo:

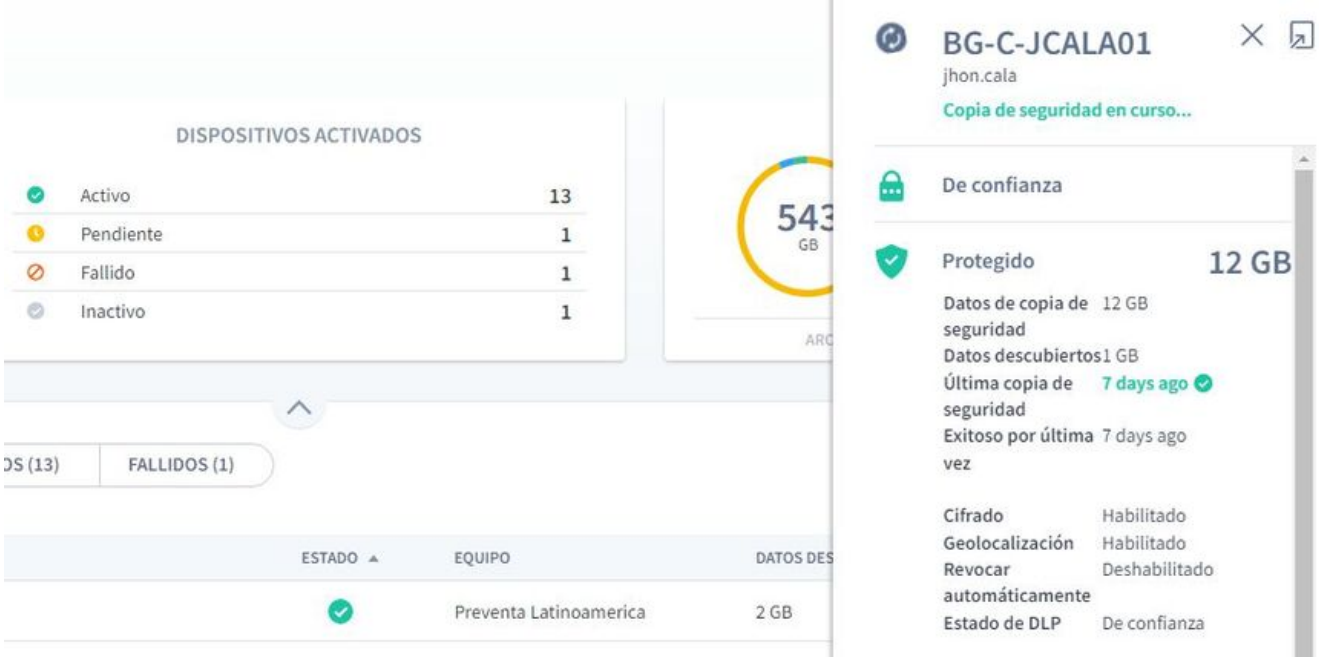
1. Clique em **Inventário** ou **Proteção**.

2. Clique no botão de opções (...) do dispositivo na lista de dispositivos.

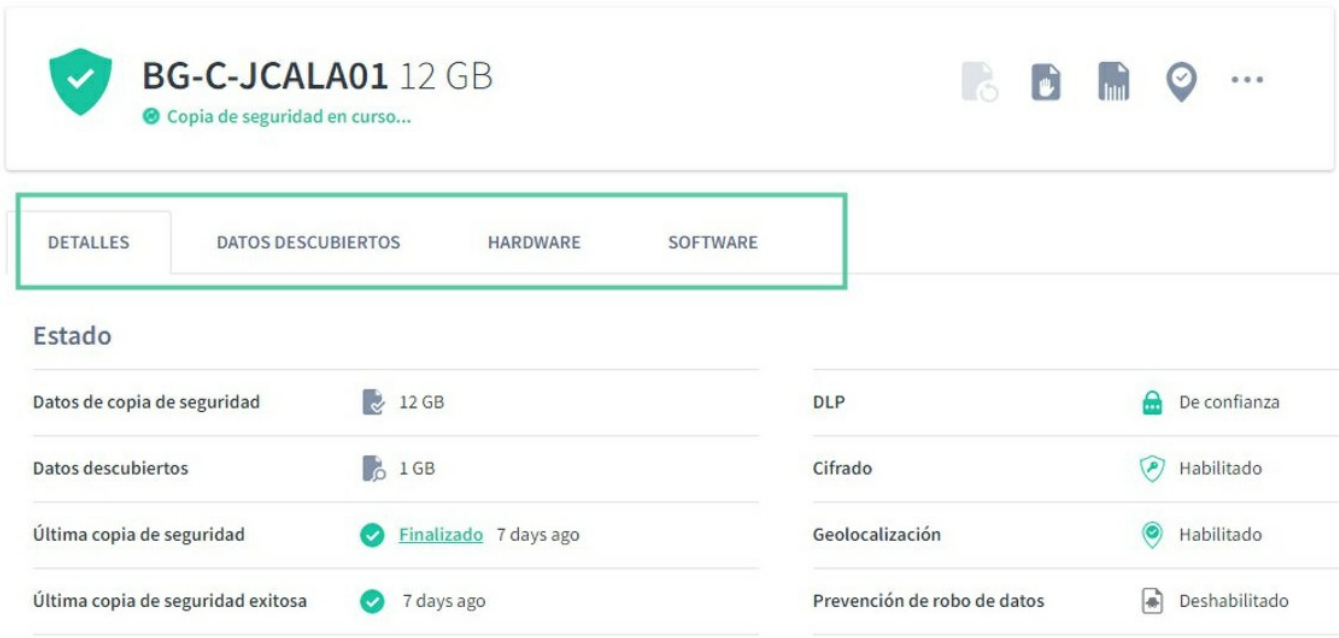
3. Clique em **Visualizar**.



Como alternativa, você pode clicar no dispositivo na lista de dispositivos e selecionar o ícone **Exibir** na parte superior do painel deslizante.

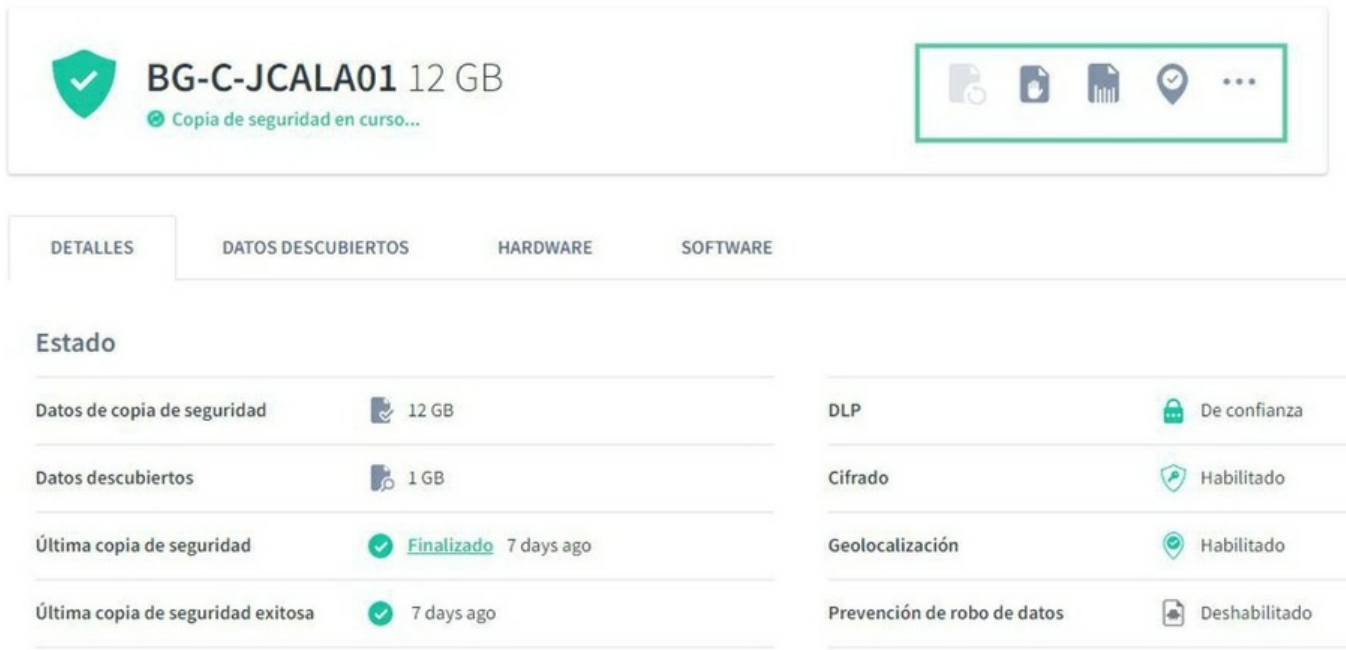


A página Dispositivo tem um painel de ação na parte superior e guias de informações abaixo. A guia **Detalhes** é exibida por padrão e você pode selecionar **Dados, Hardware e Software Descobertos**.



Ações

O banner de nome e status na parte superior da página Dispositivo contém vários ícones de ação. A disponibilidade do ícone varia dependendo de quais recursos estão habilitados na Política e se o Agente de Proteção foi habilitado.

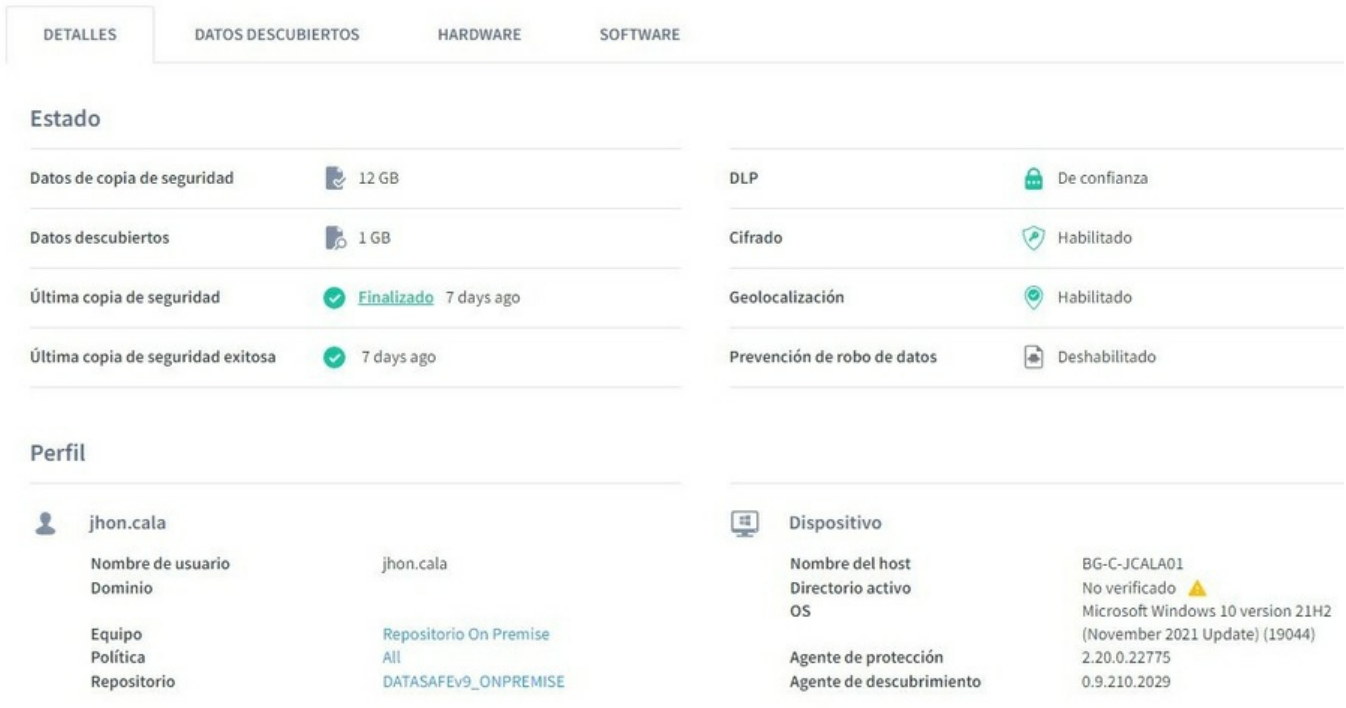


Você pode usar os ícones de ação somente depois que o Agente de Proteção tiver sido ativado:

- Fazer backup de um dispositivo manualmente
- Revogue um dispositivo.
- Limpe um dispositivo.
- Localize um dispositivo.

Detalhes

A guia Detalhes é exibida por padrão e fornece informações sobre a visualização do dispositivo Aranda Datasafe.



A seção Status inclui o tamanho dos dados de backup, a quantidade de dados descobertos, a hora e o status do backup mais recente e se os recursos DLP estão habilitados.

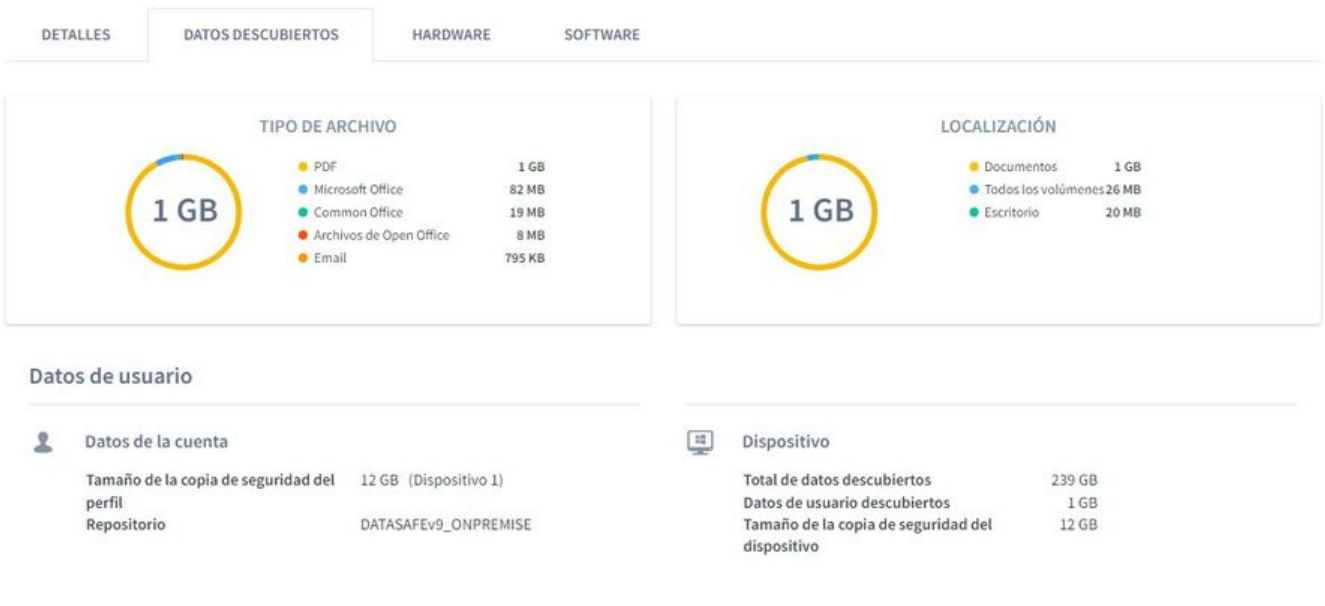
A seção Perfil exibe as credenciais do perfil do usuário e do computador, da política e do repositório aos quais o dispositivo está associado.

A seção Dispositivo exibe informações sobre o sistema operacional e os agentes em execução no dispositivo. Ele também exibe os detalhes da conexão de rede.

Dados descobertos

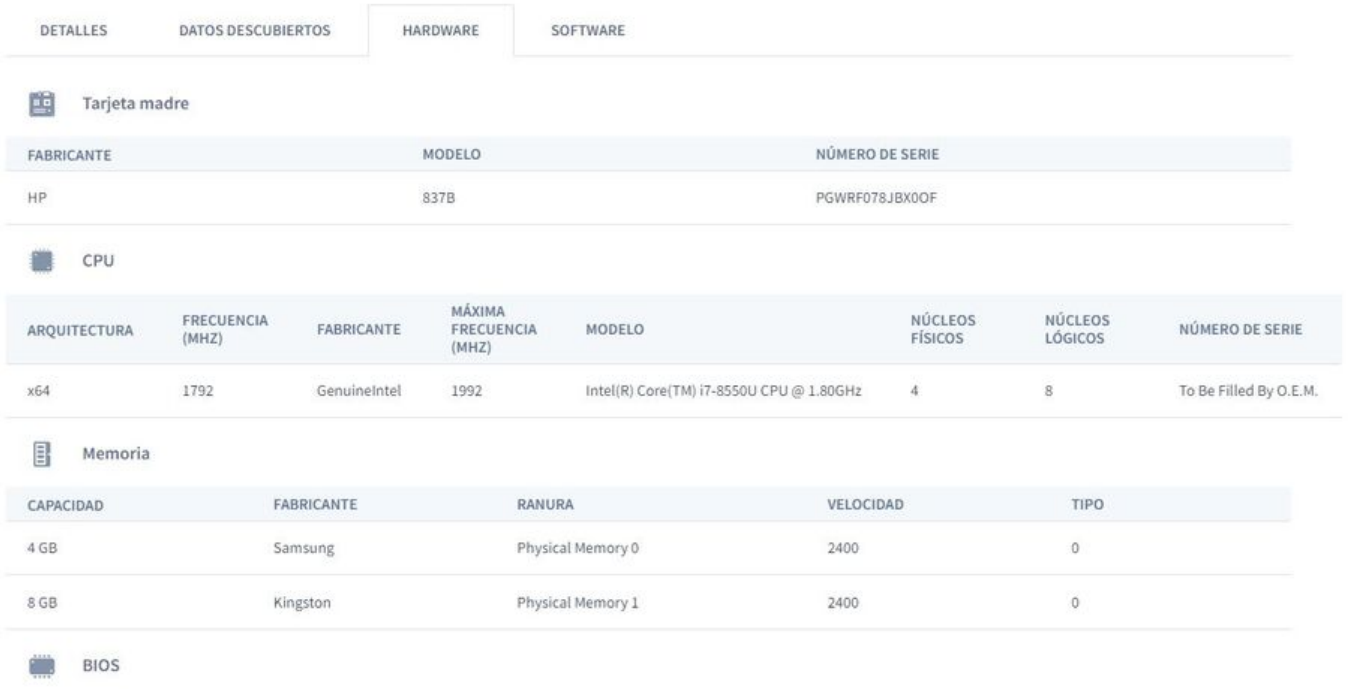
A guia Dados descobertos fornece informações sobre os dados que o Aranda Datasafe descobriu no dispositivo.

Há informações sobre os tipos de arquivo que o Aranda Datasafe descobriu e também os locais onde os dados foram encontrados.



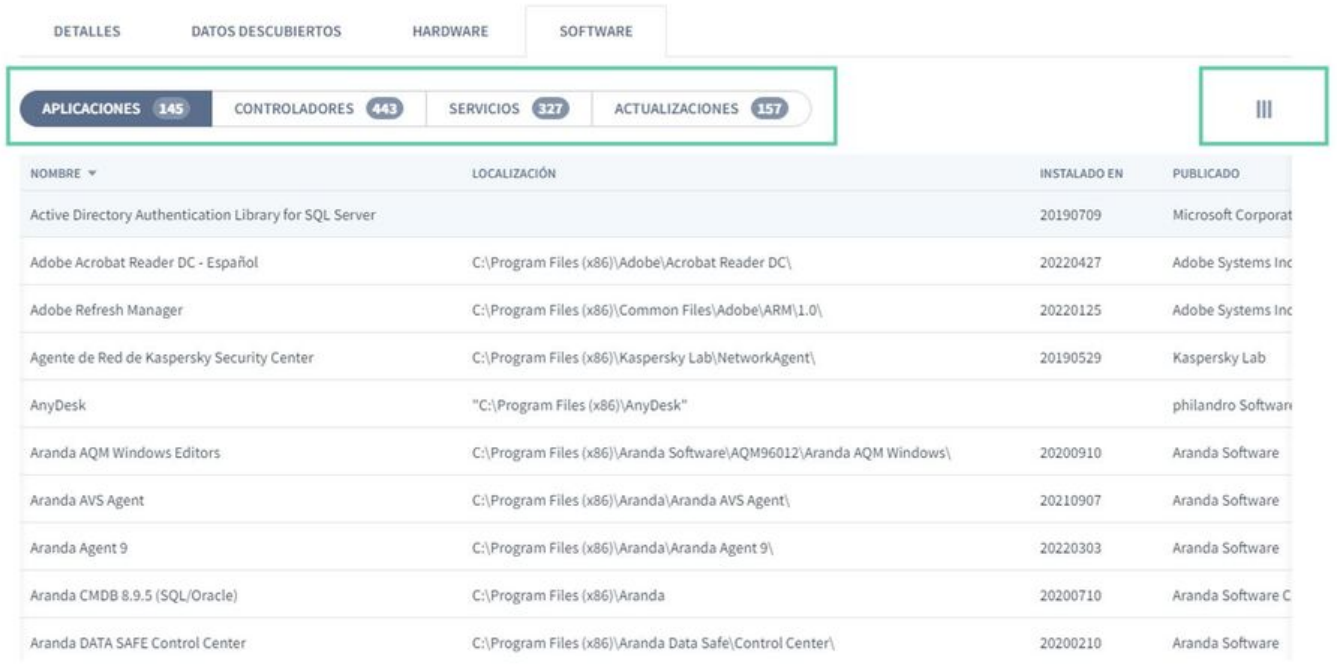
Hardware

A guia Hardware fornece informações sobre o dispositivo e seus componentes, incluindo o tipo de placa-mãe e processador e a quantidade de memória.



Software

A guia de software contém uma lista de aplicativos de software, drivers, serviços e atualizações instalados em seu dispositivo.



Por padrão, a lista mostra os **aplicativos**. Você pode clicar nos botões acima da lista para configurá-la para exibir **Drivers, Serviços ou Atualizações**.

Você pode usar a função de pesquisa para configurar a lista de software para exibir apenas informações sobre aplicativos, drivers, serviços ou atualizações que tenham um nome específico (ou parte de um nome).

Você também pode optar por ocultar colunas na lista de software. Por exemplo, você pode não estar interessado na **data de instalação** ou no **editor** no modo de exibição Aplicativos, portanto, pode ocultar essas colunas.

Para mostrar/ocultar colunas, clique no ícone Colunas e escolha quais colunas incluir ou excluir.

Ativando seus dispositivos

O Aranda Datasafe só fará backup e protegerá os dispositivos que foram ativados. Os dados de qualquer dispositivo que não esteja ativado estão potencialmente em risco.

Ao ativar um dispositivo, você cria uma solicitação para que esse dispositivo seja protegido e copiado. Se a solicitação de ativação for bem-sucedida, o dispositivo será protegido quando o próximo backup for agendado (conforme definido nas configurações de política).

Pré-requisitos

Neste artigo, explicamos como ativar seus dispositivos. Antes de ativar um dispositivo, você deve ter o seguinte:

- Uma política que define quais dados serão copiados, com que frequência será feito backup e quais configurações de proteção serão usadas **consulte Políticas**.
- Um repositório que define a área de armazenamento que será usada para armazenar os dados de backup do dispositivo. Para obter mais informações sobre repositórios, Consulte repositórios.
- Uma equipe. A política e o repositório devem ser atribuídos à equipe. O dispositivo que você está ativando também deve ser atribuído à equipe. Para mais informações, ver Equipamento.

Quando essas configurações estiverem em vigor, você poderá ativar seus dispositivos **"em risco"**.

Ativar um dispositivo

Para ativar um dispositivo "comprometido":

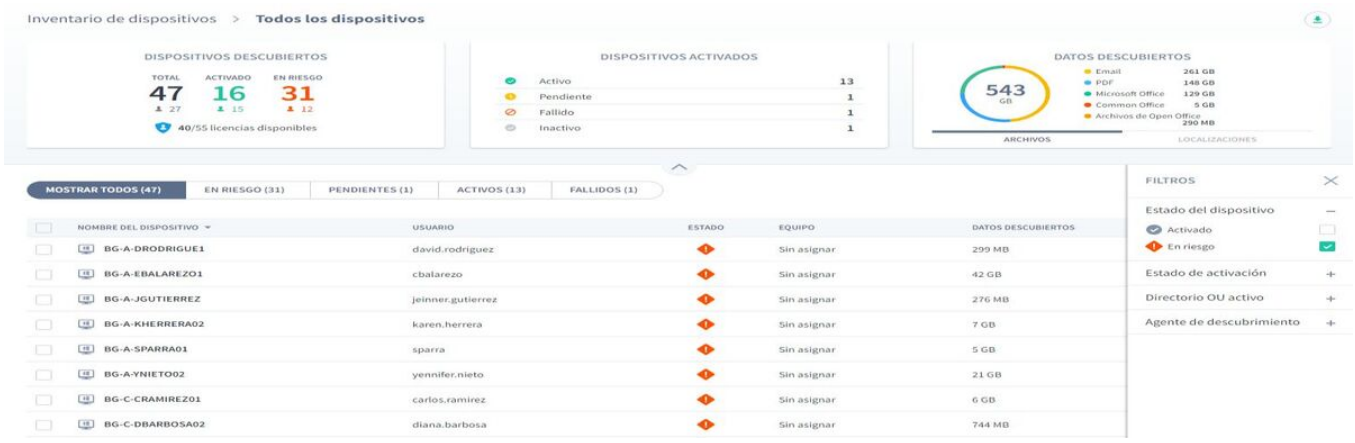
1. Clique em **Inventário**.

2. Clique no ícone de filtro acima da lista de dispositivos.

3. Escolha **Status do dispositivo** e selecione **Em risco**.

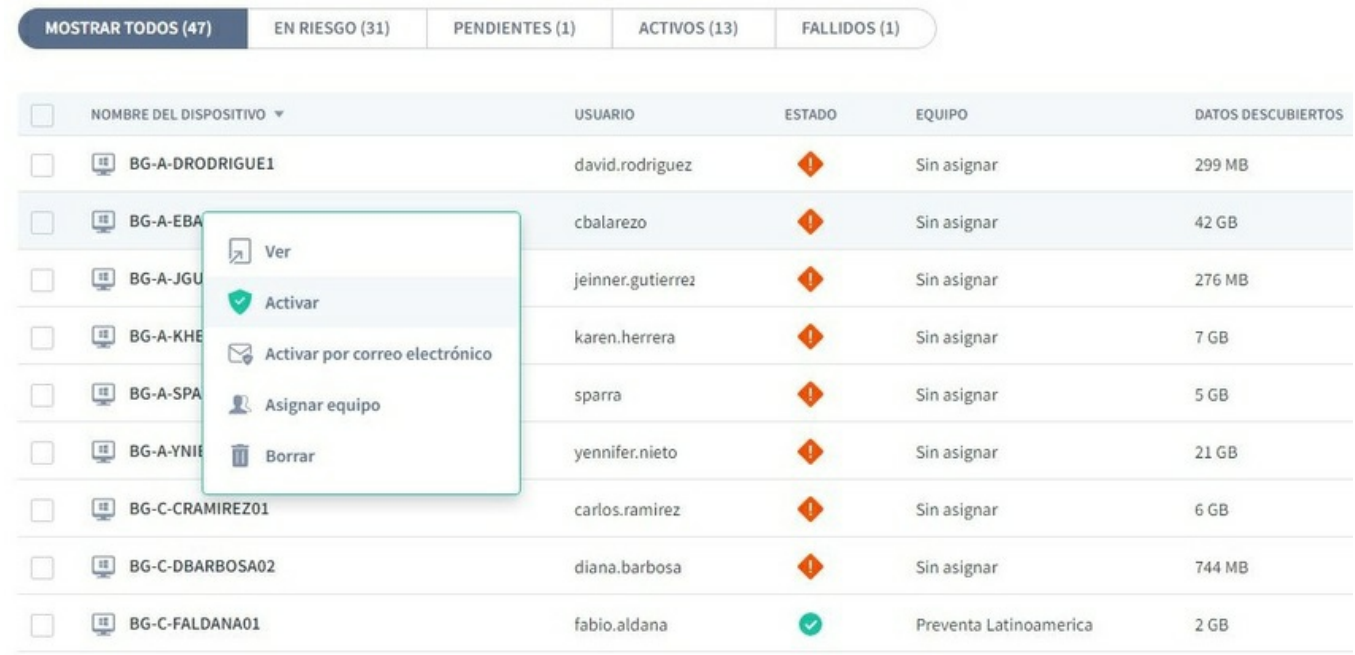
4. Clique em **Aplicar**.

A lista de dispositivos agora é filtrada para mostrar apenas os dispositivos que estão "em risco".

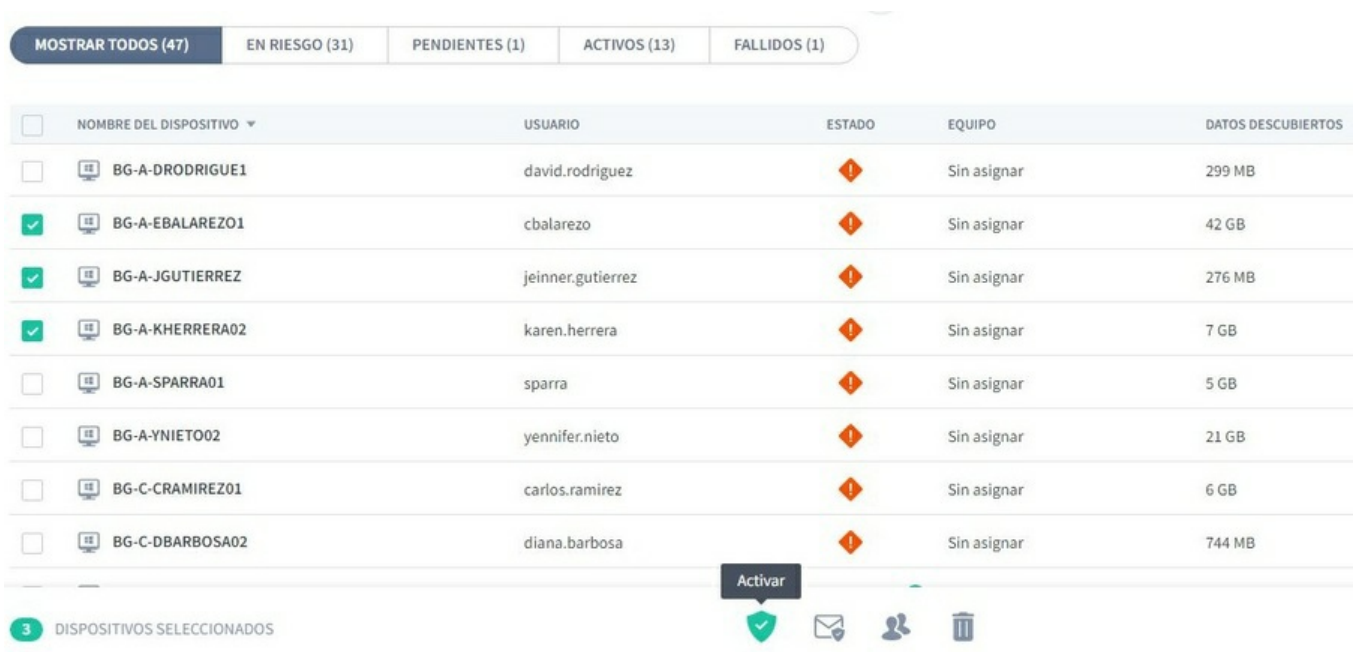


5. Existem várias maneiras de ativar dispositivos.

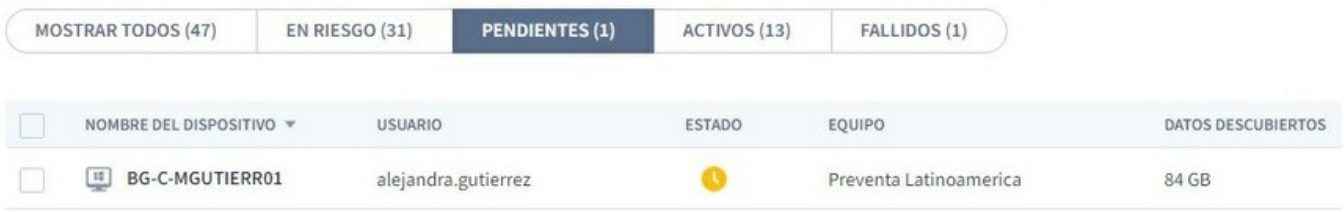
Para ativar um único dispositivo, você pode clicar no botão de opção e, em seguida, clicar em **Ativar**. Ou você pode marcar sua caixa de seleção e clicar no ícone **Ativar** na barra pop-up na parte inferior.



Para ativar vários dispositivos, marque as caixas de seleção dos dispositivos que deseja ativar. Em seguida, clique no ícone Ativar na barra pop-up na parte inferior.



Quando você ativa um dispositivo, seu status muda de Em risco para Pendente. Após um pequeno atraso, o status do dispositivo muda para Ativo e um ícone de verificação verde é exibido.



Se o dispositivo não puder ser ativado, um ícone de erro vermelho será exibido. Você precisará investigar por que a ativação falhou. Pode ser porque o usuário não está conectado ao dispositivo ou houve um problema de conexão.

6. Para descobrir quais dispositivos são protegidos pelo Aranda Datasafe, clique em Proteção. A página de proteção exibe detalhes de dispositivos que atualmente possuem dados criptografados e com backup do Aranda Datasafe.

Filtragem de página de inventário

Por padrão, a página Inventário exibe informações para todos os computadores e dispositivos. Mas, se necessário, você pode filtrar a página Inventário para mostrar apenas informações que atendam a determinados critérios. Por exemplo, você pode filtrar a página Inventário para mostrar apenas informações de dispositivos em um computador específico.

Há várias maneiras de filtrar a página Inventário (ou partes da página Inventário):

Filtrar por equipe

Usar uma pesquisa para filtrar a lista de dispositivos

Filtrar a lista de dispositivos por critérios selecionados

Mostrar ou ocultar colunas na lista de dispositivos.

Filtrar por equipe

Você pode usar a barra lateral Computadores para filtrar a página Inventário para que ela mostre apenas informações sobre os dispositivos em determinados computadores. Por exemplo, você pode configurar a página Inventário para exibir apenas informações de uma equipe de "Finanças" e de uma equipe de "RH".

Nota

Se você usar a barra lateral do Teams para filtrar a página Inventário, todos os painéis de informações e a lista de dispositivos serão filtrados.

1. Clique em **Inventário**.

2. Na seção **Equipamento**, clique em:

- **Todos os dispositivos** para exibir informações sobre todos os dispositivos em todos os computadores (isso equivale a remover o filtro do computador)
- **Não atribuído** para exibir informações apenas para os dispositivos que ainda não estão atribuídos a uma equipe
- **** para exibir informações sobre dispositivos em uma equipe específica.

Quando você seleciona um dispositivo ou dispositivos, a página Inventário é atualizada e as telas de informações e a lista de dispositivos são filtradas. Eles mostram apenas informações sobre os dispositivos nas equipes selecionadas.

Clique em **Todos os dispositivos** na barra lateral **Teams** para remover o filtro.

Use uma pesquisa para filtrar a lista de dispositivos

Você pode usar a função de pesquisa para filtrar a lista de dispositivos para que ela inclua apenas dispositivos que tenham determinados valores. Por exemplo, você pode usar a pesquisa para filtrar a lista para que ela mostre apenas dispositivos com um nome específico (ou prefixo de um nome). Isso é útil se você tiver um esquema de nomenclatura de dispositivo consistente e quiser ver apenas dispositivos específicos. Por exemplo, você pode ter dispositivos que começam com nomes que começam com ERL, para que você possa pesquisar ERL.

Você pode usar a pesquisa para filtrar a lista de dispositivos por qualquer valor de texto, incluindo nome do dispositivo, nome de usuário e nome do computador.

Para aplicar um filtro de pesquisa:

1. Clique no ícone de pesquisa acima da lista de dispositivos.

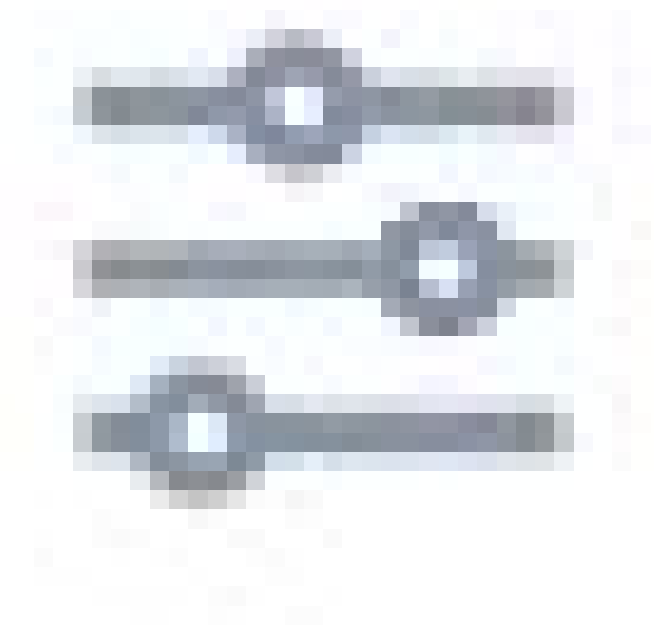
2. Insira os primeiros caracteres do valor de texto que deseja usar como filtro. O Aranda Datasafe aplica o filtro à medida que você digita, para que você possa fazer correspondências parciais OU inserir o valor do texto completo para ser mais específico.

Filtre a lista de dispositivos por critérios selecionados

Você pode filtrar a lista de dispositivos para mostrar apenas os dispositivos que correspondem aos critérios escolhidos.

Para filtrar a lista de dispositivos:

1. Clique no ícone de filtro



para exibir as opções de Filtros deslizantes.

2. Expanda Categorias de filtro e selecione os critérios de filtro que deseja aplicar. A lista de dispositivos mostrará apenas os dispositivos que correspondem a todos os critérios selecionados.

3. Clique em **Aplicar**.

Você pode escolher qualquer uma destas opções de filtro:

Filtrar	Descrição	Opções
Status do dispositivo	Filtre os dispositivos com base em seu status de ativação.	Ativado (selecionado para ativação) Em risco (ainda não selecionado para ativação)
Status de ativação	Filtre a lista para mostrar apenas dispositivos com um status de ativação específico.	Pendente O processo de ativação está programado para começar. -ativo. O dispositivo foi ativado com sucesso Falha - O processo de ativação não foi bem-sucedido.
UO do Active Directory	Filtre por uma unidade organizacional de dispositivos do Active Directory. Esses dados de UO vêm do agente de descoberta no dispositivo do usuário.	Lista de UOs disponíveis
Agente da Descoberta	Filtre a lista para mostrar apenas os dispositivos que usam uma versão específica do software Discovery Agent.	Lista de agentes de descoberta disponíveis

Para remover os filtros, clique no ícone Filtro e clique em**Redefinir** (ou desmarque cada uma das caixas de filtro).

Mostrar ou ocultar colunas na lista de dispositivos

Você pode optar por mostrar ou ocultar colunas na lista de dispositivos. Por exemplo, talvez você não se importe com qual versão do Discovery Agent foi usada para descobrir um dispositivo, portanto, você pode ocultá-lo da exibição.

Para mostrar/ocultar colunas, clique no ícone Colunas e escolha quais colunas incluir. Para obter uma descrição de cada coluna, consulte o[Página de inventário](#).

Proteção

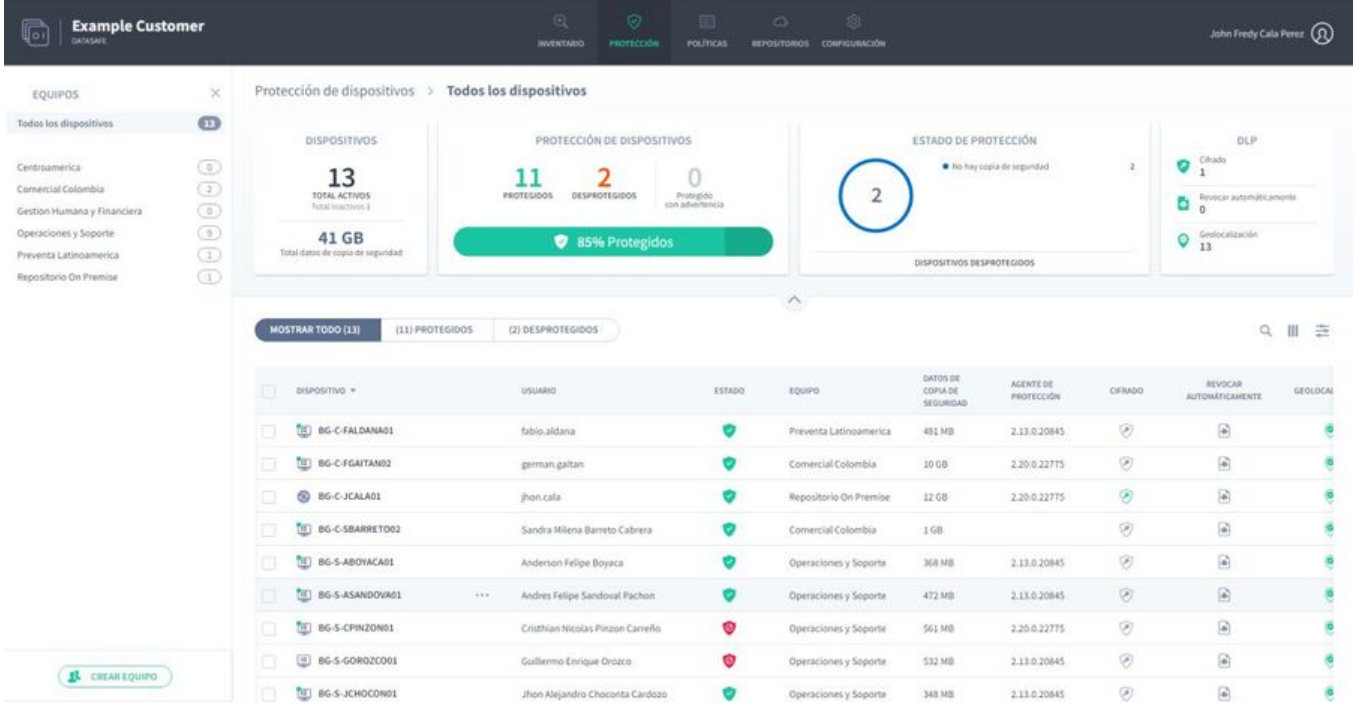
Proteção

O Aranda Datasafe protege os dados da sua empresa realizando automaticamente backups criptografados dos dados da sua empresa. Ele também possui recursos de prevenção contra perda de dados (DLP) que você pode ativar ou desativar, dependendo de seus requisitos.

Você pode usar a página Proteção para visualizar o status de proteção de todos os seus dispositivos ativados. Observe que o[Página de proteção](#) Ele não mostra dados de dispositivos que ainda não foram ativados.

Proteção do dispositivo

A página**Proteção** fornece informações sobre os dispositivos ativados e seu status de proteção atual. Você pode usá-lo para descobrir quais dispositivos estão atualmente protegidos, desprotegidos ou protegidos com aviso.



Status de proteção	Descrição
Protegido	O dispositivo foi ativado, tem o software Protection Agent instalado e seus dados são copiados pelo Aranda Datasafe.
Desprotegido	O dispositivo foi ativado, tem o software do Agente de Proteção instalado, mas não foi feito backup com êxito nos últimos 5 dias. (5 dias é o intervalo de proteção padrão) Até que um backup bem-sucedido seja feito, os dados em um dispositivo desprotegido estarão em risco. O primeiro backup do dispositivo geralmente acontece cerca de 10 minutos após a ativação do dispositivo. Mas pode levar mais tempo, dependendo de quanto tempo leva para o software Protection Agent indexar os arquivos.
Protegido com Aviso	O dispositivo foi ativado e tem o software Protection Agent instalado. O dispositivo executou um backup bem-sucedido nos últimos 5 dias, mas o Aviso falhou na última tentativa de backup.

A página Proteção exibe apenas os dispositivos que foram detectados e ativados com êxito. Se a página Proteção estiver vazia, seus dispositivos não foram descobertos ou foram descobertos, mas não ativados.

⚐ >**Nota:** No Página Inventário , usamos o termo "Em risco" para descrever um dispositivo que foi descoberto, mas não ativado. Os dispositivos "Desprotegidos" na página Proteção foram ativados, mas não foi feito backup no intervalo de proteção. Os dispositivos "em risco" e "desprotegidos" contêm dados vulneráveis.

Dispositivos

O painel Dispositivos fornece um resumo de:

- Número de dispositivos ativos e inativos
- Quantidade de dados de backup em todos os dispositivos.

Os dados de backup mostram a soma de todos os dados incluídos na política em todos os dispositivos em um momento específico. Esse número não é a informação armazenada no repositório.

Um dispositivo ativo é um dispositivo que foi ativado e conectado ao Aranda Datasafe nos últimos 30 dias.

Campo	Descrição
Total de Ativos	O número total de dispositivos ativos. Esses dispositivos foram ativados e estão**protegidos, protegidos com aviso ou desprotegidos** (consulte Proteção do dispositivo). Os dispositivos ativos não são necessariamente protegidos ou armazenados em backup.
Total Inativo	O número total de dispositivos que foram ativados, mas não se conectaram ao Aranda Datasafe nos últimos 30 dias (e, portanto, não são copiados para esse período de tempo).
Total de dados em backup	A quantidade de dados em todos os dispositivos incluídos nas políticas de backup em um ponto específico no tempo. Você pode usar isso como uma indicação de quanto espaço de armazenamento é necessário. Mas lembre-se de que a criptografia de dados de backup será alterada sempre que a Política for alterada ou quando os usuários adicionarem/removerem dados de backup em seus dispositivos.

Proteção do dispositivo

O painel Proteção de Dispositivo fornece informações sobre o número de dispositivos que foram copiados e protegidos nos últimos 5 dias. Amostra:

Campo	Descrição
Protegido	O número total de dispositivos que foram copiados com êxito nos últimos 5 dias.
Desprotegido	O número total de dispositivos que não foram submetidos a backup com êxito nos últimos 5 dias.
Protegido com Aviso	O número total de dispositivos que foram submetidos a backup com êxito nos últimos 5 dias, mas o backup mais recente falhou.

Status protegido

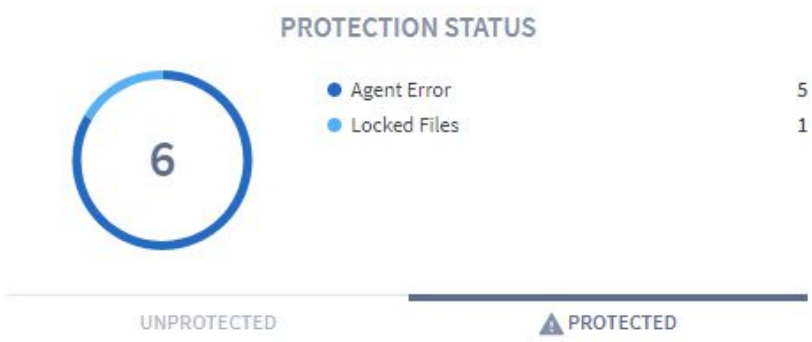
O painel Status de Proteção fornece um resumo do número de dispositivos que estão atualmente protegidos, protegidos com avisos ou desprotegidos.

Se alguns de seus dispositivos estiverem no status desprotegido ou desprotegido com aviso, o painel Status de proteção terá duas guias**Desprotegido** e **Protegido** com aviso (mostrado na parte inferior do painel).

A guia **Desprotegido** mostra:

Campo	Descrição
Sem encosto	O número de dispositivos que estão desprotegidos e não têm dados de backup no Aranda Datasafe.
Off-line	O número de dispositivos que estão desprotegidos e não têm uma conexão com o Aranda Datasafe.
Conexão perdida	O número de dispositivos que estão desprotegidos e perderam a conexão com o Aranda Datasafe
Erro do agente	O número de dispositivos que têm um erro de agente que o servidor não consegue reconhecer. Se você receber mensagens de erro do agente, entre em contato com nossa equipe de suporte técnico para obter assistência.
Limite de conexão do servidor	O número de dispositivos que tentam se conectar ao Aranda Datasafe quando o limite de conexão do servidor já foi atingido. O Aranda Datasafe permite um certo número de conexões simultâneas (60 por padrão) e, uma vez atingido esse limite, nenhuma conexão adicional pode ser feita. Os dispositivos tentarão novamente em alguns minutos para verificar se uma conexão está disponível e fazer backup dela.
Outros	O número de erros que não são categorizados. Se você tiver outros erros, entre em contato com nossa equipe de suporte técnico para obter assistência. (reportedecasos@arandasoft.com)

A guia **Protegido com aviso** mostra o número de dispositivos protegidos com um aviso. Se houver avisos, as estatísticas serão fornecidas para os avisos (conforme mostrado abaixo):



Campo	Descrição
Erro do agente	O número de dispositivos protegidos, mas com um erro de agente que o servidor não consegue reconhecer. Se você receber mensagens de erro do agente, entre em contato com nossa equipe de suporte técnico para obter assistência.
Arquivos bloqueados	O número de dispositivos protegidos, mas com arquivos bloqueados (arquivos que estavam abertos no dispositivo quando o backup foi feito). O Aranda Datasafe pode fazer backup de arquivos bloqueados, mas o sucesso do backup depende do serviço VSS do Windows funcionar corretamente. Se você bloqueou avisos de arquivo, recomendamos que filtre a Lista de dispositivos na página Protegido para mostrar apenas os dispositivos com o status "protegido com aviso". Em seguida, exiba o log de backup do dispositivo para determinar quais arquivos foram bloqueados. Você pode então decidir se deseja fechar os arquivos nos dispositivos e fazer backup dos dispositivos manualmente ou deixá-los até o próximo backup agendado.

DLP

O painel DLP exibe um resumo do número de dispositivos que usam os recursos de Prevenção contra Perda de Dados (criptografia, revogação automática e geolocalização). Os recursos DLP são habilitados e desabilitados nas configurações de política.

Barra lateral do Teams

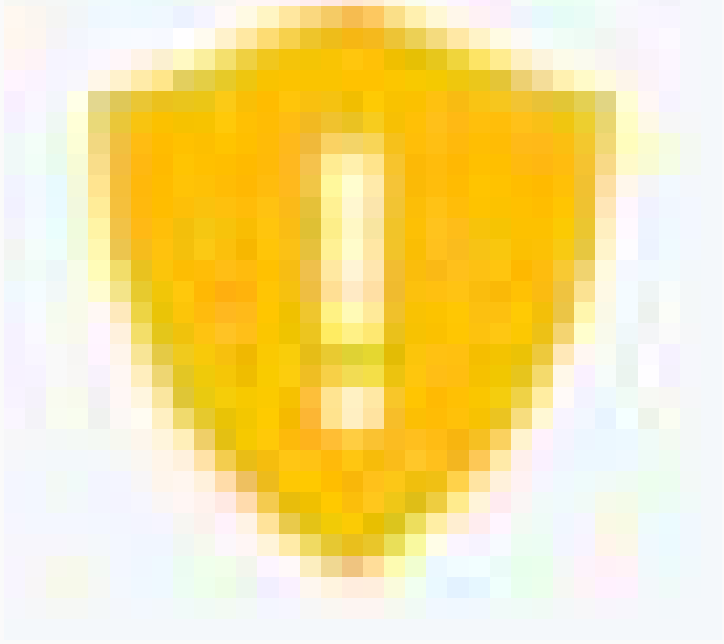
No lado esquerdo da página Proteção está a barra lateral do Teams. Isso exibe uma lista dos dispositivos configurados no Datasafe Aranda (além de Todos os dispositivos e Não atribuídos, que estão integrados).

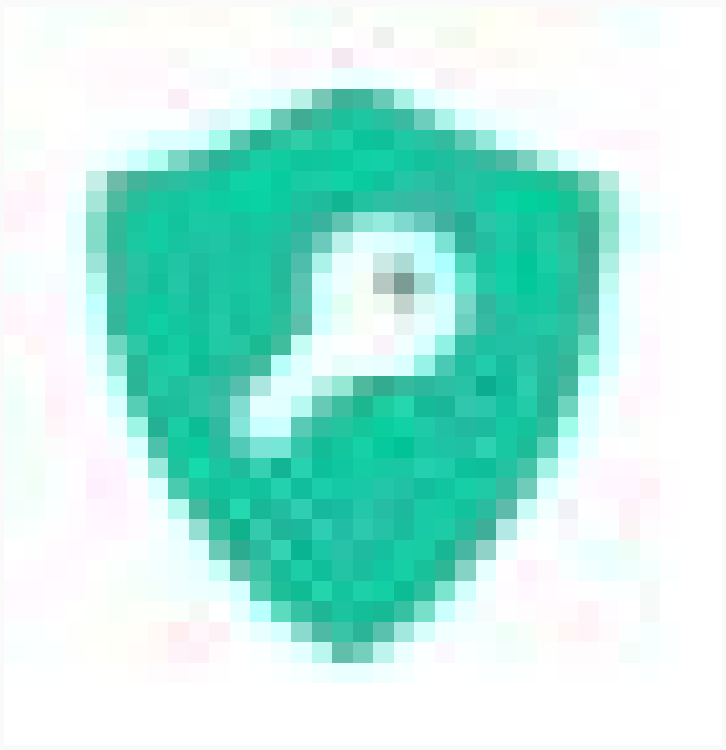
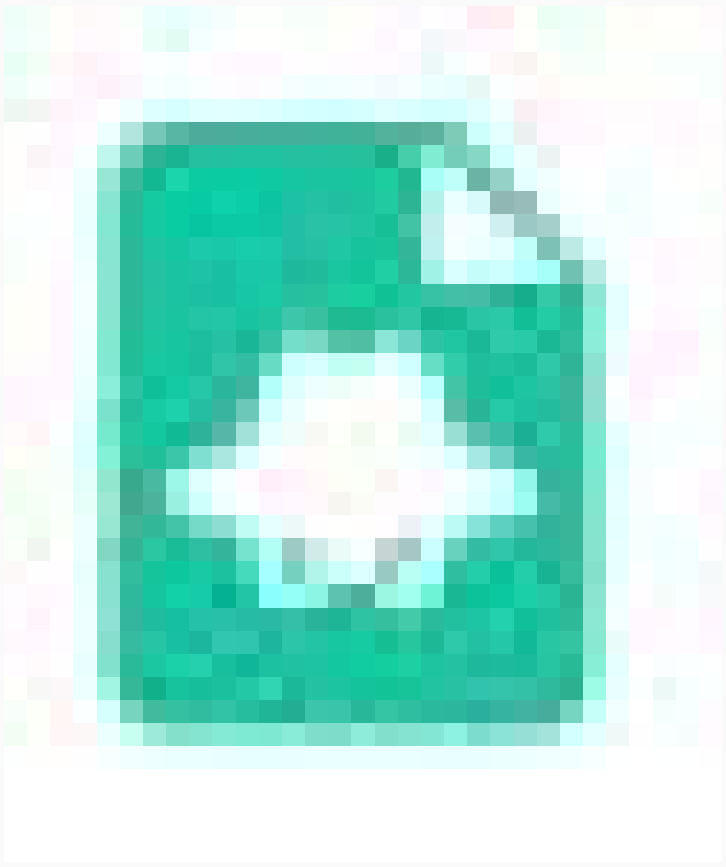
Se você clicar em um computador, os painéis de proteção e a lista de dispositivos serão atualizados para que ele exiba apenas informações dos dispositivos no computador selecionado. Você pode clicar em **Todos os dispositivos** para definir o inventário para exibir dados para cada dispositivo.

Os usuários administradores podem usar um atalho de teclado para selecionar computadores sobre os quais gerar relatórios. Pressione a tecla CTRL e selecione o equipamento que deseja incluir.

Lista de proteção de dispositivos

A seção inferior Proteção exibe a Lista de Proteção do Dispositivo, que contém um resumo dos dispositivos que o Aranda Datasafe descobriu e seu status de proteção.

Campo	Descrição
Dispositivo	O nome do dispositivo.
Usuário	O nome do usuário associado ao dispositivo.
Situação	Exibe o status de proteção: Protegido  Protegido com aviso Desprotegido 

Campo	Descrição
Equipe	O computador ao qual o dispositivo está atribuído.
Dados Apoiados	O Aranda Datasafe faz backup de uma certa quantidade de dados no dispositivo (de acordo com uma Política). A quantidade é exibida na coluna Dados de backup.
Agente de Proteção	A versão do software do Agente de Proteção que está atualmente instalada no dispositivo.
Criptografia	Mostra se o recurso de criptografia local está habilitado para o dispositivo. Você pode habilitar e desabilitar a criptografia local na Política associada ao Computador (do qual o dispositivo é membro). Um ícone verde significa que está ativado, um ícone cinza significa que está desativado. 
Revogação automática	<p>Mostra se o recurso de revogação automática está habilitado para o dispositivo. Você pode habilitar e desabilitar a revogação automática na Política associada à Equipe (da qual o dispositivo é membro). Um ícone verde significa que está ativado, um ícone cinza significa que está desativado. 
	Mostra se o recurso de geolocalização está habilitado para o dispositivo. Você pode habilitar e desabilitar a geolocalização na Política associada à Equipe (da qual o dispositivo é membro). Um ícone verde significa que está ativado, um ícone cinza significa que está desativado. 

Campo	Descrição
Geolocalização	
Status do DLP	Exibe o status da prevenção contra perda de dados. Isso pode ser: **Confiável**: o dispositivo foi autenticado e pode se conectar ao Aranda Datasafe. **Revogado**: o dispositivo foi revogado, portanto, usuários não autorizados não podem acessar os dados criptografados no dispositivo. Ele não é confiável e nenhum outro backup ou restauração será executado. **Apagado**: O dispositivo foi apagado. Ele não é confiável e nenhum outro backup ou restauração será executado.

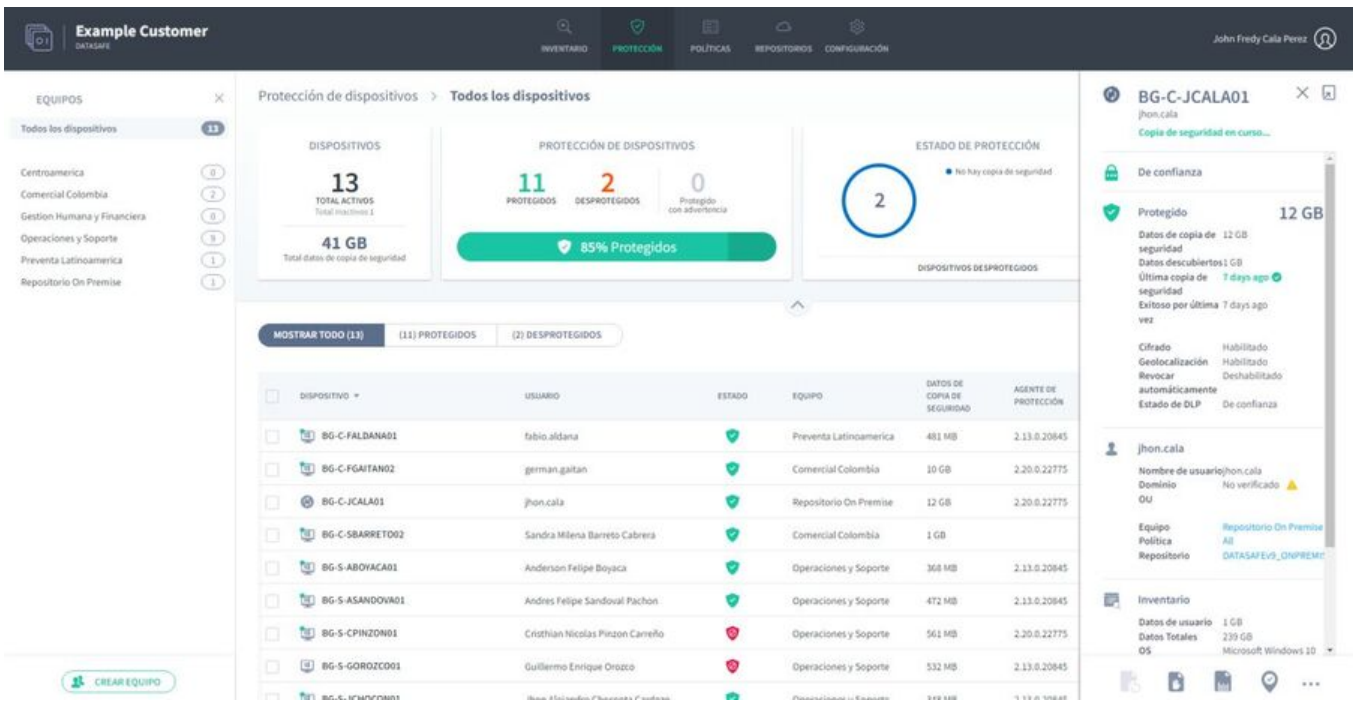
Por padrão, a lista de dispositivos exibe informações para todos os dispositivos (filtro**Mostrar Tudo**). Se preferir, você pode clicar em uma das outras opções de filtro. Existem três outras opções de filtro possíveis, uma para cada estado: **protegido, protegido com aviso, desprotegido**. As opções de filtro só estarão disponíveis se houver dispositivos nesse estado específico.

Se você realçar um dispositivo na lista, um botão de opção (...) aparecerá à direita do nome do dispositivo. Clique no botão de opção para exibir um menu de contexto com estas opções:

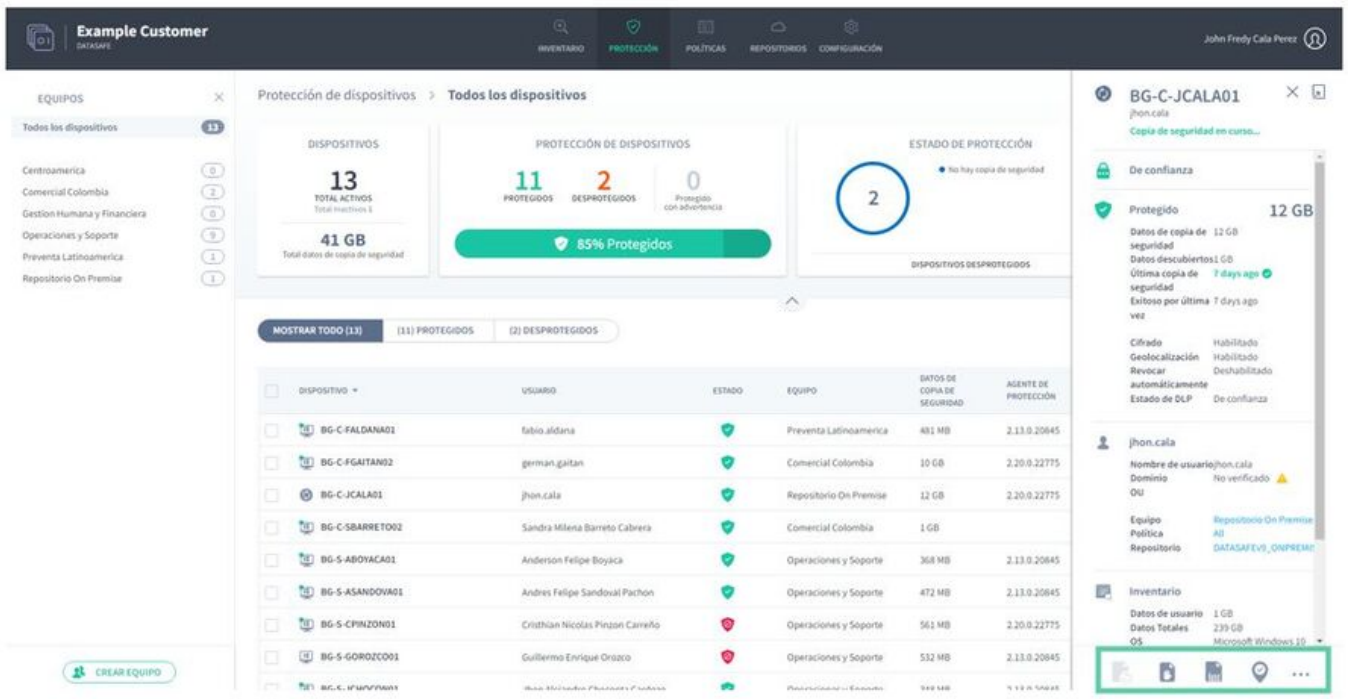
Campo	Descrição
Visão	Exibe a página Dispositivo, que contém detalhes sobre o dispositivo, incluindo seu hardware e software.
Atribuir equipe	Use-o para atribuir o dispositivo a uma equipe. O Aranda Datasafe só pode fazer backup e proteger dispositivos atribuídos a computadores, pois os computadores devem estar associados a um repositório e a uma política.
Remover	Use-o para remover um dispositivo. Se você excluir o último dispositivo restante de um usuário, uma licença será liberada e estará disponível para uso por outros usuários.

Barra lateral do dispositivo

Se você clicar em um dispositivo na lista de dispositivos, a barra lateral do dispositivo será exibida. Exibe informações adicionais sobre o dispositivo selecionado. Se você clicar no ícone Exibir no canto superior, o Aranda Datasafe exibirá a página Dispositivo, que contém uma visão mais detalhada do dispositivo, incluindo seu hardware e software.



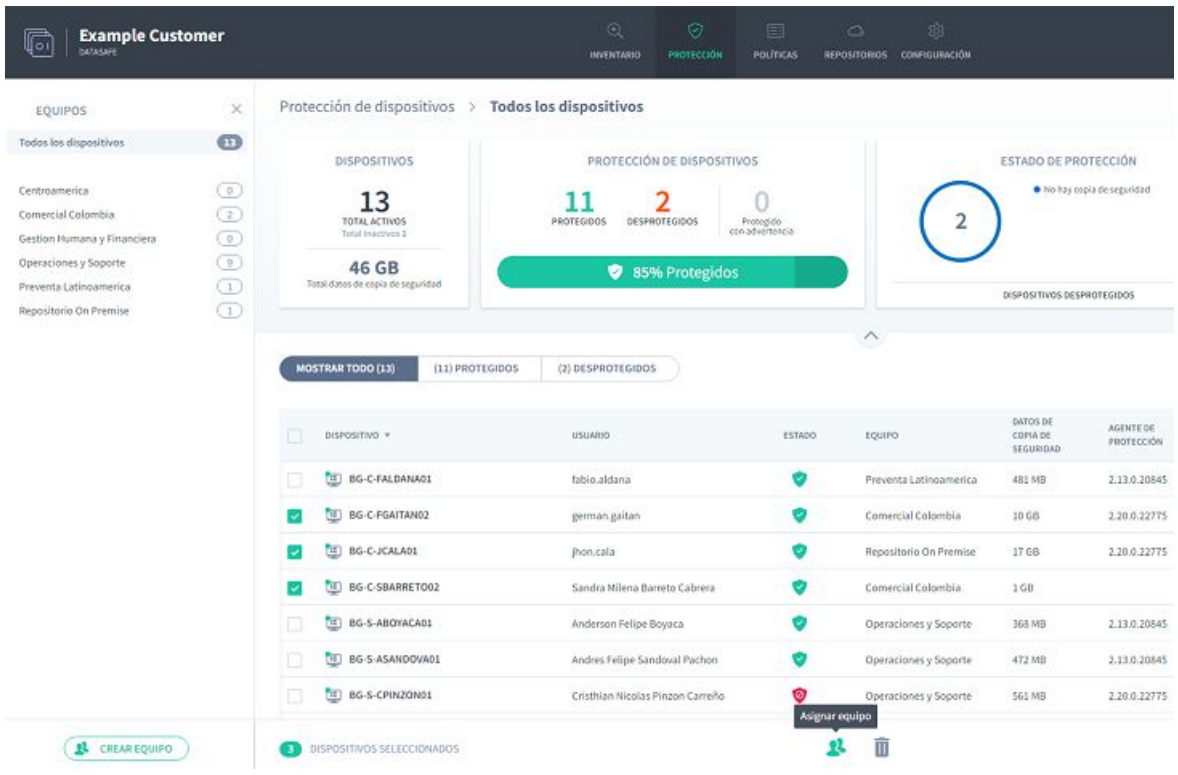
Na parte inferior da barra lateral do dispositivo, há ícones para fazer backup manual do dispositivo, revogá-lo, apagá-lo e usar a geolocalização para descobri-lo. Os mesmos ícones também estão disponíveis na página Dispositivo.



Ações de vários dispositivos

Você pode usar a lista de dispositivos para aplicar uma única ação a vários dispositivos. Por exemplo, você pode atribuir vários dispositivos ao mesmo computador.

Use a caixa de seleção à esquerda de cada linha de dispositivos para selecionar um dispositivo. Quando você marca as caixas de seleção, as opções de ação aparecem na parte inferior da lista. Eles funcionam da mesma maneira que para dispositivos individuais, exceto que a ação será aplicada a todos os dispositivos selecionados.



Proteção de filtragem

Por padrão, a página Proteção exibe informações de todos os computadores e dispositivos. Mas, se necessário, você pode filtrar a página Proteção para mostrar apenas informações que atendam a determinados critérios. Por exemplo, você pode filtrar a página Proteção para mostrar apenas informações sobre os dispositivos em um computador específico.

Há várias maneiras de filtrar a página Proteção (ou partes da página Proteção):

Filtrar por equipe

Usar uma pesquisa para filtrar a lista de dispositivos

Filtrar a lista de dispositivos por critérios selecionados

Mostrar ou ocultar colunas na lista de dispositivos

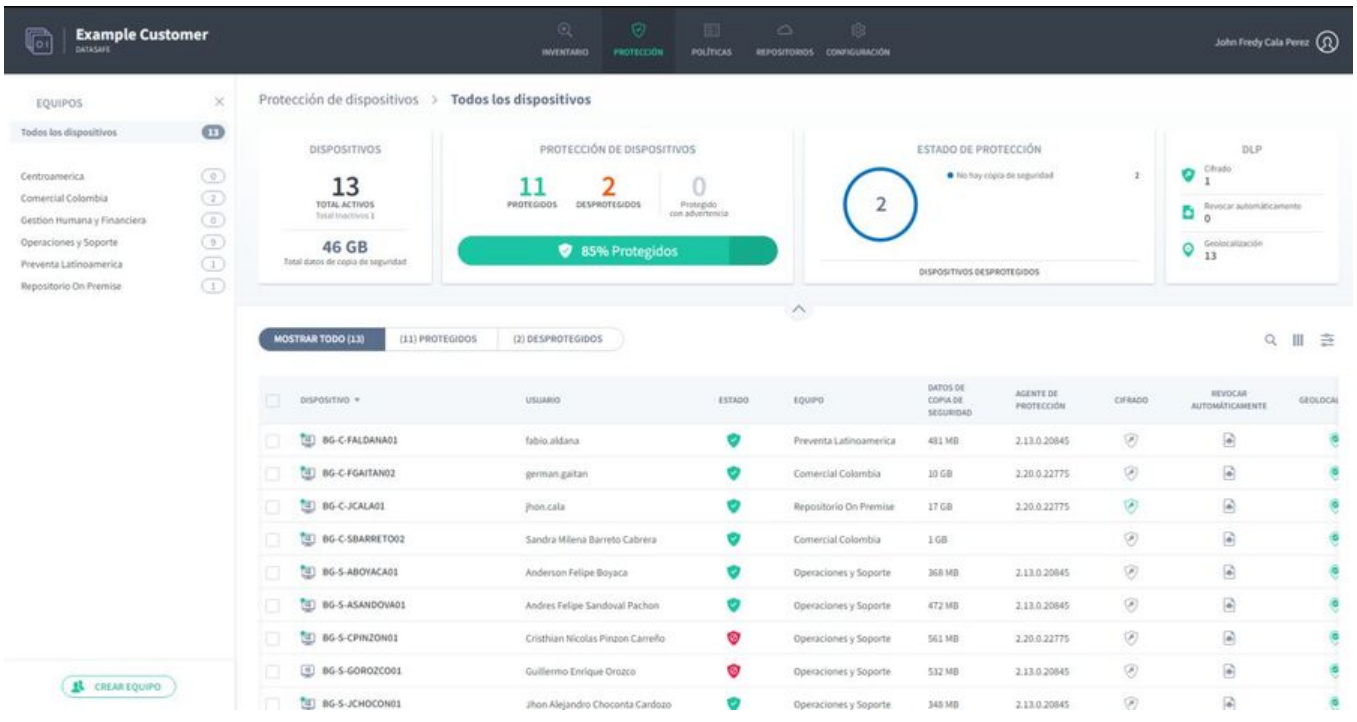
Filtrar por equipe

Você pode usar a barra lateral **Dispositivos** para filtrar a página **Proteção** para que ela mostre apenas informações sobre dispositivos em determinados **Dispositivos**. Por exemplo, você pode configurar a página Proteção para exibir apenas informações de uma equipe de "Finanças" e de uma equipe de "Recursos humanos".

1. Clique em **Proteção**.

2. Na seção **Equipamento**, clique em:

- **Todos os dispositivos** para exibir informações sobre todos os dispositivos em todos os computadores (isso equivale a remover o filtro do computador)
- **Não atribuído** para exibir informações apenas para os dispositivos que ainda não estão atribuídos a uma equipe
- **** para exibir informações sobre dispositivos em uma equipe específica.



Quando você seleciona um dispositivo ou dispositivos, a página **Proteção** atualiza e filtra as telas de informações e a lista de dispositivos. Eles mostram apenas informações sobre os dispositivos nas equipes selecionadas.

Clique em **Todos os dispositivos** na barra lateral **Teams** para remover o filtro.

Use uma pesquisa para filtrar a lista de dispositivos

Você pode usar a função **pesquisar** para filtrar a lista de dispositivos para que ela inclua apenas dispositivos que tenham determinados valores. Por exemplo, você pode usar a pesquisa para filtrar a lista para que ela mostre apenas dispositivos com um nome específico (ou prefixo de um nome). Isso é útil se você tiver um esquema de nomenclatura de dispositivo consistente e quiser ver apenas dispositivos específicos. Por exemplo, você pode ter dispositivos que começam com nomes que começam com ERL, para que você possa pesquisar ERL.

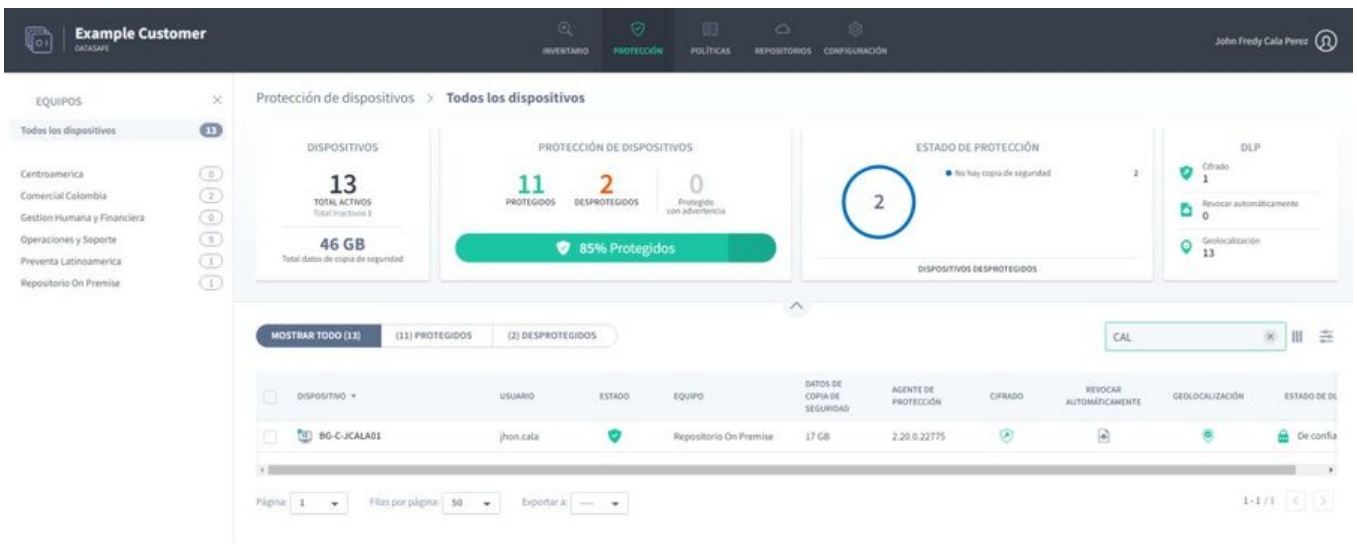
Você pode usar a pesquisa para filtrar a lista de dispositivos por qualquer valor de texto, incluindo o nome do dispositivo, o nome do usuário e o nome do computador.

Para aplicar um filtro de pesquisa:

1. Clique no ícone de pesquisa acima da lista de dispositivos.

2. Insira os primeiros caracteres do valor de texto que deseja usar como filtro. O Aranda Datasafe aplica o filtro à medida que você digita, para que você possa fazer correspondências parciais ou inserir o valor de texto completo para ser mais específico.

Você pode pesquisar o nome do dispositivo, nome de usuário ou nome do computador.



Filtre a lista de dispositivos por critérios selecionados

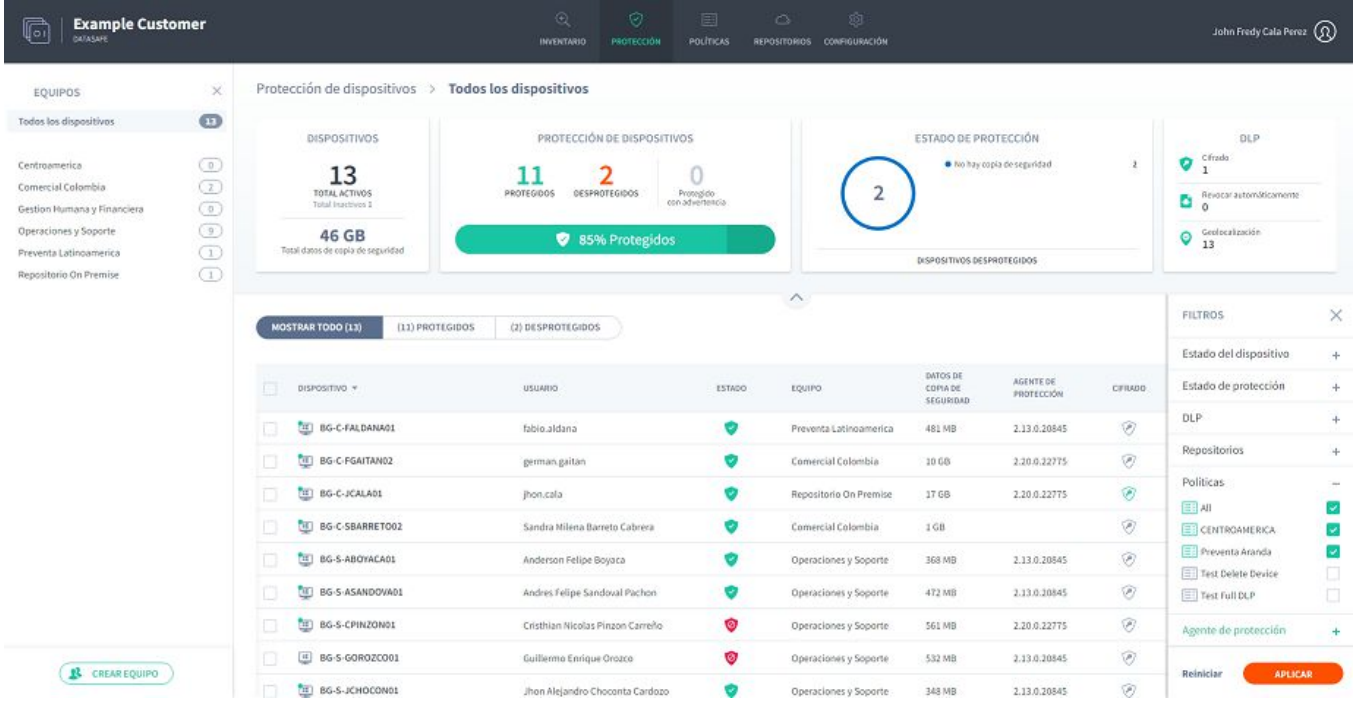
Você pode filtrar a lista de dispositivos para mostrar apenas os dispositivos que correspondem aos critérios escolhidos.

Para filtrar a lista de dispositivos:

1. Clique no ícone de filtro para exibir as opções de filtro deslizante.

2. Expanda Categorias de filtro e selecione os critérios de filtro que deseja aplicar. A lista de dispositivos mostrará apenas os dispositivos que correspondem a todos os critérios selecionados.

3. Clique em Aplicar.



Você pode escolher qualquer uma destas opções de filtro:

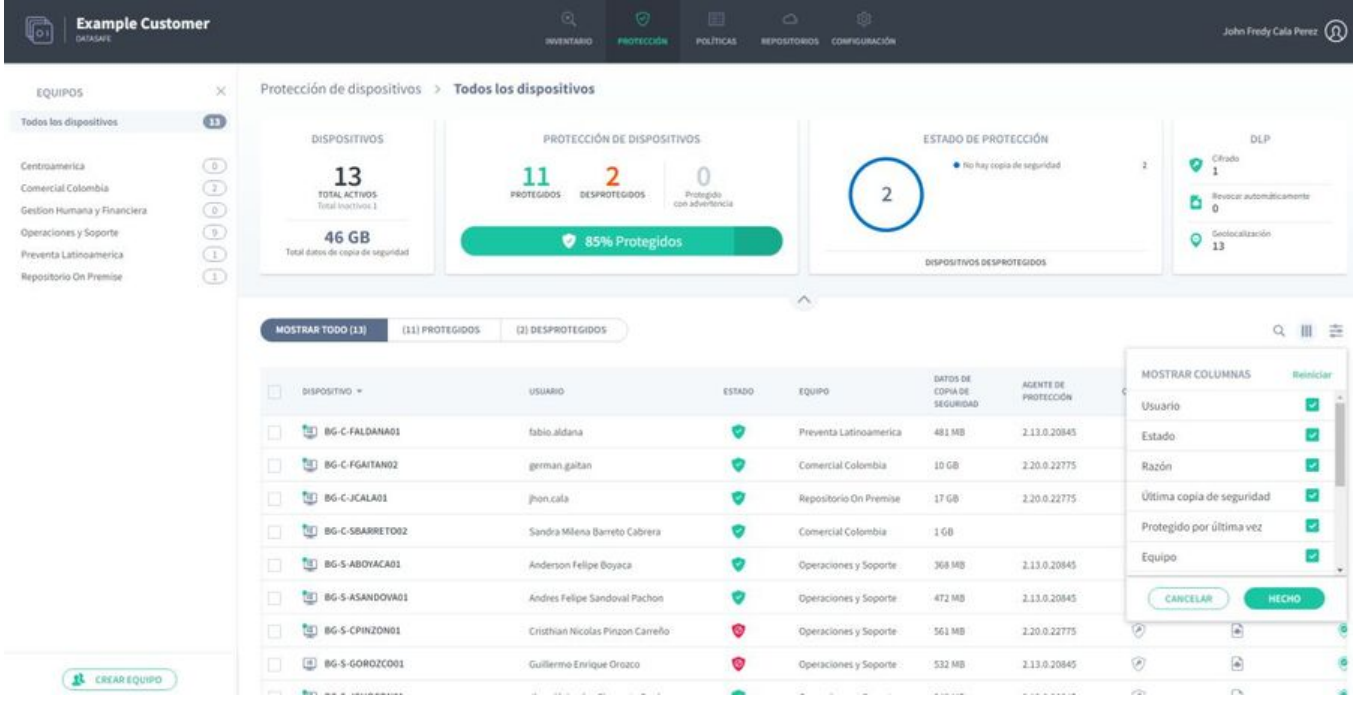
Filtrar	Descrição	Opções
Status do dispositivo	Filtre os dispositivos com base em seu status de ativação.	- Ativo - Inativo
Status Protegido	Filtre a lista para mostrar apenas dispositivos com um status de proteção específico.	- Protegido – Protegido com aviso (o dispositivo foi protegido nos últimos 5 dias, mas o backup mais recente falhou) – Desprotegido. - Offline (o Aranda Datasafe descobriu o dispositivo, mas não consegue se conectar).
DLP	Filtre dispositivos por status DLP.	- Confiável: o dispositivo foi autenticado - Revogado: o certificado de segurança do dispositivo foi removido* - Apagado: os dados protegidos do dispositivo foram excluídos. Os dispositivos geralmente são revogados ou apagados quando estão ausentes, roubados ou não foram conectados ao Aranda Datasafe dentro de um determinado período de tempo.
Repositórios	Filtre a lista para mostrar apenas os dispositivos associados a um repositório específico.	Lista de repositórios disponíveis
Políticas	Filtre a lista para mostrar apenas os dispositivos associados a uma política específica.	Lista de Políticas Disponíveis
Agente de Proteção	Filtre a lista para mostrar apenas os dispositivos que usam uma versão específica do software Protection Agent.	Lista de versões disponíveis do agente de proteção

Para remover os filtros, clique no ícone Filtro e clique em**Redefinir** (ou desmarque cada uma das caixas de filtro).

Mostrar ou ocultar colunas na lista de dispositivos

Você pode optar por mostrar ou ocultar colunas na lista de dispositivos. Por exemplo, talvez você não se importe com qual versão do agente de proteção foi usada para descobrir um dispositivo, portanto, você pode ocultá-lo da exibição.

Para mostrar/ocultar colunas, clique no ícone Colunas e escolha quais colunas incluir. Para obter uma descrição de cada coluna, consulte a página Proteção.



Descrição das políticas

Visão geral das políticas

O Aranda Datasafe precisa saber quais arquivos deseja proteger e fazer backup. Forneça essas instruções configurando uma política.

Uma política é um conjunto de regras que definem:

- Dados protegidos: quais dados são selecionados para proteção e backup.
- Opções de backup e restauração: com que frequência os backups são executados.
- DLP: se algum recurso de prevenção contra perda de dados for usado para proteger seus dados em caso de perda ou roubo de um dispositivo. Isso inclui criptografia local, prevenção de roubo de dados e geolocalização.
- Migração: se as configurações de perfil de usuário do Windows podem ser copiadas para migração para outros dispositivos.

Você pode criar quantas políticas precisar. Você pode ter uma Política para todos ou pode ter Políticas diferentes para cada departamento da sua organização.

Para exibir, criar e editar políticas, você usará oPágina de política e o Página do Editor de Políticas.

Políticas

A página Políticas fornece acesso às Políticas no Aranda Datasafe. Você pode usá-lo para:

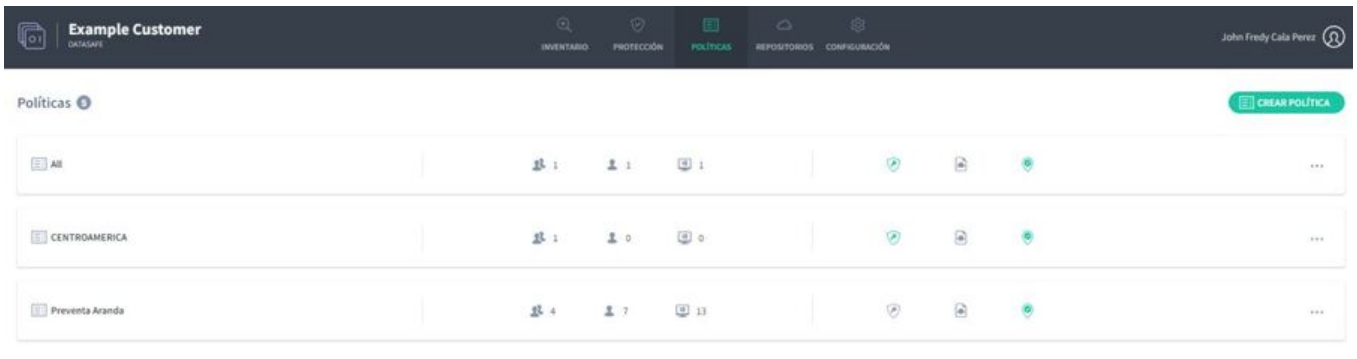
- Exibir uma lista de políticas
- Exibir ou editar uma política
- Criar uma política
- Excluir uma política

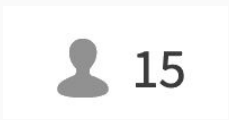
Clique em **Políticas** para exibir a página Políticas.

Lista de políticas

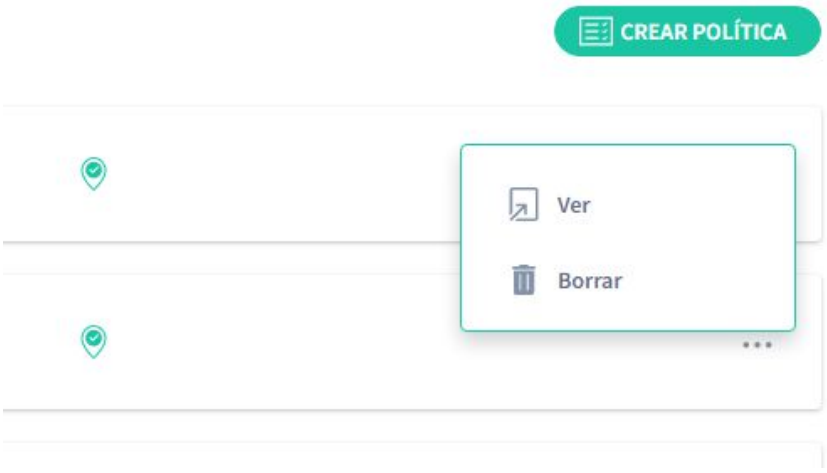
Quando você exibe a página Políticas, ela apresenta uma lista das Políticas que estão atualmente no Aranda Datasafe.

O nome da Política é mostrado à esquerda e há vários ícones.



Ícone	Descrição
	Número de equipes que usam a política.
	Número de contas de usuário associadas à política.
	Número de dispositivos associados à política.
	O status da função de criptografia (verde = criptografia local ativada, cinza = criptografia local desativada)
	O status da função de revogação automática (verde = ligado, cinza = desligado).
	O status da função de geolocalização (verde = ligado, cinza = desligado).

No lado direito da linha, há um menu de contexto (...). Se você clicar nele, poderá optar por visualizar a política ou excluí-la.



Exibir ou editar uma política

Para exibir ou editar uma política, clique no nome da política ou use a opção Exibir no menu de contexto.

Quando você exibe ou edita uma política, seus detalhes são exibidos na página do editor de políticas.

Editor de Políticas

Use a página do editor de políticas para exibir e editar várias configurações de uma política, incluindo:

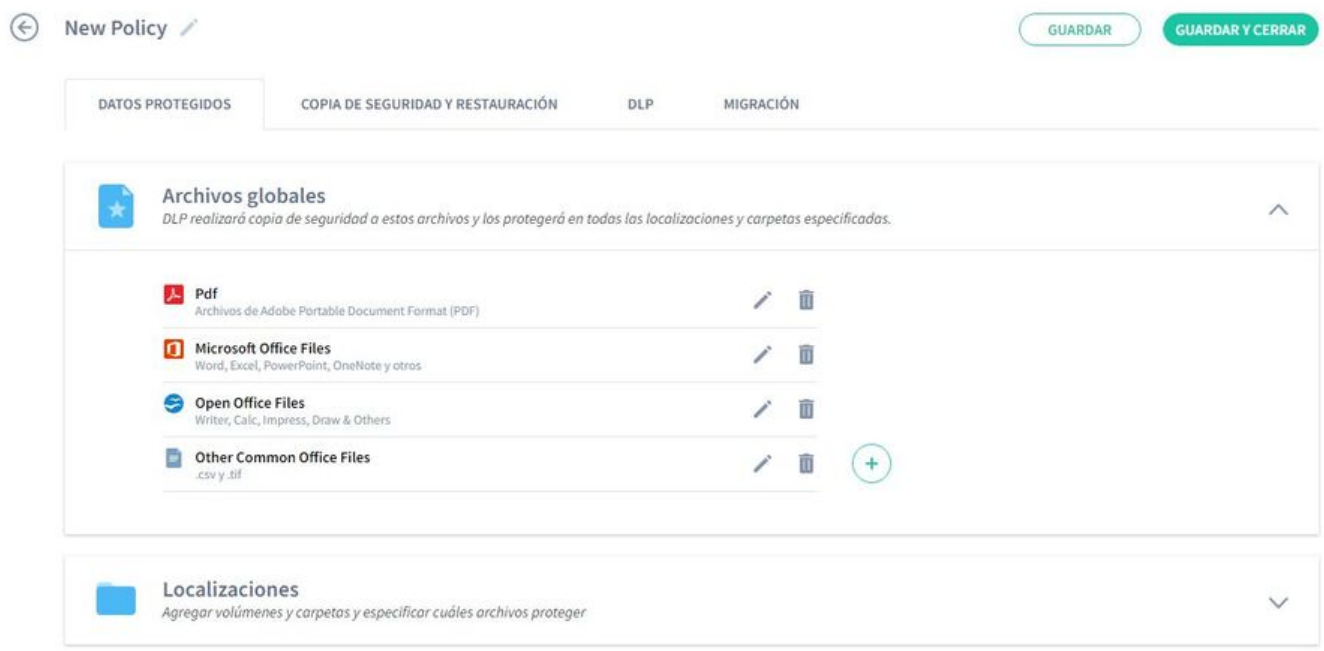
- Que tipos de dados são copiados e protegidos
- Quais locais são protegidos e suportados
- Qual e-mail é protegido e copiado
- Quais dados não são protegidos ou armazenados em backup
- Quando os backups automáticos serão realizados
- Quais recursos de prevenção contra perda de dados são usados
- Quais recursos de migração de dados são usados.

Para exibir a página do editor de políticas, clique em**Políticas**.

- Dados protegidos
- Restaurar backup
- DLP (Prevenção de Perda de Dados) -Migração.

Dados protegidos

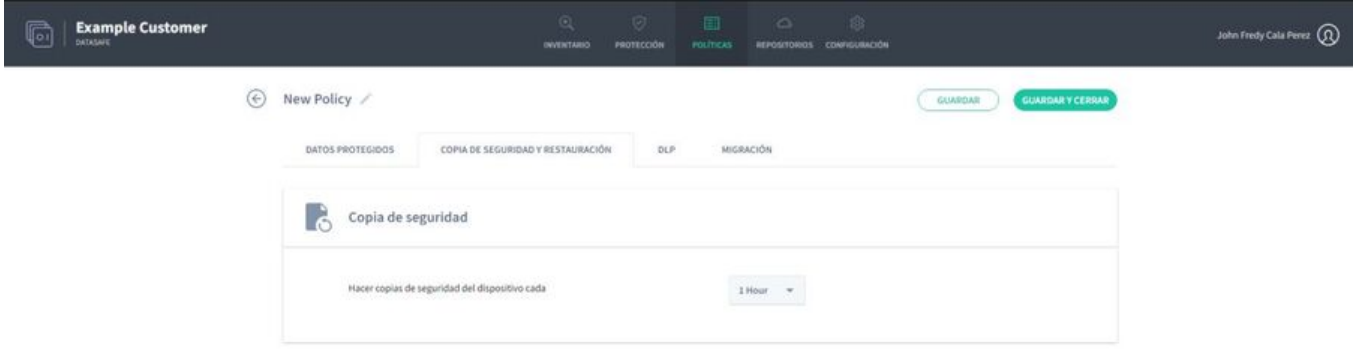
Use as configurações de Dados Protegidos para escolher quais tipos e locais de arquivo serão copiados ou excluídos de seus backups.



Configurações	Descrição	Ver artigo
Arquivos Globais	Arquivos globais são grupos de tipos de arquivos, por exemplo, há um grupo de arquivos global para arquivos do Microsoft Office. Você pode adicionar, editar ou excluir grupos de tipos de arquivos globais.	Escolha quais tipos de arquivo são "arquivos globais"
Localizações	Escolha quais volumes e pastas o Aranda Datasafe fará backup e protegerá. Para cada local, você pode escolher quais arquivos serão copiados (todos, globais e personalizados	Escolher quais locais são protegidos
Unidades de nuvem	Escolha quais unidades de nuvem o Aranda Datasafe fará backup e protegerá. Para cada unidade de nuvem, você pode escolher quais arquivos serão copiados (todos, globais e personalizados).	Escolher quais unidades de nuvem estão protegidas
E-mails	Escolha quais arquivos de e-mail o Aranda Datasafe fará backup e protegerá.	Backup e proteção de e-mail
Exclusões Globais	Use-o para definir qualquer tipo de arquivo ou local que o Aranda Datasafe não deva fazer backup ou proteger.	Excluir arquivos e pastas do backup e da proteção

Backup e restauração

Use as configurações de Backup e restauração para agendar backups automáticos.



Você pode optar por executar backups a cada:

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

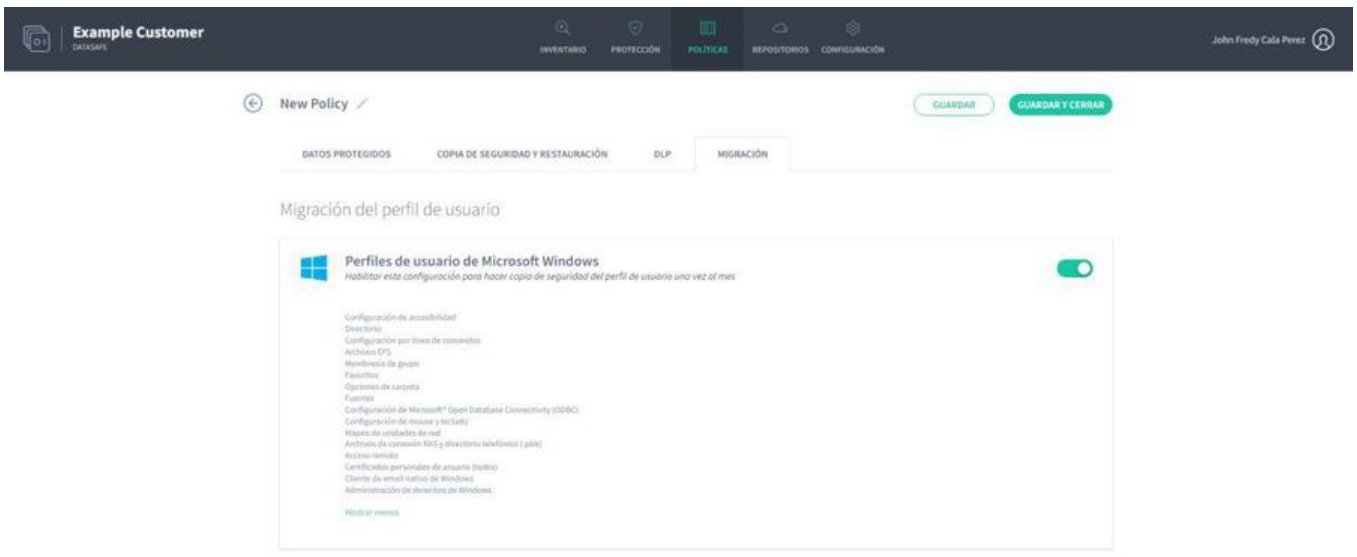
DLP (Prevenção de Perda de Dados)

Use as configurações de DLP para escolher quais recursos de prevenção contra perda de dados você deseja que a Política use.

Configurações	Descrição	Ver artigo
Criptografia	Você pode ativar a criptografia local para criptografar dados em cada dispositivo. Usuários não autorizados não poderão visualizar os arquivos criptografados.	Ativar criptografia local
Prevenção de roubo de informações	<p>Se um dispositivo não se conectar ao Aranda Datasafe dentro de um determinado período de tempo, o Aranda Datasafe poderá revogar o acesso aos arquivos no dispositivo. Enquanto revogado, o usuário não pode acessar os dados protegidos. Use a Prevenção contra roubo de dados para ativar ou desativar esse recurso.	Habilite a prevenção contra roubo de dados.
Geolocalização	Você pode ativar a geolocalização para dispositivos. Se você ativar a geolocalização, poderá usar o Aranda Datasafe para visualizar um mapa da última localização conhecida de um dispositivo.	Ativar geolocalização

Migração

Usar configurações de migração para habilitar ou desabilitar a migração de configurações de perfil de usuário para uma política



O recurso Migração de Perfil de Usuário foi projetado para ser usado quando você estiver substituindo um dispositivo. Em vez de configurar seu novo dispositivo do zero, você pode usar a Restauração para carregá-lo com o perfil de usuário e as configurações de outro dispositivo.

Criar políticas

Uma política é um conjunto de regras que definem:

- Quais dados são protegidos e armazenados em backup
- Com que frequência os backups ocorrem
- Se algum recurso de prevenção contra perda de dados for usado para proteger seus dados em caso de perda ou roubo de um dispositivo
- Se for feito backup das informações de configuração do perfil do Windows.

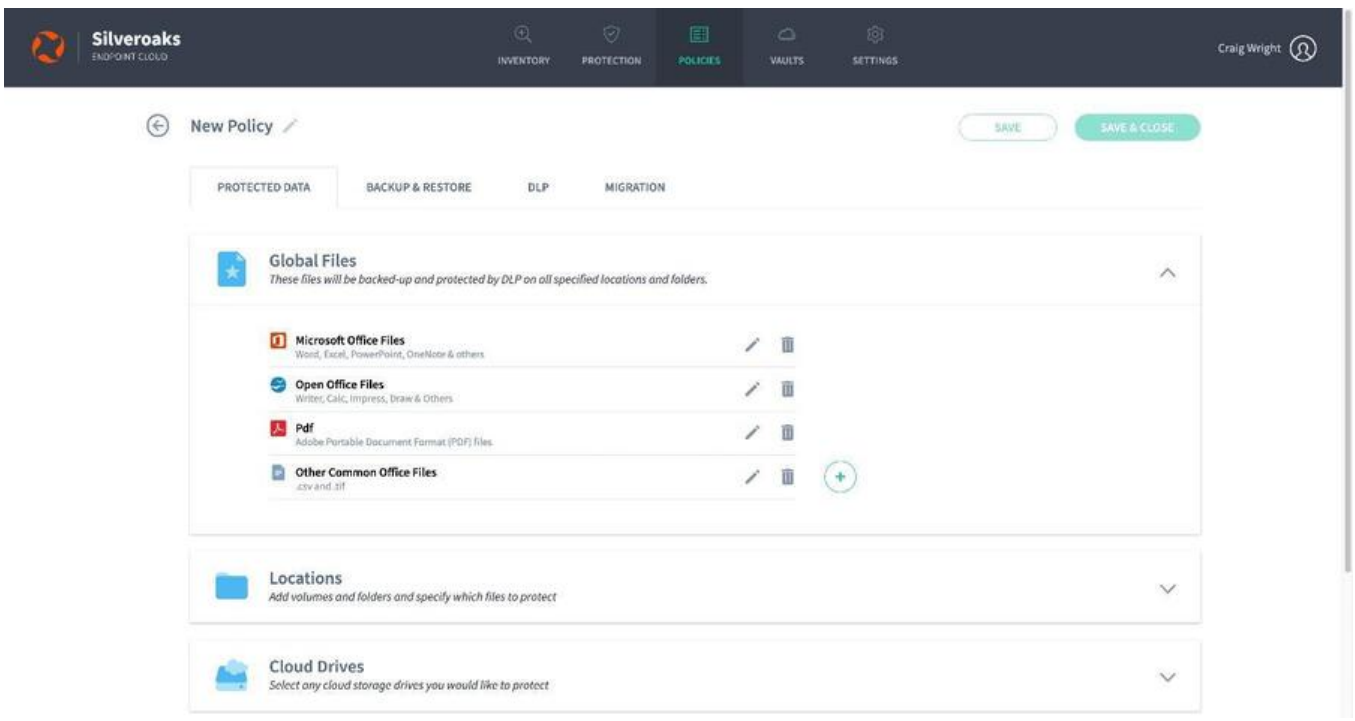
Você pode criar quantas políticas precisar. Você pode ter uma Política para todos ou pode ter Políticas diferentes para cada equipe.

Para criar uma nova política:

1. Clique em **Políticas**.

Se você não tiver nenhuma política no Aranda Datasafe, clique em **Adicionar uma política**. Se você já tiver algumas políticas, clique em **Criar Política**.

O Aranda Datasafe cria uma nova Política e a abre, pronta para você definir sua configuração.



2. Dê um nome à Política. Clique no ícone de edição ao lado do nome padrão e insira o novo nome.

Sua nova política tem configurações padrão, e muitos administradores do Aranda Datasafe consideram essas configurações adequadas às suas necessidades. Se você tiver requisitos diferentes, poderá alterar as configurações nas seguintes seções:

- **Dados protegidos**: Usado para definir quais dados são criptografados e copiados.
- Backup e restauração: usado para escolher a frequência com que os backups são feitos.
- **DLP**: usado para escolher medidas de prevenção contra perda de dados para a política.
- **Migração**: Usado para escolher se deseja fazer backup das configurações relacionadas aos perfis de usuário do Windows.

Editar políticas

Se você quiser fazer alterações em uma política existente:

1. Clique em **Políticas**.

2. Clique na Política que deseja alterar.

O Aranda Datasafe abre a página do editor de políticas, que você pode usar para alterar as configurações de políticas.

Você pode alterar as configurações nas seguintes seções:

- **Dados protegidos**: Usado para definir quais dados são criptografados e copiados.
- Backup e restauração: usado para escolher a frequência com que os backups são feitos.
- **DLP**: usado para escolher medidas de prevenção contra perda de dados para a política.
- **Migração**: Usado para escolher se deseja fazer backup das configurações relacionadas aos perfis de usuário do Windows.

Excluir políticas

Se você não precisar mais de uma política ou tiver criado uma política por engano, poderá excluí-la.

Cuidado: se você excluir uma política associada a computadores e dispositivos, esses computadores e dispositivos não terão mais uma política atribuída a eles. Isso significa que eles não serão copiados automaticamente e outros recursos, como geolocalização, não estarão disponíveis.

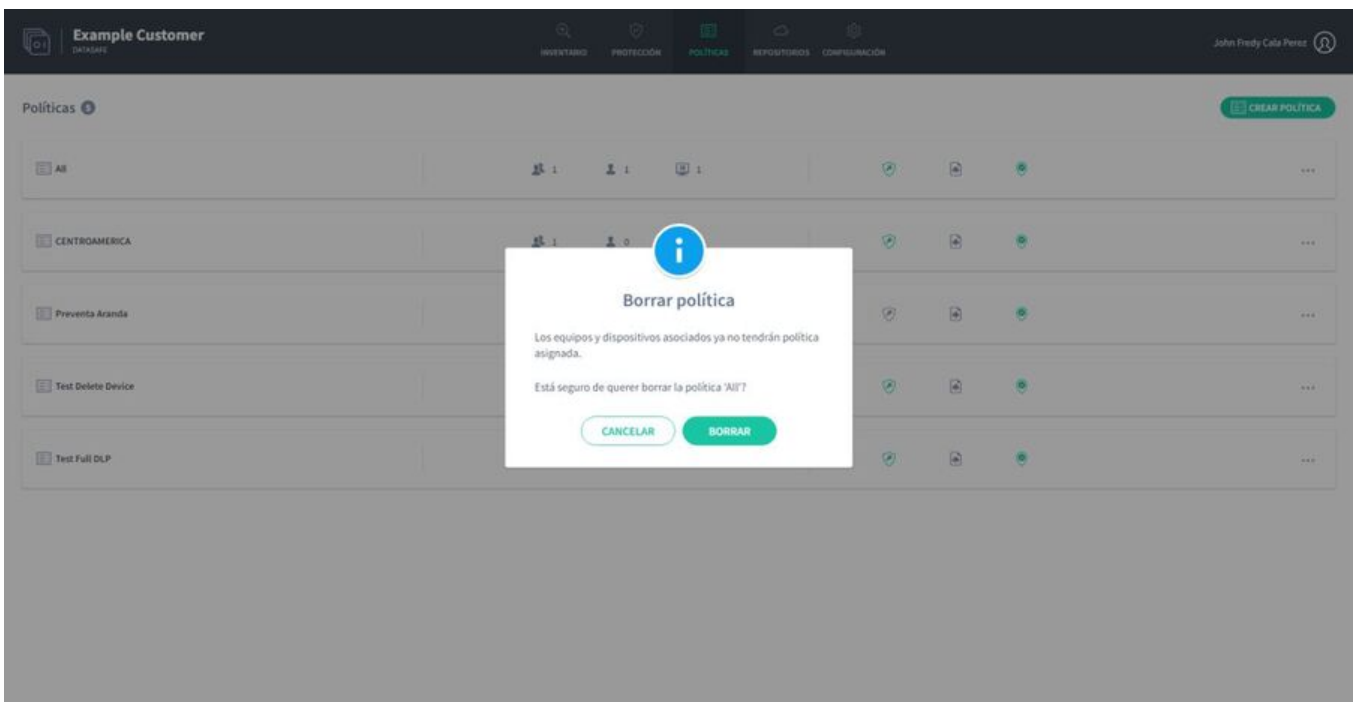
Para excluir uma política:

1. Clique em Políticas para exibir a página Políticas . 2. Na lista Políticas, localize a política que deseja excluir.

3. Clique no botão de opção (...) da Política.

4. Clique em Excluir.

5. Quando solicitado, clique em Excluir para confirmar.



Arquivos Globais

Você pode usar o recurso **Arquivos Globais** para criar coleções de tipos de arquivo. Isso torna muito mais rápido escolher quais arquivos são copiados, porque em vez de ter que escolher cada tipo de arquivo separadamente para cada local, você pode escolher uma coleção de arquivos globais.

Por exemplo, por padrão, cada política tem uma coleção de arquivos do Microsoft Office de arquivos globais. Esta coleção inclui arquivos salvos no Word, Excel, PowerPoint, etc. Ao escolher quais tipos de arquivo devem ser copiados, você pode escolher a coleção Arquivos Globais em vez de ter que selecionar cada tipo de arquivo do MS Office separadamente.

Você pode usar a configuração Arquivos Globais em uma política para:

- Adicionar ou remover tipos de arquivo das diferentes coleções de arquivos globais
- Crie uma nova coleção para diferentes tipos de arquivo. Por exemplo, talvez você queira criar uma nova coleção que contenha os tipos de arquivo para seu software proprietário.

Alterar uma coleção existente de arquivos globais

Para fazer alterações em uma coleção existente de arquivos globais:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Certifique-se de que a guia **Dados protegidos** seja exibida.

3. Na lista de **Arquivos Globais**, encontre a coleção de Arquivos Globais que deseja alterar e clique no ícone Editar (lápis).

4. Use o campo **Editar nome do tipo de arquivo** para renomear a coleção de arquivos global, se necessário.

5. Use a caixa **Adicionar ou remover extensões** para adicionar ou remover extensões de arquivo.

Para adicionar uma extensão de arquivo, clique em uma parte vazia da caixa e insira os caracteres da extensão de arquivo. Pressione Enter e um bloco azul aparecerá para o novo tipo de extensão. Clique em **Salvar alterações** para confirmar.

Para remover um tipo de extensão de arquivo, clique no X no bloco azul correspondente. Clique em **Salvar alterações** para confirmar.

Adicionar uma nova coleção de arquivos global

Para adicionar uma nova coleção de arquivos global:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e, em seguida, clique em **Política**).

2. Certifique-se de que a guia **Dados protegidos** seja exibida.

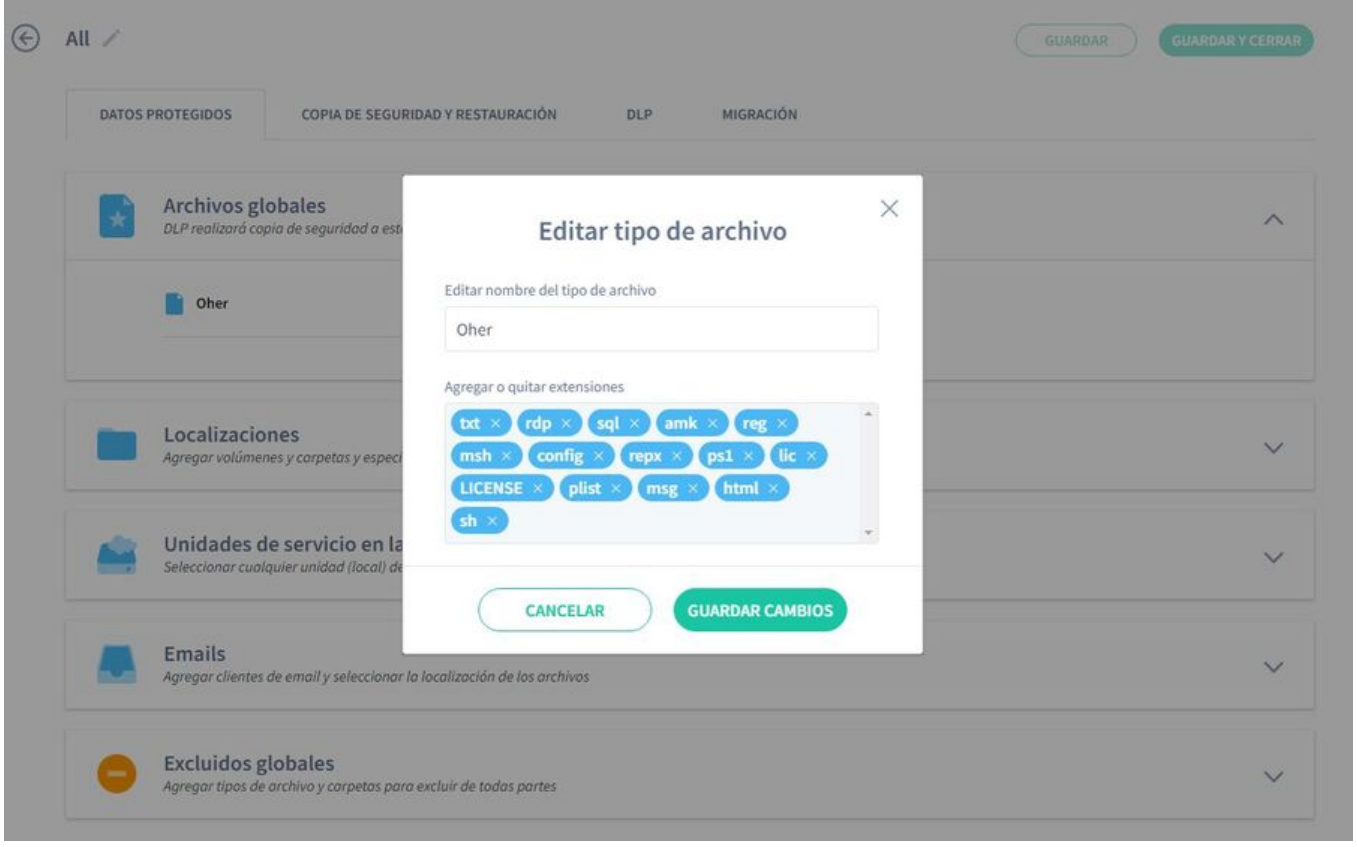
3. Na seção Arquivos globais da guia **Dados protegidos**, clique no ícone de adição (+) para exibir a caixa de diálogo Adicionar tipo de arquivo.

4. Use a opção **Selecionar um tipo de arquivo** para definir o nome da sua nova coleção global de arquivos. Você pode escolher na lista de tipos de arquivo disponíveis ou selecionar Adicionar novo tipo de arquivo.

5. Se você selecionou **Adicionar novo tipo de arquivo** na etapa 2, insira o nome da nova coleção de arquivos global no campo **Editar nome do tipo de arquivo**. Se você escolher um tipo de arquivo existente, poderá editar o nome ou deixá-lo como está.

6. Use a caixa **Adicionar ou remover extensões** para adicionar ou remover extensões de arquivo da nova coleção global de arquivos. Isso funciona da mesma maneira que ao editar uma coleção de arquivos globais (veja acima).

7. Clique em **Salvar alterações**.



Excluir uma coleção de arquivos globais

Para excluir uma coleção de Arquivos Globais do Aranda Datasafe:

1.Abra o Editor de Políticas para a Política que deseja alterar (clique em**Políticas** e, em seguida, clique em Política).

2. Certifique-se de que a guia**Dados protegidos** seja exibida.

3.In lista de**Arquivos Globais**, encontre a coleção de Arquivos Globais que deseja excluir e clique no ícone da lixeira.

Locais protegidos

Você pode configurar o Aranda Datasafe para fazer backup e proteger arquivos em locais específicos em um computador (somente unidades locais, por padrão). Alguns locais comuns são incluídos por padrão, incluindo Todos os Volumes, Área de Trabalho e Documentos, e você pode adicionar outros locais, se necessário.

Para escolher os locais a serem protegidos, use a configuração**Locais** em uma Política. Para cada local, você pode escolher quais arquivos são copiados e protegidos:

- Todos os arquivos
- somente arquivos globais
- arquivos que você escolhe manualmente.

Você pode usar a seção Locais para:

Adicionar um local.

Editar um local.

Excluir um local.

Adicionar local

1. Abra o Editor de políticas da política que deseja alterar (clique em Políticas e, em seguida, clique em Política).

2. Na guia**Dados protegidos**, expanda as configurações de**Locais**.

3. Clique no ícone de adição (+) para exibir um menu de contexto. O menu de contexto tem opções para alguns locais comumente protegidos, incluindo Downloads e Vídeos. Para adicionar seu próprio local, clique em **Adicionar novo local**.

4. Insira um nome de local significativo para que outras pessoas entendam onde fica esse local.

5. No campo **Caminho**, insira o local da pasta dos arquivos que deseja proteger.

6. Se você deseja incluir várias pastas, clique no ícone de adição (+) para **Adicionar outro caminho**. Isso cria outro campo de caminho.

7. Clique em **Salvar alterações** para confirmar.

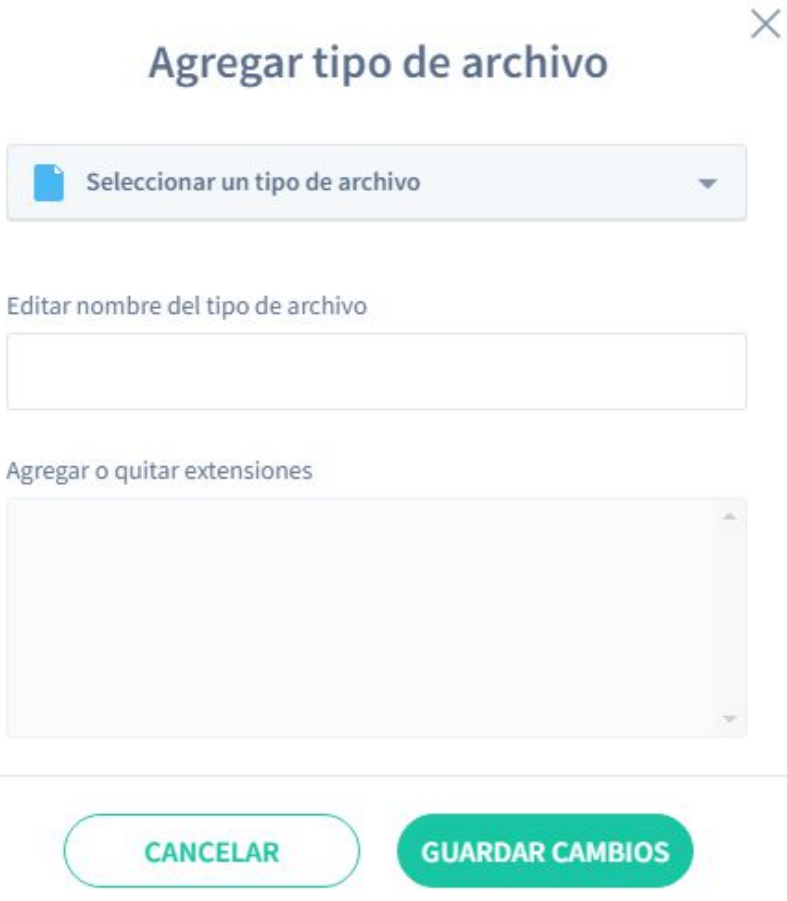
8. Escolha se deseja proteger **Todos os arquivos**.

Se você ativar esse recurso, todos os arquivos no local serão protegidos, com exceção de qualquer tipo de arquivo excluído (exclusão de arquivo global ou exclusão de seleção de arquivo personalizado). Se você desativá-lo, poderá escolher quais arquivos proteger.

9. Escolha se deseja proteger as **fontes globais** para este local. Se você habilitar esse recurso, todos os tipos globais serão copiados e protegidos. Se você desativá-lo, os tipos de arquivo globais não serão incluídos (a menos que você os adicione como seções de arquivo personalizadas na próxima etapa).

10. . Use a Seleção de arquivo personalizada para incluir ou excluir qualquer tipo de arquivo específico para esse local. Se você habilitar esse recurso, poderá usar a seção Inclui e Excluir (consulte as etapas abaixo). Por exemplo, você pode optar por incluir uma coleção de arquivos globais em vez de todos os tipos de arquivos globais.

Na seção **Inclui**, clique em **Adicionar tipo de arquivo**.



11. Use a caixa de diálogo Adicionar tipo de arquivo para escolher os tipos de arquivo que deseja proteger para esse local. Você pode escolher qualquer uma de suas coleções de arquivos globais e, em seguida, **Adicionar ou Remover Extensões** para especificar quais tipos de arquivo serão copiados.

Como alternativa, você pode clicar em **Adicionar novo tipo de arquivo** para criar sua própria seleção personalizada (digite o nome no campo **Editar nome do tipo de arquivo** e use **Adicionar ou remover extensões** para escolher os tipos de arquivo). Clique em **Salvar alterações** para confirmar.

12. Na seção Exclusões, use **Adicionar tipo de arquivo** a Excluir para escolher qualquer tipo de arquivo que não deva ser protegido para este local. Por exemplo, se você deseja que o Aranda Datasafe proteja todos os arquivos globais, exceto PDFs, a maneira mais rápida é habilitar os Arquivos Globais para o local e, em seguida, excluir PDFs.

Use a caixa de diálogo Adicionar Tipo de Arquivo para escolher os tipos de arquivo que você não deseja que sejam protegidos para esse local.

Você pode escolher qualquer uma de suas coleções de arquivos globais e, em seguida, adicionar ou remover extensões para especificar quais tipos de arquivo excluir. Como alternativa, você pode adicionar uma nova extensão de arquivo para excluí-lo. Clique em Salvar alterações para confirmar.

13. Na seção **Exclusões**, use **Adicionar uma pasta a ser excluída** para escolher pastas específicas que não devem ser protegidas para este local. Clique em Adicionar uma pasta a ser excluída para exibir um menu de contexto. Você pode escolher Pastas do sistema, Pastas temporárias ou Adicionar uma nova pasta. Se você adicionar uma nova pasta, a caixa de diálogo Adicionar pasta será exibida e você poderá definir o nome e os caminhos da pasta.

Clique em Salvar alterações para confirmar que as pastas não serão protegidas.

14. Clique em **Salvar alteração**.

edit location

Para fazer alterações em um local existente:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Na guia **Dados protegidos**, expanda as configurações de **Locais**.

3. Clique no ícone Editar (lápis) para o local que deseja alterar.

4. Use as configurações de **Todos os arquivos, Arquivos globais e Seleção de arquivo personalizado** para fazer as alterações. Eles funcionam da mesma maneira que quando você adiciona um local (veja acima).

5. Clique em **Salvar alterações**.

excluir local

Para remover um local de uma política:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. **Na guia Dados protegidos, expanda as configurações de locais**

3. Clique no ícone da lixeira do local que deseja excluir.

Unidades de nuvem protegidas

Você pode configurar o Aranda Datasafe para fazer backup e proteger arquivos em serviços de armazenamento em nuvem, como One Drive, Google Drive e Dropbox.

Para escolher quais serviços de nuvem proteger, use a configuração **Cloud Drives** em uma Política. Para cada unidade de nuvem, você pode escolher quais arquivos são copiados e protegidos:

- Todos os arquivos
- somente arquivos globais
- arquivos que você escolhe manualmente.

Adicionar uma unidade de nuvem

Para adicionar uma unidade de nuvem a uma política para que ela seja protegida:

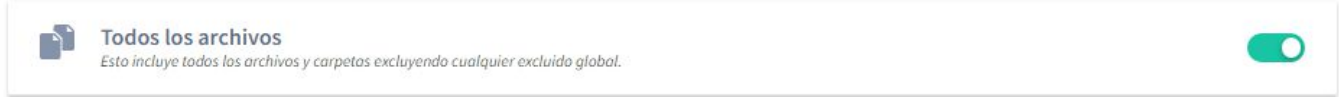
1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Na guia **Dados protegidos**, expanda as configurações de **Cloud Drives**.

3. Clique no ícone de adição (+) para exibir um menu de contexto.

4. Escolha a unidade de nuvem que deseja adicionar, por exemplo, One Drive.

5. Escolha se deseja proteger **Todos os arquivos**.

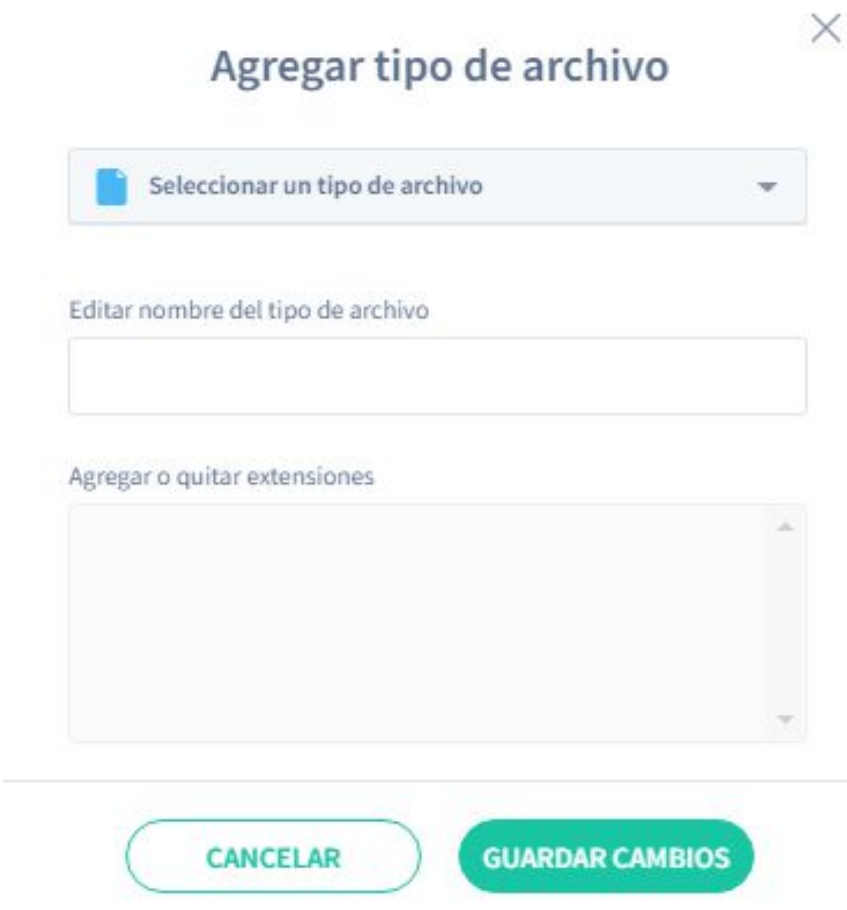


Se você habilitar esse recurso, todos os arquivos na unidade de nuvem serão protegidos, com exceção de qualquer tipo de arquivo excluído (exclusão de arquivo global ou exclusão de seleção de arquivo personalizado). Se você desativá-lo, poderá escolher quais arquivos proteger.

6. Escolha se deseja que os**arquivos globais** sejam protegidos para esta unidade de nuvem. Se você habilitar esse recurso, todos os tipos globais serão copiados e protegidos. Se você desativá-lo, os tipos de arquivo globais não serão incluídos (a menos que você os adicione como seções de arquivo personalizadas na próxima etapa).

7. Use a seleção de**arquivos personalizados** para incluir ou excluir qualquer tipo de arquivo específico para esta unidade de nuvem. Se você habilitar esse recurso, poderá usar a seção **Inclusões e Exclusões** (consulte as próximas etapas). Por exemplo, você pode optar por incluir uma coleção de arquivos globais em vez de todos os tipos de arquivos globais.

8. Na seção **Inclusões**, clique em **Adicionar tipo de arquivo**.



Use a caixa de diálogo Adicionar tipo de arquivo para escolher os tipos de arquivo que deseja proteger para esta unidade de nuvem. Você pode escolher qualquer uma de suas coleções de arquivos globais e, em seguida, **Adicionar ou Remover Extensões** para especificar quais tipos de arquivo serão copiados.

Como alternativa, você pode clicar em **Adicionar novo tipo de arquivo** para criar sua própria seleção personalizada (digite o nome no campo **Editar nome do tipo de arquivo** e use **Adicionar ou remover extensões** para escolher os tipos de arquivo). Clique em **Salvar alterações** para confirmar.

9. Na seção **Exclusões**, use **Adicionar tipo de arquivo** a Excluir para escolher qualquer tipo de arquivo que não deva ser protegido para esta unidade de nuvem. Por exemplo, se você deseja que o Aranda Datasafe proteja todos os arquivos globais, exceto PDFs, a maneira mais rápida é habilitar os Arquivos Globais para a unidade de nuvem e, em seguida, excluir PDFs.

Use a caixa de diálogo **Adicionar Tipo de Arquivo** para escolher os tipos de arquivo que você não deseja que sejam protegidos para esta unidade de nuvem.

Você pode escolher qualquer uma de suas coleções de arquivos globais e, em seguida, adicionar ou remover extensões para especificar quais tipos de arquivo excluir. Como alternativa, você pode adicionar uma nova extensão de arquivo para excluí-lo. Clique em **Salvar alterações** para confirmar.

10. Na seção **Exclusões**, use **Adicionar uma pasta** para excluir para escolher pastas específicas que não devem ser protegidas para esta unidade de nuvem. Clique em Adicionar uma pasta a ser excluída para exibir um menu de contexto. Você pode escolher Pastas do sistema, Pastas temporárias ou Adicionar uma nova pasta. Se você adicionar uma nova pasta, a caixa de diálogo Adicionar pasta será exibida e você poderá definir o nome e os caminhos da pasta.

Clique em **Salvar alterações** para confirmar que as pastas não serão protegidas

Edite uma unidade de nuvem

Para fazer alterações em uma unidade de nuvem existente:

1. . Abra o Editor de Políticas da Política que você deseja alterar (clique em **Políticas** e clique em Política).

2. Na guia **Dados protegidos**, expanda as configurações de **Cloud Drives**.

3. Clique no ícone Editar (lápis) da unidade de nuvem que deseja alterar.

4. Use as configurações de **Todos os arquivos, Arquivos globais e Seleção de arquivo personalizado** para fazer as alterações. Eles funcionam da mesma maneira que quando você adiciona uma unidade de nuvem (veja acima).

5. Clique em **Concluído**.

Excluir uma unidade de nuvem

Para remover uma unidade de nuvem de uma política:

1. Encontre a política que deseja alterar no Editor de políticas (clique em **Políticas** e depois em Política).

2. Na guia **Dados protegidos**, expanda as configurações de **Cloud Drives**.

3. Clique no ícone da lixeira da unidade de nuvem que deseja excluir.

Proteção e backup de e-mail

Você pode configurar o Aranda Datasafe para fazer backup e proteger seus arquivos de cliente de e-mail. Por exemplo, você pode adicionar o Microsoft Outlook como um cliente de e-mail e, em seguida, configurar o Aranda Datasafe para fazer backup e proteger todos os arquivos PST do Outlook ou apenas os arquivos PST ativos.

As configurações de email estão na política usada para fazer backup do seu dispositivo.

Adicione um cliente de e-mail para backup

Para adicionar um cliente de e-mail:

1. Abra o Editor de políticas da política que deseja alterar (clique em Políticas e, em seguida, clique em Política).

⚐ > Observação: o editor de políticas é exibido automaticamente quando você cria uma nova política.

2. Certifique-se de que a guia **Dados protegidos** seja exibida.

3. Expanda a seção **E-mails**.

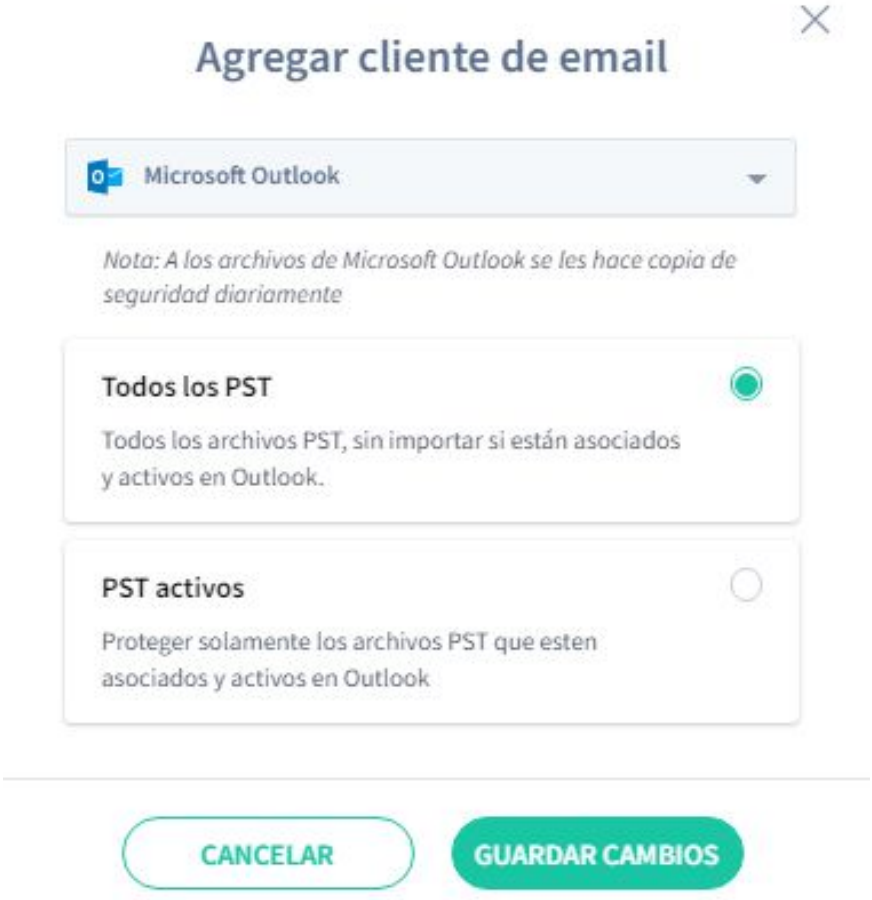
4. Clique no ícone de adição (+).

5. Selecione o cliente de e-mail, por exemplo, Microsoft Outlook.

6. Escolha quais arquivos PST você deseja fazer backup:

- Todos os arquivos PST: O Aranda Datasafe fará backup de todos os arquivos PST, mesmo que estejam inativos ou não associados ao cliente de e-mail.
- PST ativo: O Aranda Datasafe fará backup apenas de arquivos PST associados ao cliente de e-mail e atualmente ativos no perfil do Outlook.

7. Clique em **Salvar alterações**.



Edite um cliente de e-mail

Para fazer alterações em um cliente de e-mail existente:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Certifique-se de que a guia **Dados protegidos** seja exibida.

3. Expanda a seção **E-mails**.

4. Clique no ícone Editar (lápis) do cliente de e-mail que deseja alterar.

5. Use a caixa de diálogo Editar cliente de e-mail para escolher quais arquivos serão copiados:

- **Todos os arquivos PST**: O Aranda Datasafe fará backup de todos os arquivos PST, mesmo que estejam inativos ou não associados ao cliente de e-mail.
- **PST ativo**: O Aranda Datasafe fará backup apenas dos arquivos PST associados ao cliente de e-mail e que estão ativos no momento.

6. Clique em **Salvar alterações**.

Excluir um cliente de e-mail

Para excluir um cliente de e-mail:

1. Abra o Editor de políticas da política que deseja alterar (clique em Políticas e, em seguida, clique em Política).

2. Certifique-se de que a guia Dados protegidos seja exibida.

3. Expanda a seção E-mails.

4. Clique no ícone Lixeira do cliente de e-mail que deseja excluir.

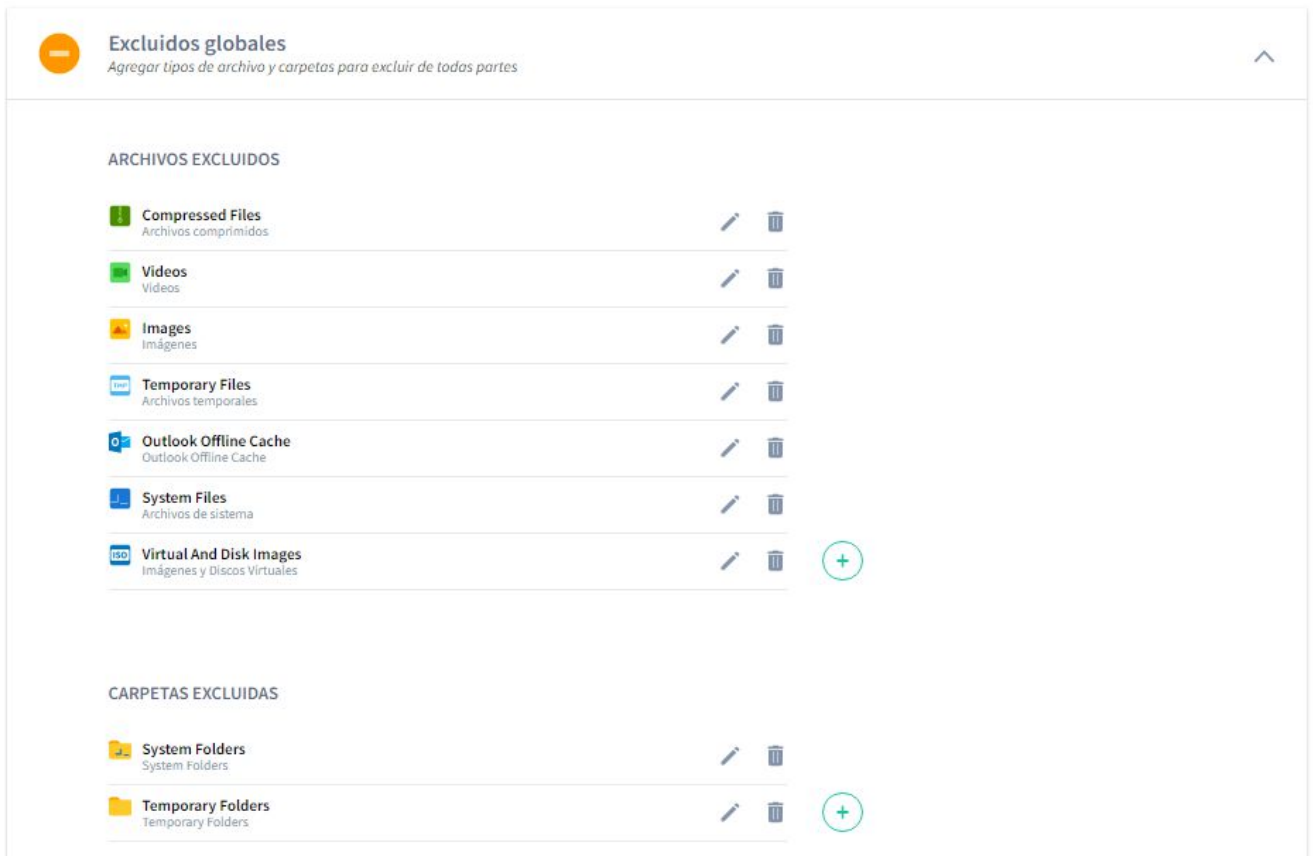
Excluir arquivos e pastas do backup e da proteção

Você pode querer excluir certos tipos de arquivos do backup e proteção do Aranda Datasafe. Por exemplo, você pode excluir arquivos de imagem, vídeos e músicas. Você também pode excluir determinadas pastas.

Há duas maneiras de excluir arquivos e pastas:

- Você pode excluir para um local específico
- Você pode excluir para todos os locais.

Neste artigo, explicamos como usar o recurso Exclusões Globais para excluir arquivos e pastas de todos os locais. O recurso Exclusões Globais é útil quando você sabe que há determinados tipos de arquivo que você nunca deseja que sejam protegidos em um único local. Permite criar um grupo de tipos de arquivo que você pode excluir para todos os locais em uma única ação.



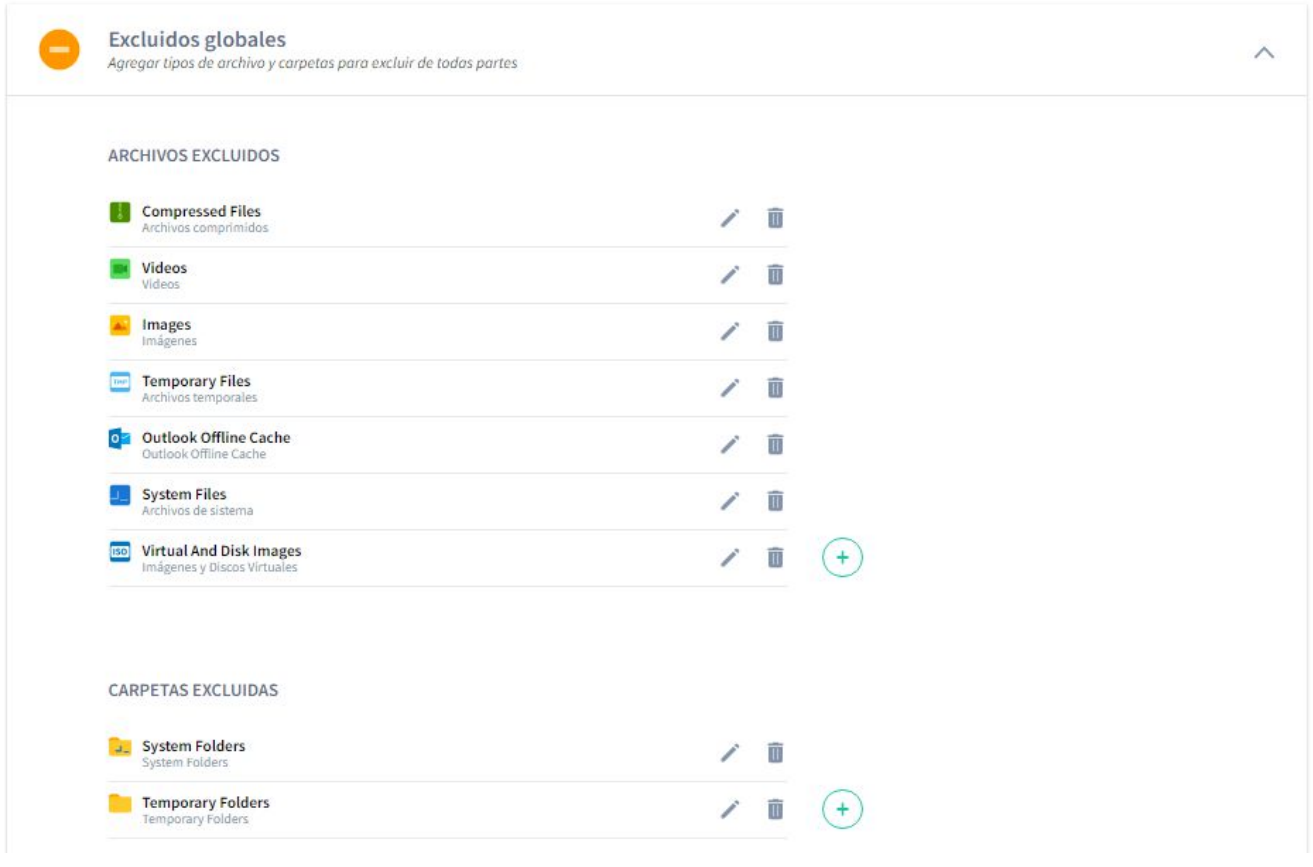
Para saber como excluir arquivos de um local específico, consulte [Escolher quais arquivos e pastas] estão protegidos.

Excluir arquivos da proteção para todos os locais

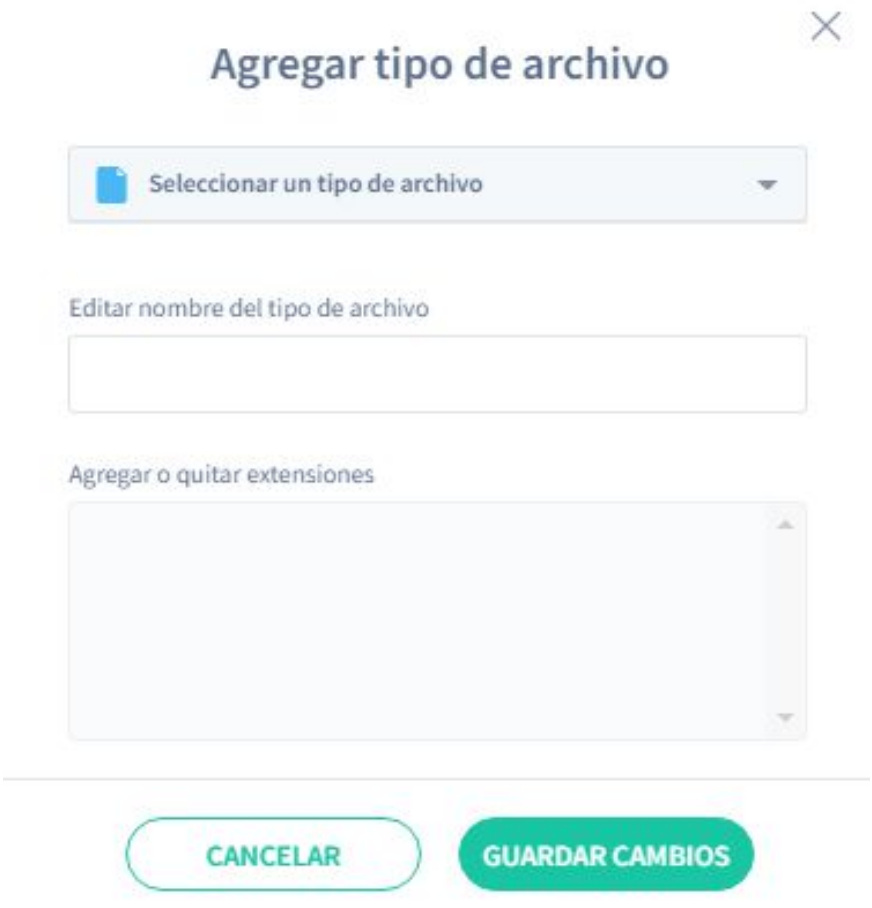
Para impedir que determinados tipos de arquivo sejam copiados e protegidos para todos os locais:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Na guia **Dados protegidos**, expanda as configurações de **Exclusão global**.



3. Na seção Arquivos excluídos, clique no ícone de adição (+) para exibir a caixa de diálogo Adicionar tipo de arquivo.



4. Use a opção **Selecione um tipo de arquivo** para definir o nome do seu novo grupo de arquivos global. Você pode escolher na lista de tipos de arquivo disponíveis ou pode selecionar **Adicionar novo tipo de arquivo**.

5. Se você selecionou **Adicionar novo tipo de arquivo** na etapa 4, insira o nome do novo grupo Arquivos globais no campo **Editar nome do tipo de arquivo**. Se você escolher um tipo de arquivo existente, poderá editar o nome ou deixá-lo como está.

6. Use a caixa **Adicionar ou remover extensões** para adicionar ou remover extensões de arquivo do novo grupo Arquivos globais. As extensões de arquivo que você adicionar à caixa serão excluídas; O Aranda Datasafe não protegerá esses tipos de arquivo para dispositivos que usam esta Política.

7. Clique em **Salvar alterações**.

Editar regras globais de exclusão de arquivos

Para alterar os arquivos incluídos nas exclusões globais:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Certifique-se de que a guia **Dados protegidos** seja exibida.

3. Na lista de **exclusões globais**, encontre o grupo que deseja alterar e clique no ícone **Editar** (lápis).

4. Use o campo **Editar nome do tipo de arquivo** para renomear o grupo, se necessário.

5. Use a caixa **Adicionar ou remover extensões** para adicionar ou remover extensões de arquivo.

Para adicionar uma extensão de arquivo, clique em uma parte vazia da caixa e insira os caracteres da extensão de arquivo. Pressione Enter e um bloco azul aparecerá para o novo tipo de extensão. Clique em **Salvar alterações** para confirmar.

Para remover um tipo de extensão de arquivo, clique no X no bloco azul correspondente. Clique em **Salvar alterações** para confirmar.

Excluir pastas da proteção para todos os locais

Você pode excluir pastas da proteção do Aranda Datasafe. Por exemplo, seus usuários podem ter pastas de dados pessoais onde armazenam dados não comerciais e você não deseja fazer backup dessas informações.

Para excluir pastas de todos os locais:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Certifique-se de que a guia **Dados protegidos** seja exibida.

3. Na seção **Exclusões globais**, clique no ícone de mais (+).

4. Você pode escolher Pastas do sistema ou Pastas temporárias ou clicar em Adicionar nova pasta para escolher uma pasta específica. Se você adicionar uma nova pasta, a caixa de diálogo Adicionar pasta será exibida e você poderá definir o nome e os caminhos da pasta.

5.Clique em **Salvar alterações**.

Edite as pastas excluídas

Se você tiver definido Pastas Excluídas em Exclusões Globais para uma política, poderá editá-las para:

- Renomeie a pasta
- Alterar o caminho
- Adicione rotas adicionais.

Para editar pastas de exclusão global:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Certifique-se de que a guia **Dados protegidos** seja exibida.

3. Na seção **Exclusões globais**, clique no ícone Editar (lápis) do grupo de exclusão global que deseja alterar.

4. Use o campo **Nome da pasta** para alterar o nome do grupo.

5.Use os campos **Caminho** para alterar os locais das pastas.

6.Clique em **Salvar alterações**.

Remover arquivos ou pastas das exclusões globais

Para remover arquivos ou pastas das exclusões globais de uma política:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Certifique-se de que a guia **Dados protegidos** seja exibida.

3.In seção Exclusões globais, clique no ícone da lixeira do grupo ou pasta de exclusão global que deseja excluir.

Quando você exclui um grupo de arquivos ou pastas de exclusões globais em uma política, eles não são mais excluídos da proteção do Aranda Datasafe. (A menos que eles também sejam excluídos nas configurações de localização.)

Agendar backups automáticos

O Aranda Datasafe fará backup automático dos dispositivos que usam uma política. O primeiro backup é feito cerca de 10 minutos após a ativação de um dispositivo e, depois disso, os backups são executados regularmente.

Você pode definir a programação nas configurações de **Backup e Restauração** de uma Política.

Definir o agendamento para backups automáticos

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Clique na guia **Backup e Restauração**.

3. Use a opção Executar backups de dispositivo em todas as opções para escolher com que frequência os backups automáticos serão executados. Você pode escolher:

- 1 hora
- 2 horas
- 4 horas
- 48 horas
- Clique em **Salvar** ou **Salvar e Fechar** para confirmar.

Exemplo: Se você tiver uma política de 'Finanças' e a tiver configurado para fazer backup a cada 2 horas. Também possui uma equipe de 'Finanças' e recebeu a política de 'Finanças'.

Os dispositivos da equipe de Finanças terão seus dados copiados automaticamente a cada 2 horas (já que esse é o agendamento definido na política usada por sua equipe).

Para dispositivos em outros computadores, o agendamento de backup pode ser diferente, pois seus computadores podem usar uma política diferente configurada para fazer backup em um horário diferente, como a cada 8 horas.

Ativar criptografia local

Pré-requisitos: antes de habilitar os recursos DLP, verifique se os Serviços de Certificados do Active Directory foram configurados.

Você pode configurar a política para habilitar a criptografia de arquivos que estão nos dispositivos do usuário. Chamamos isso de "criptografia de arquivo local".

Uma vez habilitado, cada dispositivo que usa a Política receberá um certificado (também conhecido como chave) e a criptografia local será aplicada. Somente usuários autenticados podem acessar dados em um dispositivo se o certificado estiver disponível.

O certificado é usado para controlar o acesso aos dados em um dispositivo. Ao revogar o certificado no Aranda Datasafe, você o exclui do dispositivo e os dados no dispositivo ficam inacessíveis.

Se você habilitar o recurso **Prevenção de roubo de dados**, o certificado será revogado automaticamente em dispositivos que não se conectam ao Aranda Datasafe dentro de um determinado período de tempo (consulte Ativando a prevenção contra roubo de dados).

Para habilitar ou desabilitar a criptografia de arquivo local em uma política:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Clique na guia **DLP**.

3. Use o controle deslizante **Criptografia** para ativar ou desativar a criptografia de arquivo local (verde está ativado, cinza está desativado).

4. Clique em **Salvar ou Salvar & Fechar** para confirmar.

Ativar a prevenção contra roubo de dados

Com o recurso de prevenção de roubo de dados do Aranda Datasafe, você pode configurar dispositivos para revogar o acesso a arquivos se eles não se conectarem ao Aranda Datasafe dentro de um determinado período de tempo. Para revogar um dispositivo, o Aranda Datasafe remove o certificado de criptografia do dispositivo.

Enquanto um dispositivo está sendo revogado, ele não pode ser usado para acessar dados protegidos.

Você pode habilitar ou desabilitar o recurso de prevenção contra roubo de dados em uma política. Quando a Prevenção de roubo de dados estiver ativada, todos os dispositivos que usam a política precisarão se conectar ao Aranda Datasafe regularmente ou serão revogados.

Pré-requisitos: antes de habilitar os recursos DLP, verifique se os Serviços de Certificados do Active Directory estão configurados.
O recurso de prevenção contra roubo de dados só estará disponível se o recurso de criptografia de arquivo local estiver habilitado para a política. (Ele usa o certificado de criptografia gerado ao usar a criptografia de arquivo local.)

Para ativar ou desativar a prevenção contra roubo de dados:

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Clique na guia **DLP**.

3. Use o controle deslizante de **Prevenção de roubo de dados** para ativar ou desativar a Prevenção de roubo de dados (verde está ativado, cinza está desativado).

Uma mensagem é exibida lembrando você de configurar os Serviços de Certificados do Active Directory (AD CS). Recomendamos que você configure o AD CS antes de habilitar o DLP. Clique em **OK** para fechar a mensagem.

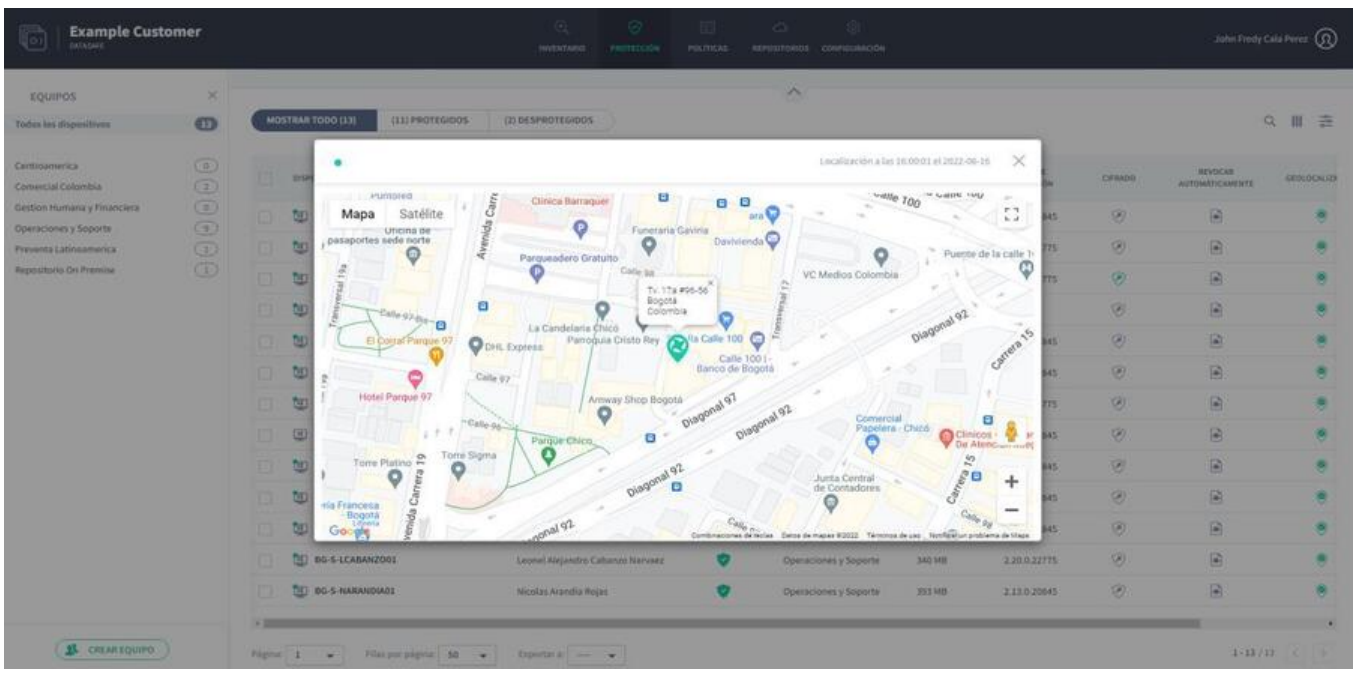
4. Use a opção **Revogar se o dispositivo se desconectar por dias** para definir quanto tempo o Aranda Datasafe aguardará antes de bloquear um dispositivo.

5. Clique em **Salvar ou Salvar & Fechar** para confirmar.

Ativar geolocalização

Pré-requisitos: antes de habilitar os recursos DLP, verifique se os Serviços de Certificados do Active Directory estão configurados.
Você pode usar o recurso de geolocalização para encontrar a última localização conhecida de seus dispositivos protegidos. Ele pode ser usado com qualquer dispositivo que tenha wi-fi habilitado.

Quando a geolocalização está ativada, você pode usar o Aranda Datasafe para localizar um dispositivo e ele exibirá a última localização conhecida em um mapa incorporado do Google.



Você pode habilitar ou desabilitar o recurso de **geolocalização** em uma política. Se ativado, todos os dispositivos que usam essa política e têm Wi-Fi ativado podem ser localizados **usando Localizar dispositivo** no Aranda Datasafe.

Para habilitar ou desabilitar a geolocalização em uma política:

1. Abra o Editor de políticas da política que deseja alterar (clique em Políticas e, em seguida, clique em Política).

2. Clique na guia **DLP**.

3. Use o controle deslizante **Geolocalização** para ativar ou desativar a criptografia local (verde está ativado, cinza está desativado).

4. Clique em **Salvar** ou **Salvar & Fechar** para confirmar.

Habilitar a migração de perfil de usuário

O recurso de migração foi projetado para ajudá-lo a migrar as configurações de perfil de usuário do Windows de um dispositivo protegido para outro. Esse tipo de dados inclui configurações de acessibilidade, configurações de mouse e teclado, favoritos e muitas outras configurações específicas do usuário.

Por exemplo, digamos que você tenha um laptop com backup e protegido pelo Aranda Datasafe. Você decide substituir o laptop por um laptop mais novo e com especificações mais altas. Ao usar o recurso de migração, você pode transferir as configurações do perfil de usuário do Windows do laptop antigo para o novo. Isso é muito mais rápido e fácil do que configurar o novo laptop do zero.

Você pode habilitar ou desabilitar o recurso de migração para cada política.

1. Abra o Editor de Políticas da Política que deseja alterar (clique em **Políticas** e clique em Política).

2. Clique na guia **Migração**.

3. Use o controle deslizante para ativar ou desativar os perfis de usuário do Microsoft Windows (verde está ativado, cinza está desativado).

4. Clique em **Salvar** ou **Salvar & Fechar** para confirmar.

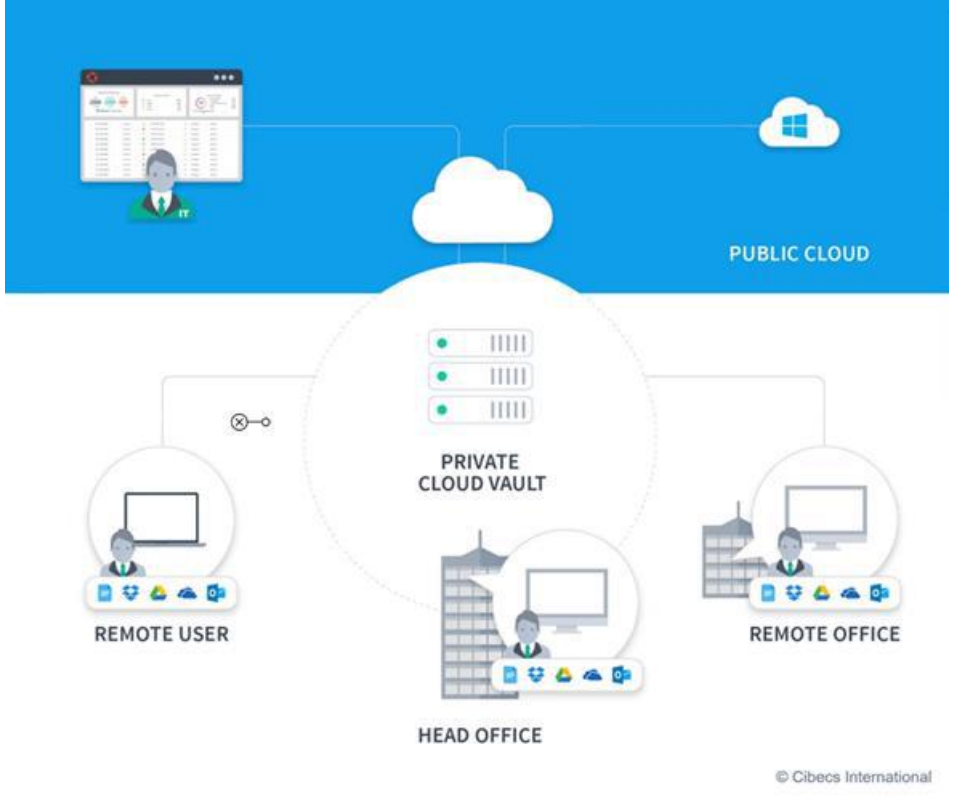
Para transferir as configurações de perfil de usuário do Windows de uma máquina para outra, você pode fazer backup manualmente do dispositivo a ser substituído. Em seguida, faça login no novo dispositivo, execute uma restauração e escolha quais configurações de perfil e dados usar. Para obter mais informações, consulte Migrar dados de perfil de usuário para um novo dispositivo.

Repositórios

Visão geral dos repositórios

Um repositório é uma área de armazenamento que pode ser instalada em um servidor em seu local ou em um servidor acessível remotamente. Ele armazena dados de backup criptografados de seus dispositivos ativados.

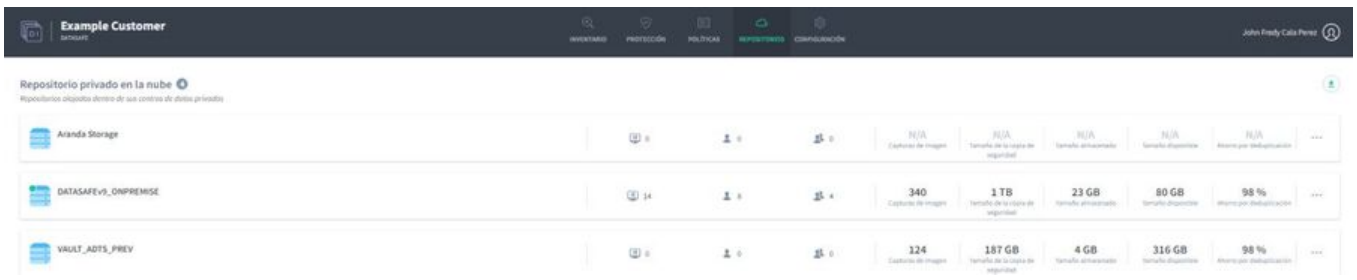
Para máxima eficiência, o Aranda Datasafe usa a desduplicação em nível de bloco do lado da origem para garantir que apenas os dados novos ou alterados sejam carregados no repositório. Os dados inalterados já existem no repositório, portanto, não precisam ser recarregados.



Repositórios

Você pode usar a página Repositórios para exibir informações sobre seus repositórios, que são áreas de armazenamento para seus backups.

Para exibir a página Repositórios, clique em Repositórios no banner superior.



A página de repositórios fornece uma lista de seus repositórios. Você pode pesquisar a lista de repositórios por nome e também pode baixar o instalador do repositório e Desconectar um repositório .

Lista de repositórios

Campo	Descrição
Status on-line	- Online: ícone verde - Off-line: ícone cinza
Aliases de repositório	O nome dado ao repositório quando ele foi criado. Geralmente é um nome descritivo que facilita a identificação do repositório.
Nome do host do repositório	O FQDN (Nome de Domínio Totalmente Qualificado) do repositório. Esse nome de host será usado para se conectar a um repositório.
Dispositivos	O número de dispositivos associados ao repositório pelo computador ao qual pertencem. Esses dispositivos farão backup no repositório associado.
Usuários	O número de dispositivos associados ao repositório pelo computador ao qual pertencem. Esses usuários terão backup de seus dados no repositório associado.
Equipamento	O número de computadores atribuídos ao repositório.
Instantâneo	O número de backups que foram feitos para um repositório. Um instantâneo é um backup feito em um determinado momento.
Tamanho do Encosto	O tamanho dos dados de backup antes da aplicação da eliminação de duplicação.
Backup Almacenado	A quantidade de espaço de armazenamento usada para armazenar os dados de backup.
Economia de desduplicação	A quantidade de espaço de armazenamento economizada usando a eliminação de duplicação, que é exibida como uma porcentagem. Em vez de fazer backup de cada arquivo todas as vezes, o Aranda Datasafe faz backup apenas dos arquivos que foram alterados desde o último backup. Isso é chamado de desduplicação e significa que menos espaço é necessário para seus backups e o processo de backup é mais eficiente.

Instalar e configurar um repositório

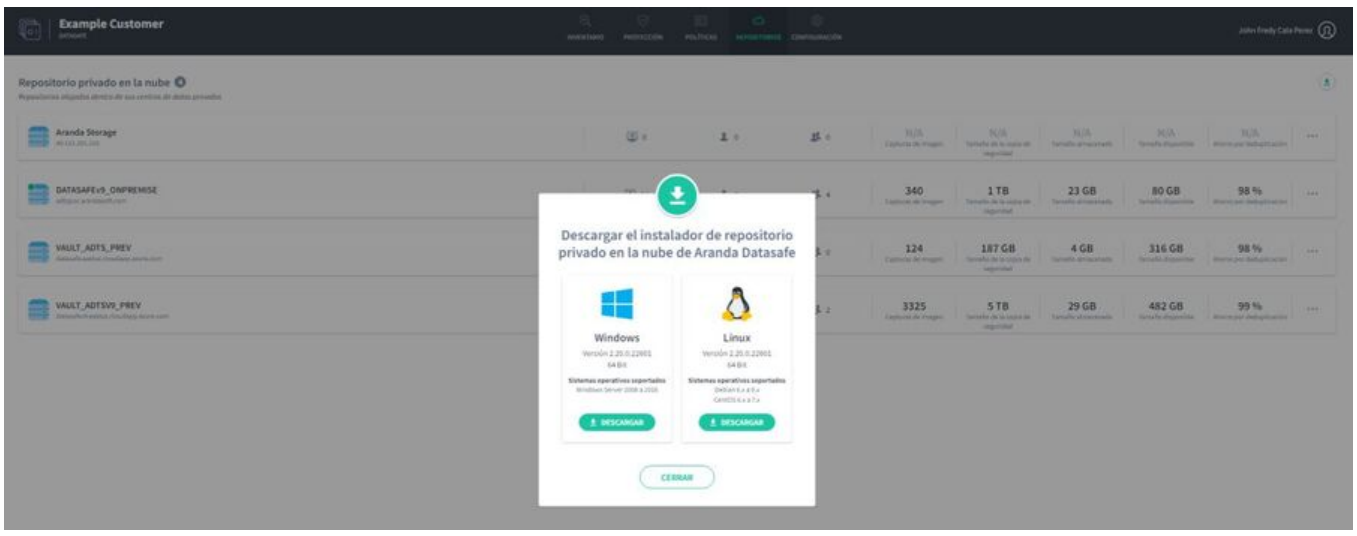
Para adicionar um novo repositório para armazenamento, você deve primeiro baixar o instalador do repositório. Você pode executá-lo em seu servidor e registrá-lo para se conectar ao Aranda Datasafe.

⚐ >**Observação:** Para registrar um repositório, você precisará ter o endereço de e-mail e a senha de uma conta de usuário do Aranda Datasafe com a função de **Administrador ou Oficial de Segurança**.

Para baixar e instalar o pacote Private Cloud Vault:

1. Clique em **repositórios**.

2. Clique em Baixar **Cofre de nuvem privada**.



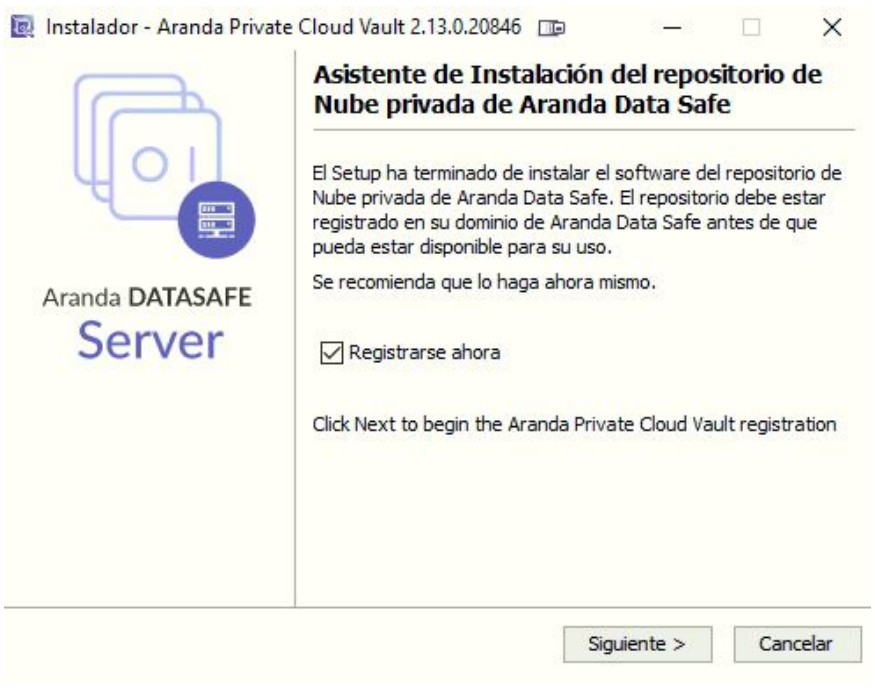
3. Quando o pacote Private Cloud Vault for baixado, procure-o em seu computador e copie-o para o servidor.

4. No servidor, instale o software Private Cloud Vault. Você pode instalá-lo no local padrão ou escolher outro local, se preferir.

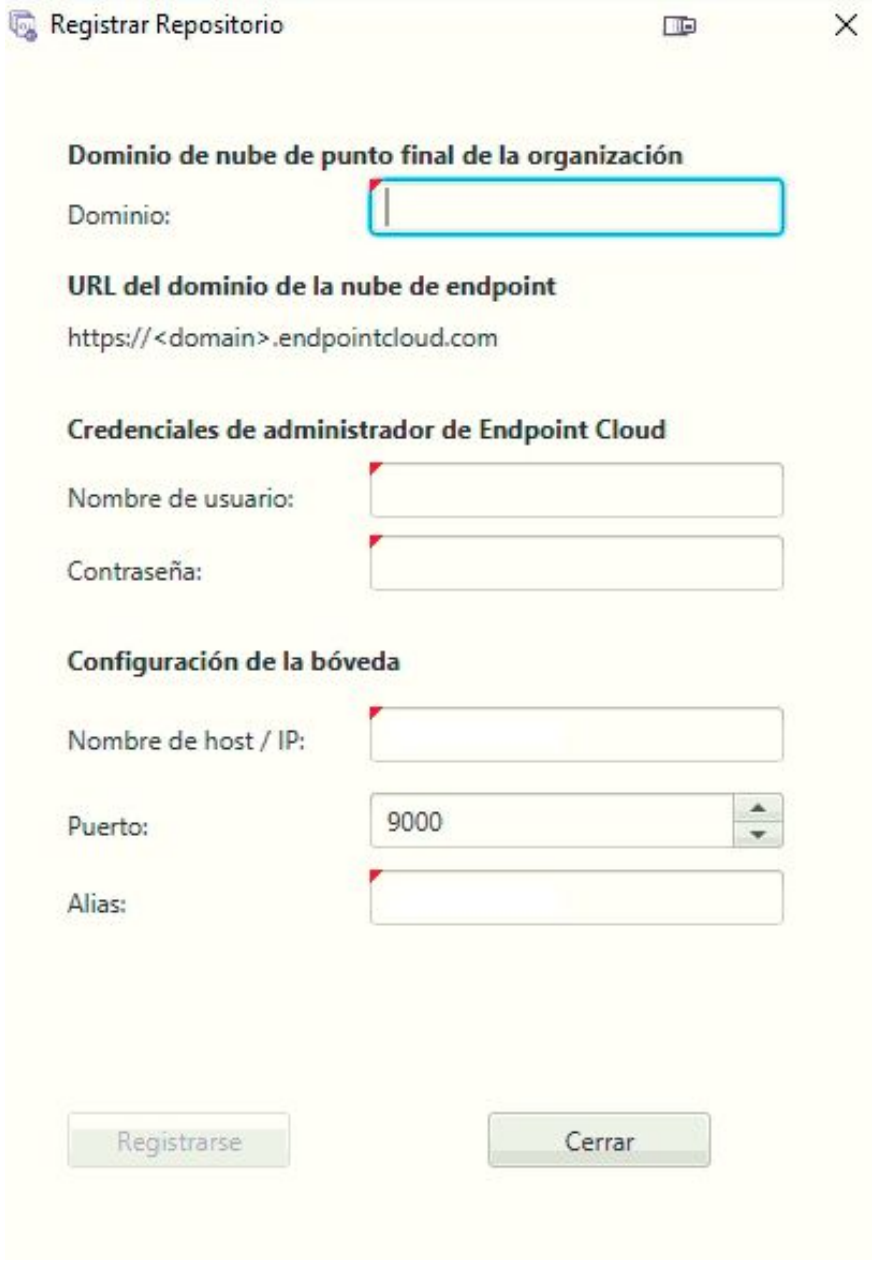
Importante: Você deve escolher um local que tenha uma quantidade adequada de espaço de armazenamento para seus dados. Geralmente, recomendamos 20 GB por usuário, mas isso pode variar dependendo do tipo e da quantidade de dados que sua organização usa.

Siga as etapas do assistente de instalação.

Depois de instalar o software, verifique se a opção Inscrever-se agora está marcada e clique em Avançar.



5. Insira os detalhes de registro:



Campo	Descrição
Domínio	O nome do seu locatário do Aranda Datasafe. Este é geralmente o nome da sua organização e é a primeira parte do seu endereço Aranda Datasafe.
Nome de usuário	Insira o nome de usuário de uma conta do Aranda Datasafe que tenha a função de Administrador ou Responsável pela Segurança. Somente essas contas de usuário têm permissão para registrar um repositório.
Senha	Digite a senha da conta Aranda Datasafe.
Nome do host / IP	Insira o nome ou endereço IP do servidor que tem o software do repositório instalado. Se o servidor estiver em um endereço da Internet, insira o URL.
Porto	9000. (A porta deve ser definida como 9000).
Pseudônimo	Digite o nome do repositório como ele aparecerá no Aranda Datasafe.

Importante: Os agentes de descoberta e os agentes de proteção devem ser capazes de se comunicar com o repositório pela porta 9000.

6. Clique em **Inscrever-se**.

Excluir um repositório

Se você não precisar mais de um repositório, poderá removê-lo do Aranda Datasafe "separando-o". Quando você exclui um repositório:

- Você não pode mais restaurar dispositivos do repositório excluído
- O repositório não pode ser atribuído a nenhuma equipe (se você tiver equipes usando o repositório excluído, precisará atribuir a eles um repositório diferente, caso contrário, seus dispositivos não serão copiados).

Para excluir um repositório:

1. Clique em **repositórios**.

2. Localize o repositório que deseja excluir.

3. Selecione o botão de opção (...) do repositório e clique em **Excluir repositório**.

4. Para confirmar que deseja excluir o repositório, insira DETACH em letras maiúsculas na caixa de diálogo.

5. Clique em Desconectar para excluir o repositório.

Administradores

Visão geral dos administradores

O Aranda Datasafe possui um login seguro para impedir o acesso não autorizado. Para fazer login, você precisará ter um Conta de Administrador ou um Conta de Oficial de Segurança .

Para obter uma conta, deve ser convidado para o Aranda Datasafe por outro administrador. Você receberá o convite por e-mail e poderá seguir o link para configurar sua conta.

Ao fazer login, os recursos disponíveis para você dependerão da função atribuída à sua conta. Mas todos os administradores e agentes de segurança podem usar o Aranda Datasafe

para monitorar, gerenciar e configurar o backup e a proteção dos dados da sua organização.

Configurações de administradores

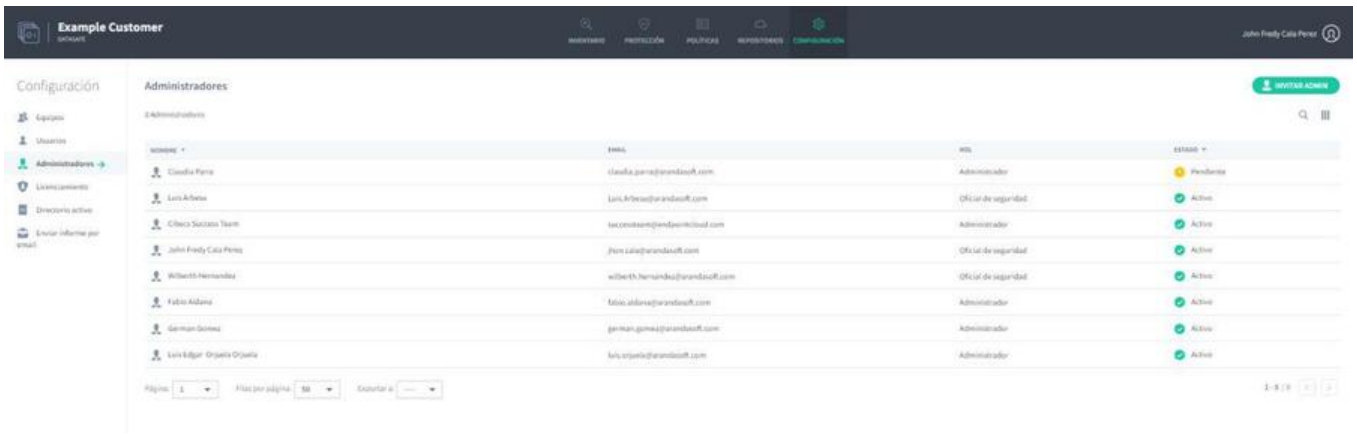
A página de configurações tem uma seção de administradores que você pode usar para:

- Visualize o nome e o endereço de e-mail de cada administrador.
- Veja se alguém é administrador ou oficial de segurança do Aranda Datasafe
- Convide alguém para se tornar um administrador do Aranda Datasafe
- Remova um administrador ou oficial de segurança.

Para exibir a seção Administradores:

1. Clique em **Configurações**.

2. No painel lateral, clique em **Administradores**.



Para cada administrador, você pode visualizar:

Campo	Descrição
Nome	O nome do administrador.
E-mail	O endereço de e-mail usado para convidar o administrador para o Aranda Datasafe.
Função	A função do administrador afeta os recursos que estão disponíveis para eles. As funções possíveis são: Responsável pela segurança: tem permissões completas de administrador e também pode baixar e registrar o AD Connector e pode alterar a função dos administradores. O oficial de segurança detém a chave para os dados de backup da organização. Recomenda-se que pelo menos dois agentes de segurança sejam implantados por locatário do cliente. **Administrador**: Tem acesso a todos os recursos do Aranda Datasafe, mas não pode baixar ou registrar o AD Connector ou alterar a função dos administradores.
Situação	Mostra se o administrador ativou a conta (Ativa) ou ainda não respondeu ao convite por e-mail (Pendente).

Se você passar o mouse sobre um administrador, poderá selecionar o menu de contexto (...). A partir daqui, você pode:

- Atribuir permissões de responsável pela segurança a um administrador ativo. A opção Atribuir Responsável pela Segurança só estará disponível se você entrar como Responsável pela Segurança.
- Remover um administrador.

Convidar administrador

Se você quiser dar a alguém acesso ao Aranda Datasafe, você pode convidá-lo para participar como administrador. Quando você envia o convite, o Aranda Datasafe cria um novo usuário de nível de administrador automaticamente e envia um e-mail para o novo usuário. Eles podem usar o e-mail para ativar sua conta.

Para convidar um novo administrador:

1. Clique em **Configurações**.

2. Clique em **Administradores**.

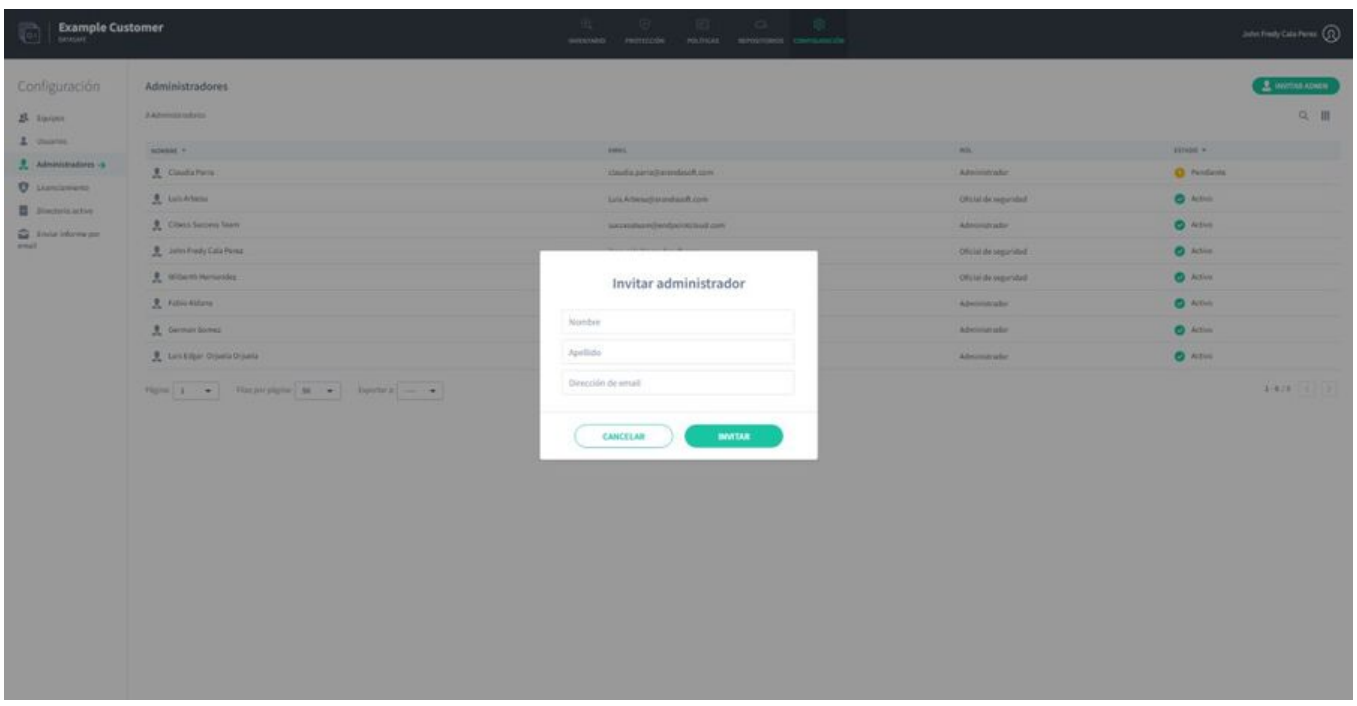
3. Clique em **Convidar administrador**.

4. Na caixa de diálogo Convidar administrador, insira o nome, sobrenome e endereço de e-mail do usuário que deseja adicionar como administrador.

5. Clique em **Convidar**.

O usuário receberá um convite por e-mail. Quando receberem o e-mail, poderão usá-lo para ativar sua conta. Uma vez ativados, eles poderão fazer login no Aranda Datasafe e acessar os recursos de nível de administrador.

Para obter mais informações sobre o convite por email, consulte Ative sua conta.

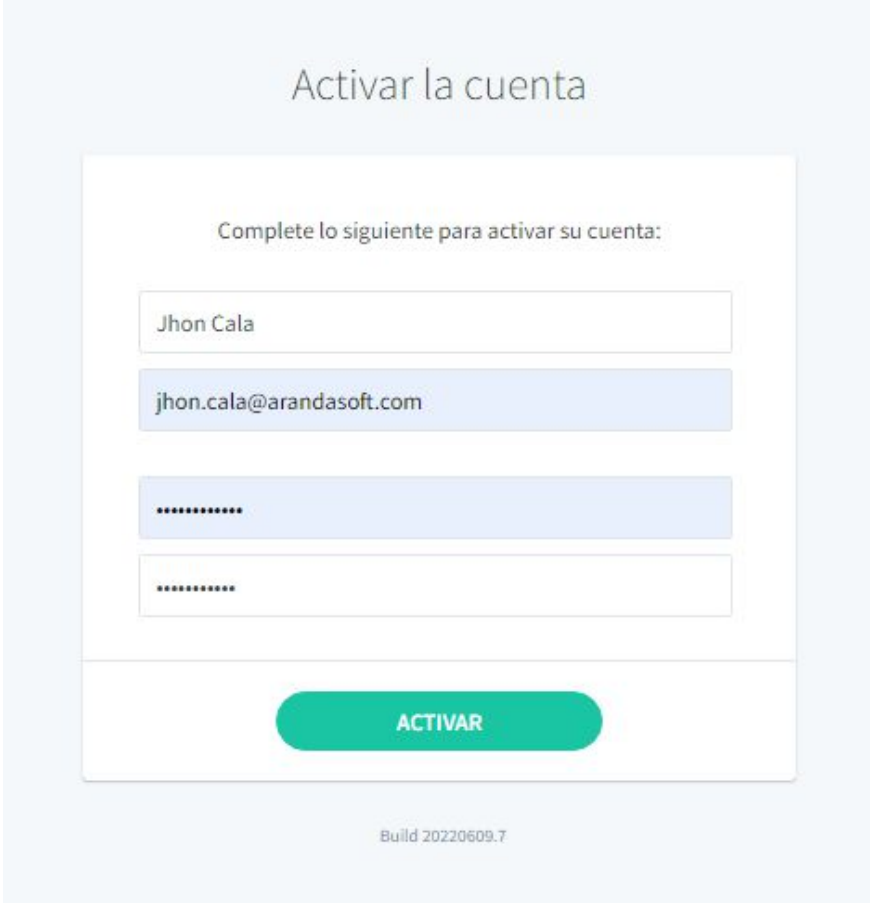


Ativar conta

Se você for usar o Aranda Datasafe, deverá receber um e-mail convidando-o a ativar sua conta.

Se você não receber o e-mail, verifique suas pastas de spam e lixo eletrônico. Se você ainda não conseguir encontrar o e-mail, entre em contato com o suporte da Aranda.

Depois de receber o e-mail, clique em **Ativar conta**. Seu navegador abre a página da web de ativação. Na primeira vez que você acessar o Aranda Datasafe, precisará inserir uma senha e digitá-la novamente para confirmar. Clique em **Ativar** para fazer login.



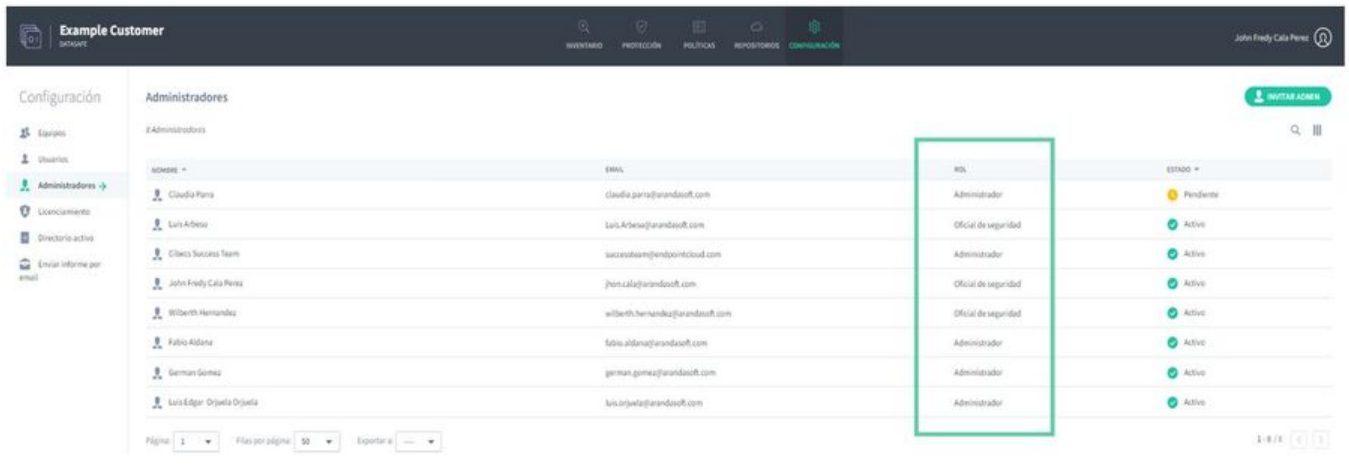
Função de administrador

Ao ativar um convite para ingressar no Aranda Datasafe, você recebe automaticamente uma conta. A conta tem uma função, seja como administrador ou como oficial de segurança.

Se você receber uma conta de administrador, poderá acessar todos os recursos do Aranda Datasafe, mas não poderá baixar e registrar o AD Connector.

Somente pessoas com a função de Responsável pela Segurança podem baixar e registrar o AD Connector.

Você pode ver o papel deles na seção**Administradores** na página**Configurações** (consulte Administradores - Página de configurações).



Função de Segurança Oficial

O papel de**Oficial de Segurança** é o papel de mais alto escalão. Os usuários com essa função têm acesso a uma gama mais ampla de recursos no Aranda Datasafe do que outros usuários, portanto, você deve ter cuidado ao atribuir essa função.

Os agentes de segurança são os únicos usuários que podem:

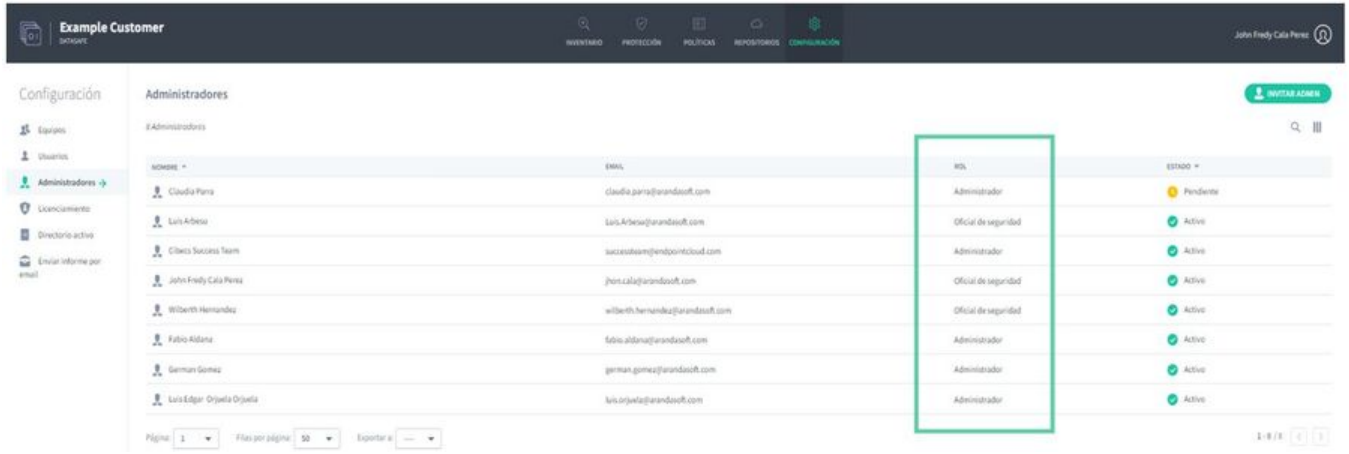
- Baixe e registre o conector do AD. Isso é necessário para permitir que o Aranda Datasafe proteja seus dispositivos e dados.
- Permitir o acesso a dados criptografados, necessários para restaurar os dados de um usuário.

O Aranda Datasafe deve ter pelo menos um usuário com a função de**Oficial de Segurança**.

Para verificar se sua conta de usuário tem a função de**Oficial de Segurança**:

1. Clique em**Configurações**.

2. Clique em**Administradores**.



3. Encontre sua conta de usuário na lista e veja se você tem a função de **Oficial de Segurança**.

Somente usuários com a função **Responsável pela segurança** podem alterar a função de uma conta de usuário.

Alterar função da conta

Se você entrar como responsável pela segurança, poderá alterar a função de uma conta de administrador. Isso é útil quando você deseja atualizar um administrador para responsável pela segurança, para que você possa registrar o conector do AD e restaurar os dados do usuário.

Para alterar a função de uma conta:

1. Faça login como oficial de segurança.

2. . Clique em **Configurações**.

3. Clique em **Administradores**.

4. Clique no botão de contexto (...) do administrador que você deseja alterar.

5. Clique em **Atribuir Oficial de Segurança**.

6. Digite sua senha para confirmar a alteração.

Remover um administrador ou responsável pela segurança

Se você fizer login no Aranda Datasafe como responsável pela segurança, poderá excluir outras contas de administrador e oficial de segurança. Normalmente, ele excluirá apenas contas que não estão mais em uso, por exemplo, se um membro da equipe tiver deixado a organização.

Cuidado: Se você excluir uma conta, o usuário dessa conta não poderá fazer login no Aranda Datasafe.

Para remover um administrador ou responsável pela segurança:

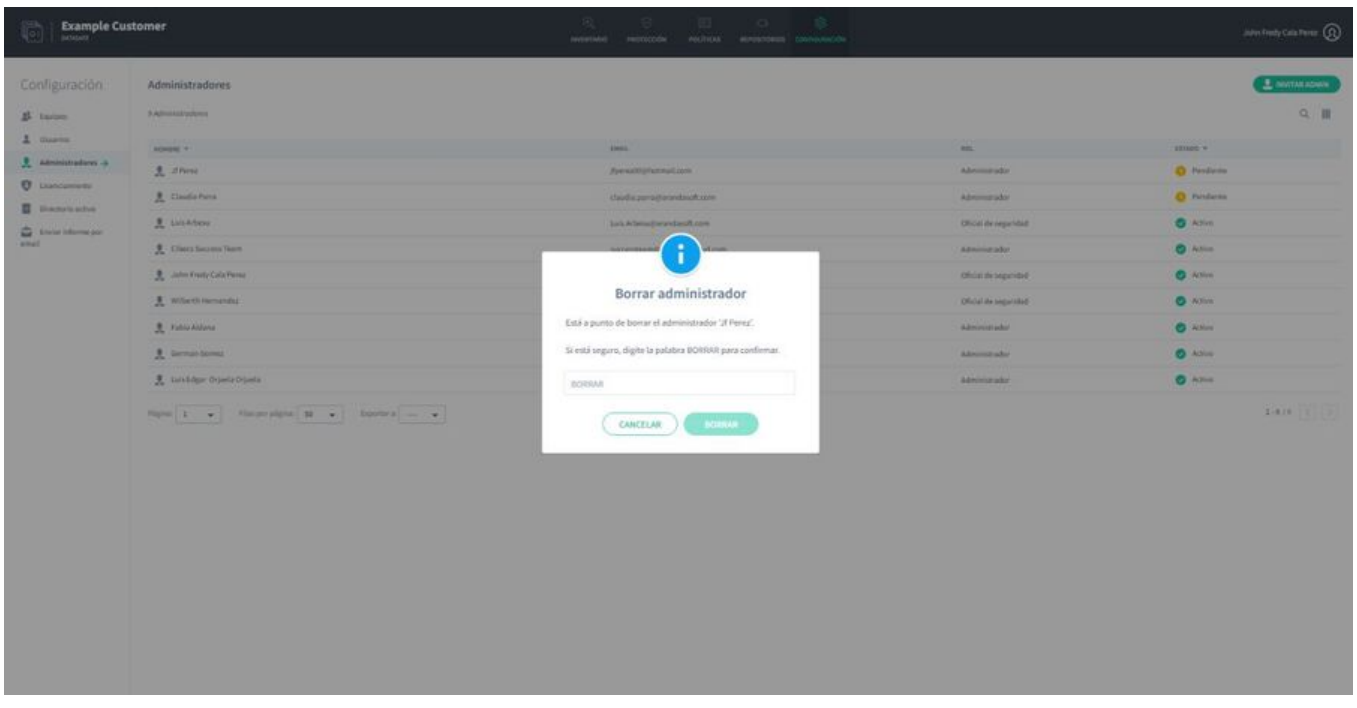
1. Clique em **Configurações**.

2. Clique em **Administradores**.

3. Clique no botão de contexto (...) do administrador ou responsável pela segurança que você deseja remover.

4. Clique em **Excluir**.

5. Digite Excluir na caixa de diálogo para confirmar e clique em **Excluir**.



Equipamento

Equipamento

No Aranda Datasafe, você precisa organizar seus dispositivos em equipes. Normalmente, os usuários do Aranda Datasafe criam equipes para grupos significativos, como departamentos de uma empresa ou localizações geográficas de diferentes instalações. Mas não há limitações: você pode criar equipes para qualquer agrupamento que desejar.

Quando o Aranda Datasafe descobre seus dispositivos pela primeira vez, eles são "não atribuídos". Isso significa que eles não estão em uma equipe.

Você precisa criar suas próprias equipes para poder:

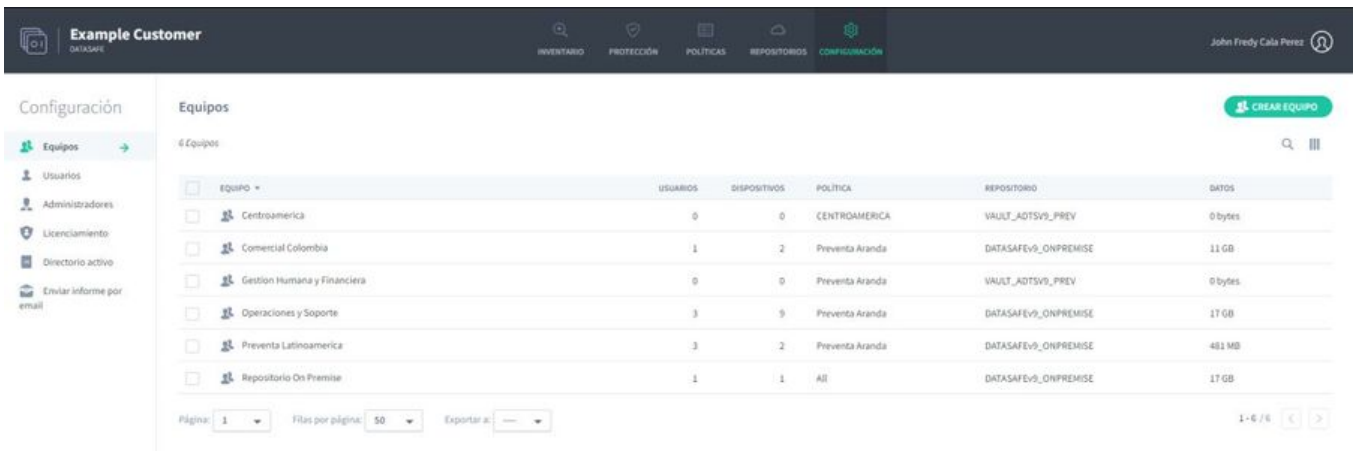
- Atribua uma **política** à equipe. Uma política é um conjunto de regras que definem:
    - Quais dados são protegidos e armazenados em backup
    - Com que frequência os backups ocorrem
    - Se algum recurso de **prevenção contra perda de dados** for usado para proteger seus dados em caso de perda ou roubo de um dispositivo. Isso inclui criptografia local, prevenção de roubo de dados e geolocalização.
    - Se os dados do perfil de usuário do Windows podem ser copiados para **migrá-los** para outros dispositivos.
- Atribua uma área de armazenamento **(repositório)**. O repositório é uma área de armazenamento em um servidor e é usado pelo Aranda Datasafe ao fazer backup de dispositivos em seu computador.
- Visualize e filtre informações sobre dispositivos em computadores específicos.

Para criar, editar e exibir equipamentos, você pode usar a página **Inventário**, a página **Proteção** ou a página **Configurações** (que tem uma seção **Equipamento**).

Configuração do equipamento

Você pode usar a seção **Equipes** na página **Configurações** para exibir, editar e excluir suas equipes.

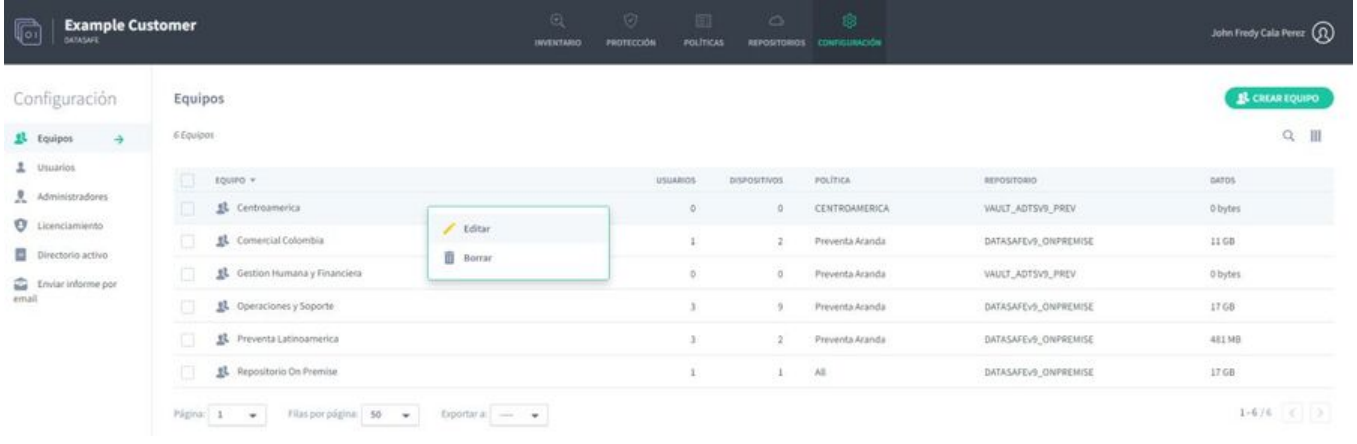
Para exibir a seção **Computadores**, clique em Configurações. A seção Equipes é exibida por padrão (se necessário, você pode exibi-la clicando em Equipes na barra lateral).



Para cada equipe, você pode ver:

Campo	Descrição
Usuários	O número de usuários na equipe
Dispositivos	O número de dispositivos atribuídos à equipe.
Política	A política atribuída à equipe. Uma política é um conjunto de regras que definem: - Quais dados são protegidos e armazenados em backup - Com que frequência os backups ocorrem - Se algum recurso de **prevenção contra perda de dados** é usado para proteger seus dados em caso de perda ou roubo de um dispositivo. Isso inclui criptografia local, prevenção de roubo de dados e geolocalização. - Se os dados do perfil de usuário do Windows podem ser copiados para **migrar** para outros dispositivos.
Repositório	O repositório atribuído à equipe. O repositório é uma área de armazenamento em um servidor e é usado pelo Aranda Datasafe ao fazer backup de dispositivos em seu computador.
Dados	A quantidade de espaço de armazenamento usada para fazer backup de dados em seu computador.

Se você passar o mouse sobre um computador, poderá selecionar seu menu de contexto (...). A partir daqui, você pode editar a equipe ou excluí-la.



Configuração de filtragem de equipamentos

Por padrão, a seção **Computadores** na página **Configurações** exibe informações para todos os computadores e dispositivos. Mas, se necessário, você pode filtrar a seção **Equipes** para mostrar apenas informações que atendam a determinados critérios. Por exemplo, você pode usar a pesquisa para filtrar a seção Computadores para que ela mostre apenas informações dos dispositivos de um determinado **computador**.

Há várias maneiras de filtrar a seção Equipes:

Usar uma pesquisa para filtrar a lista de computadores

Mostrar ou ocultar colunas na lista de equipes

Use uma pesquisa para filtrar a lista de computadores

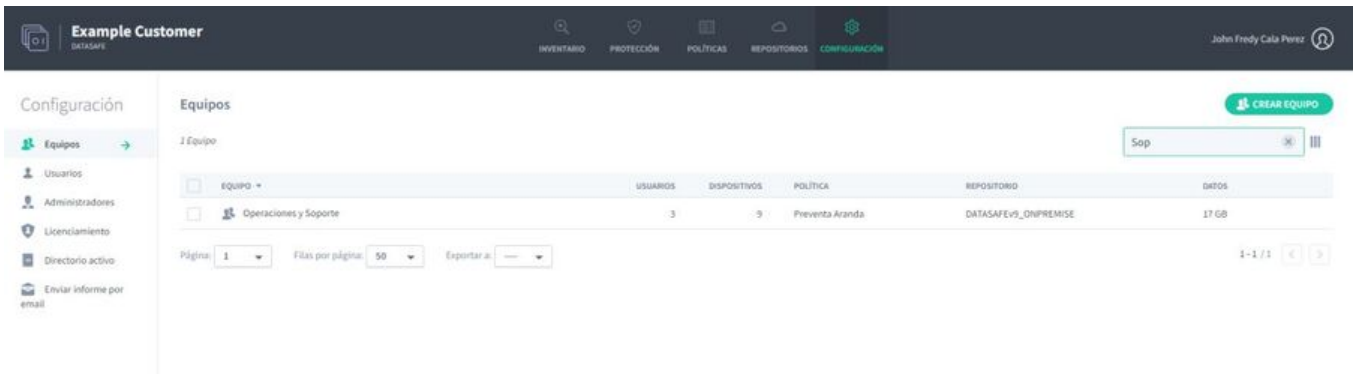
Você pode usar a função **pesquisar** para filtrar a lista de computadores para que ela inclua apenas computadores que tenham determinados valores. Por exemplo, você pode usar a pesquisa para filtrar a lista para que ela mostre apenas os computadores associados a um repositório específico.

Você pode usar a pesquisa para filtrar a lista de**equipes** por qualquer valor de texto, incluindo o nome da**equipe**, o nome da**política** e o nome do **repositório**.

Para aplicar um filtro de pesquisa:

1. Clique no ícone de pesquisa acima da lista de equipamentos.

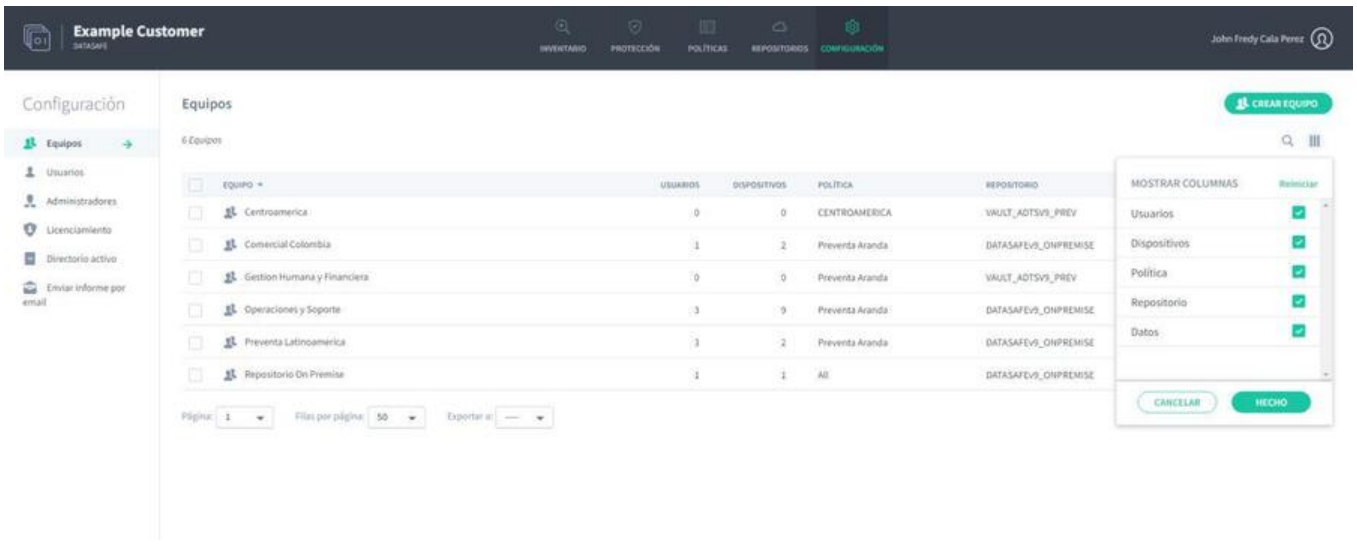
2. Insira os primeiros caracteres do valor de texto que deseja usar como filtro. O Aranda Datasafe aplica o filtro à medida que você digita, para que você possa fazer correspondências parciais ou inserir o valor de texto completo para ser mais específico.



Mostrar ou ocultar colunas na lista de equipamentos

Você pode optar por mostrar ou ocultar colunas na lista de equipes. Por exemplo, talvez você não se importe com qual repositório cada equipe usa, portanto, pode ocultar a coluna do repositório.

Para mostrar/ocultar colunas, clique no ícone Colunas e escolha quais colunas incluir.



Exibir dispositivos em uma equipe

Você pode usar as páginas **Inventário** ou **Proteção** para visualizar informações sobre os dispositivos em qualquer computador.

1. Clique em Inventário ou Proteção.

2. Na seção Equipes, clique em:

- **Todos os dispositivos** para exibir informações sobre todos os dispositivos em todos os dispositivos
- **Não atribuído** para exibir informações apenas para os dispositivos que ainda não estão atribuídos a uma equipe
- para exibir informações sobre dispositivos em um computador específico.

Quando você clica em uma opção de equipe, a página **Inventário** ou **Proteção** é atualizada e as telas do painel e da lista são filtradas para mostrar apenas informações sobre os dispositivos no dispositivo selecionado.

Clique em **Todos os dispositivos** na barra lateral **Teams** para remover o filtro.

Criar uma equipe

O Aranda Datasafe usa o Teams para organizar seus dispositivos em grupos.

Cada equipe tem um:

- **Política**: Define quando os dispositivos em seu computador serão copiados, bem como quais configurações de migração e prevenção contra perda de dados os dispositivos usarão.
- **Repositório**: Define onde os dados de backup dos dispositivos da sua equipe serão armazenados.

Ao criar uma equipe, você escolhe uma política e um repositório. Você também pode editar uma equipe para renomeá-la ou associá-la a uma política ou repositório diferente.

Crie uma equipe

Você pode criar uma nova equipe e atribuir a ela uma política e um repositório. Quando o computador estiver configurado, você poderá atribuí-lo aos seus dispositivos.

Você deve criar uma nova equipe se:

- Não há equipes no Aranda Datasafe
- Os computadores existentes não atendem aos seus requisitos, por exemplo, eles não usam a prevenção contra roubo de dados, mas você precisa dela para seus dispositivos.
- As equipes existentes fazem backup em um repositório que não é adequado para seus dispositivos.

Para criar uma equipe:

1. Existem três maneiras de criar uma equipe: na página **Inventário**, na página **Proteção** ou na seção **Equipes** na página Configurações. Então você pode:

Clique em **Inventário**.

ou:

Clique em **Proteção**.

ou:

Clique em **Configurações** e use a seção **Computadores**.

2. Clique em Criar Equipamento (canto inferior esquerdo da tela Inventário ou Proteção, canto superior direito na página Computadores - Configurações).

3. Insira um nome para a nova equipe.

4. Use a caixa de combinação **Atribuir uma política** para escolher a política para a equipe. Todos os dispositivos em seu computador usarão as configurações definidas na política (agendamento de backup, configurações de prevenção contra perda de dados etc.).

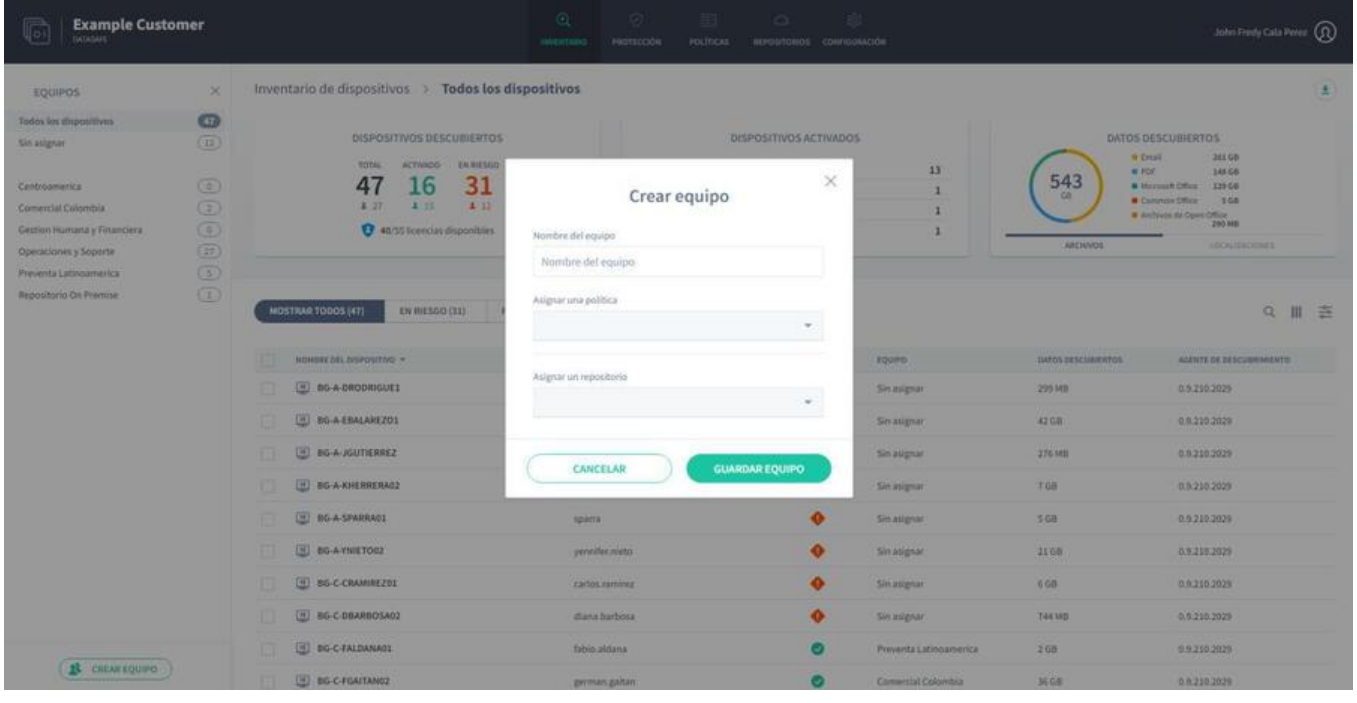
5. Use a caixa de combinação **Atribuir um repositório** para escolher a área de armazenamento que será usada para armazenar dados de backup para dispositivos em seu computador.

6. Clique em **Salvar Equipamento**.

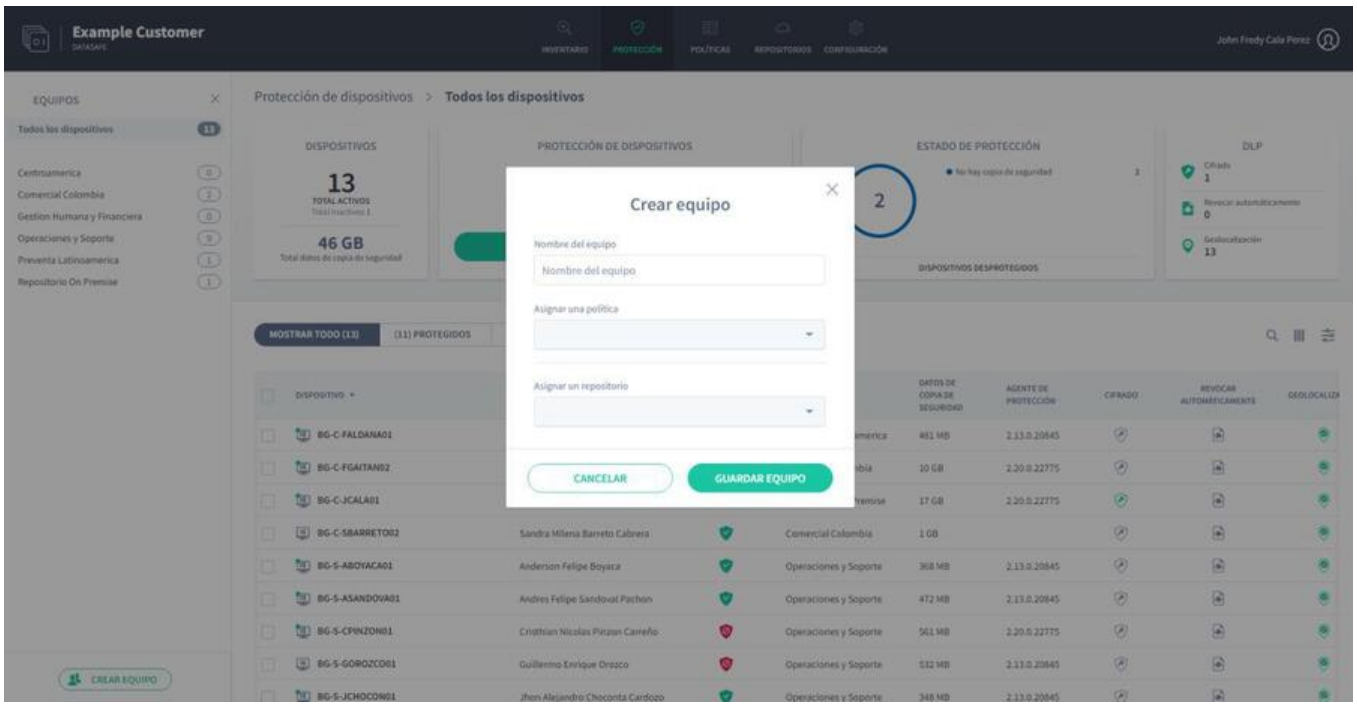
Seu novo equipamento aparece na seção **Equipamento** da página **Inventário** e na página Proteção. Ele também aparece na lista de **dispositivos** na página **Configurações**).

7. Repita as etapas 2 a 6 inclusive para criar quantos novos computadores forem necessários.

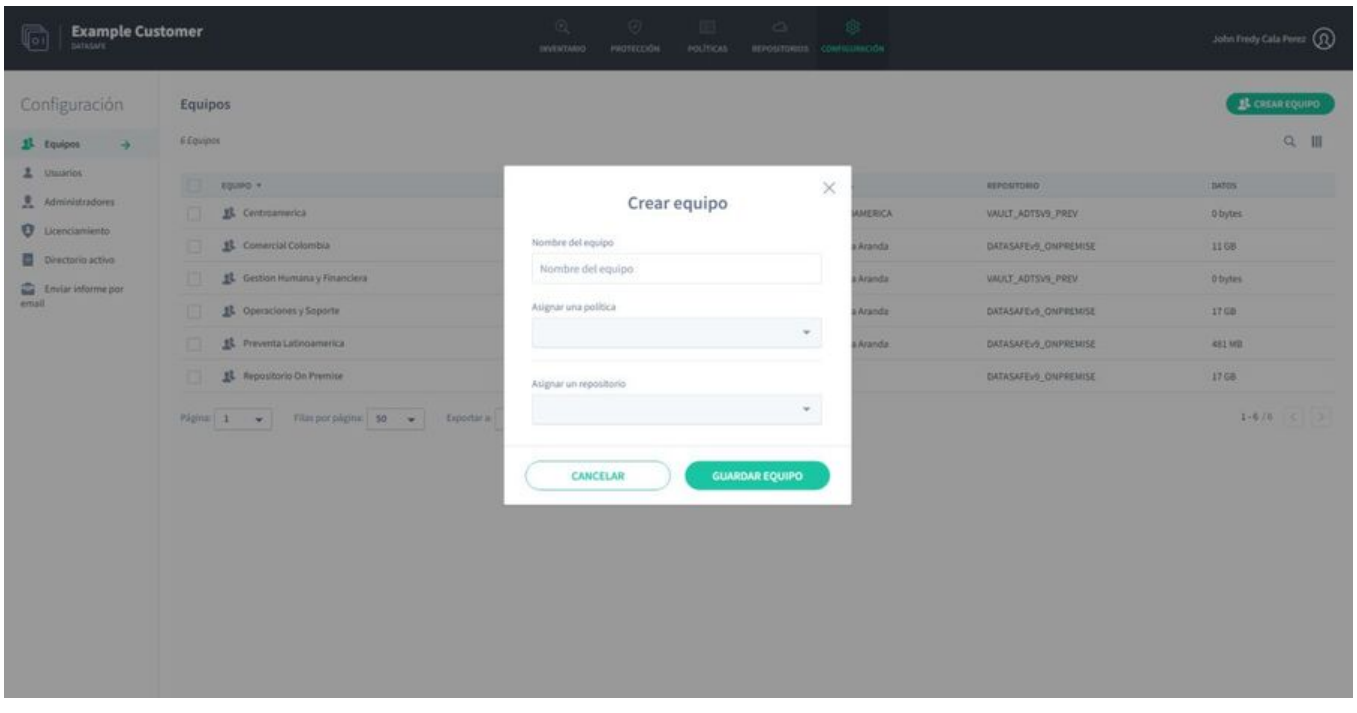
Criando uma equipe a partir do inventário:



Criando uma equipe na página Proteção:



Criando uma equipe na página Configurações:



Editar uma equipe

Se você quiser fazer alterações em um computador existente:

1. Existem três maneiras de editar um dispositivo: na página **Inventário**, na página **Proteção** ou na seção **Equipamento** na página **Configurações**. Então você pode:

Clique em **Inventário**.

ou:

Clique em **Proteção**.

ou:

Clique em **Configurações** e use a seção **Computadores**.

2. Passe o mouse sobre o equipamento que deseja editar e clique no botão de opção (...).

3. Clique em **Editar**.

4. Use o campo **Nome da equipe** para alterar o nome da equipe, se necessário.

5. Use a caixa de combinação **Atribuir uma política** para escolher a política para a equipe. Todos os dispositivos em seu computador usarão as configurações definidas na política (agendamento de backup, configurações de prevenção contra perda de dados etc.).

6. Use a caixa de combinação **Atribuir um repositório** para escolher a área de armazenamento que será usada para armazenar dados de backup para dispositivos em seu PC.

7. Clique em **Salvar equipamento**.

Atribuir políticas ao Teams

Você pode atribuir uma política a cada uma de suas equipes. Uma política é um conjunto de regras que definem:

- Quais dados são protegidos e armazenados em backup
- Com que frequência os backups ocorrem
- Se algum recurso de **prevenção contra perda de dados** for usado para proteger seus dados em caso de perda ou roubo de um dispositivo. Isso inclui criptografia local, prevenção de roubo de dados e geolocalização.
- Se é possível fazer backup dos dados do Perfil de Usuário do Windows para migração para outros dispositivos.

Normalmente, você atribui uma política a uma equipe quando cria a equipe pela primeira vez. Mas você também pode editar uma equipe para usar uma política diferente:

1. Clique em **Inventário** ou **Proteção**.

2. Passe o mouse sobre o nome da equipe e clique no botão de opção (...).

3. Clique em **Editar**.

4. Use a caixa de combinação **Atribuir uma política** para alterar a política da equipe.

5. Clique em **Salvar equipamento**.

Atribuir repositório a uma equipe

Você pode atribuir um repositório a cada uma de suas equipes. Um repositório é uma área de armazenamento em um servidor e é onde o Aranda Datasafe armazenará dados de backup para todos os dispositivos em um computador.

Normalmente, você atribui um repositório a uma equipe quando cria a equipe pela primeira vez. Mas você também pode editar uma equipe para usar um repositório diferente:

1. Clique em **Inventário** ou **Proteção**.

2. Passe o mouse sobre o nome da equipe e clique no botão de opção (...).

3. Clique em **Editar**.

4. Use a caixa de combinação **Atribuir um repositório** para alterar o repositório da equipe.

5. Clique em **Salvar equipamento**.

Atribuir dispositivo a uma equipe

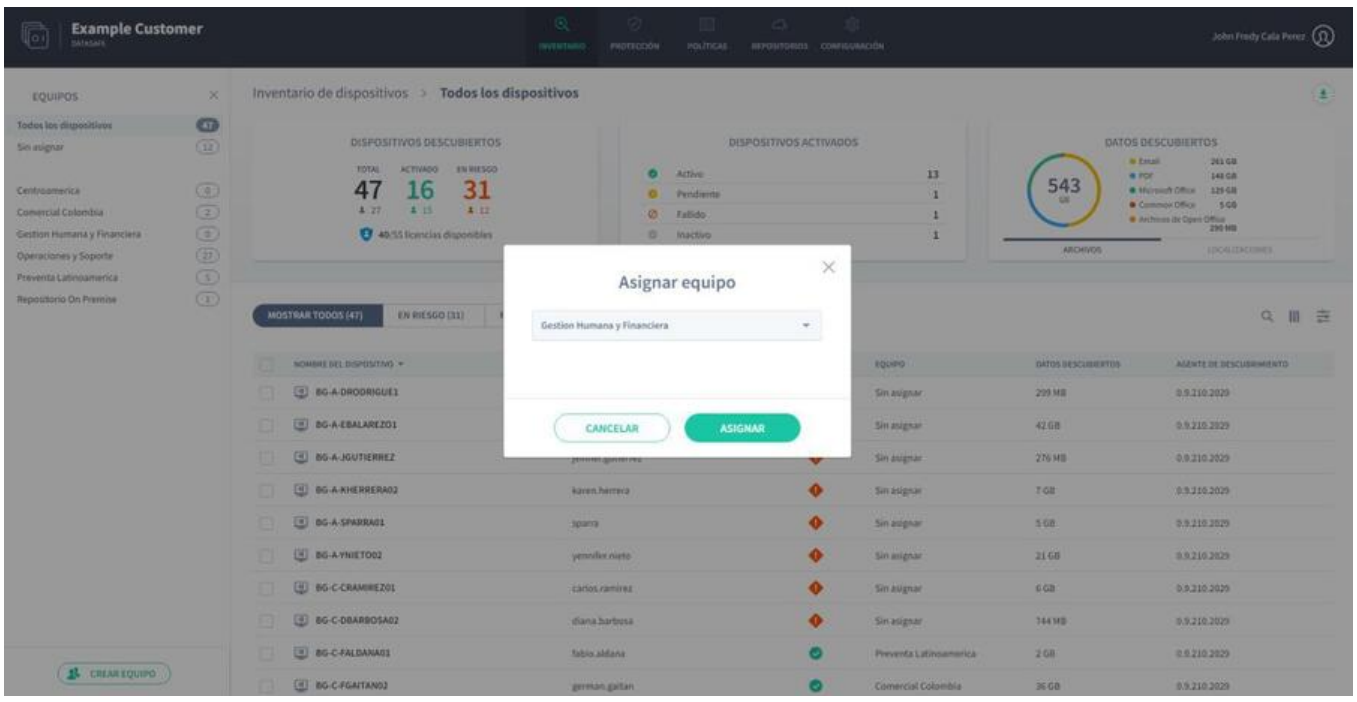
Para usar o Aranda Datasafe para fazer backup e proteger um dispositivo, o dispositivo deve ser atribuído a uma equipe. A equipe está associada a uma política e a um repositório, e eles definem:

- Quando os dispositivos são copiados
- Quais configurações de Prevenção contra perda de dados são usadas
- Quais configurações de migração são usadas

- Onde os dados de backup são armazenados.

Todos os dispositivos nesse computador usam as configurações do computador. Para atribuir um dispositivo a uma equipe:

1. Clique em **Inventário** ou **Proteção**.
2. Passe o mouse sobre um dispositivo na lista de dispositivos.
3. Clique no botão de opção no dispositivo (...).
4. Clique em **Atribuir equipe**.
5. Atribua o dispositivo a uma equipe da lista.
6. Clique em **Atribuir**.



A página será atualizada automaticamente e, após uma breve pausa, o dispositivo será atribuído para a equipe selecionada. Agora você pode usar a página **Inventário** ou **Proteção** para visualizar Informações sobre:

- Todos os dispositivos
- Dispositivos não atribuídos
- Dispositivos em cada um dos seus computadores.

Excluir equipamento

Pode haver momentos em que você precise remover um computador do Aranda Datasafe. Por exemplo, é Talvez você queira excluir uma equipe se sua organização tiver sido reestruturada ou algumas equipes em O Aranda Datasafe não existe mais em sua empresa ou se fundiu com outras equipes.

Se você não precisar mais de um equipamento, poderá removê-lo do Datasafe Washer. Quando você exclui um computador, Aranda Datasafe:

- Remova o equipamento
- Exclua todos os dispositivos atribuídos à equipe.

Importante: Se você quiser manter os dispositivos, deverá atribuí-los a uma equipe diferente antes de realizar a exclusão.

Para excluir uma equipe:

1. Clique em **Inventário** ou **Proteção**.
2. Passe o mouse sobre o equipamento que deseja excluir e clique no botão de opção (...).
3. Clique em **Excluir**.
4. Digite DELETE em letras maiúsculas e clique em **Excluir** para confirmar que deseja excluir o Equipamento

Usuários

Quando o Aranda Datasafe descobre seus dispositivos, ele cria automaticamente informações sobre as contas e dispositivos dos usuários. Essas informações são exibidas em várias telas, incluindo a página Inventário, a página Proteção e a página Configurações.

As contas de usuário e as informações do dispositivo são exibidas como:

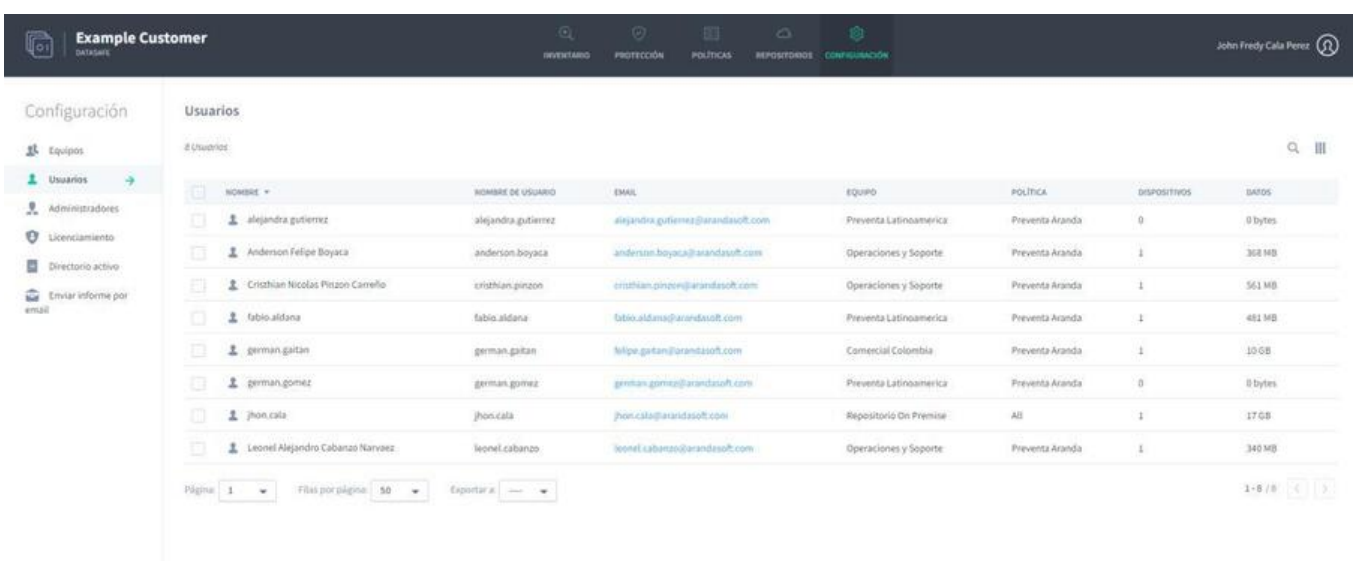
- **Usuário**: Um usuário representa um perfil de usuário do Microsoft Windows. Durante o processo de descoberta, o Aranda Datasafe se conecta aos dispositivos configurados para serem protegidos e recupera as informações de perfil do usuário. Crie um usuário para cada perfil de usuário do Windows (normalmente, isso significa um usuário por pessoa).
- **Nome do dispositivo**: cada usuário tem um ou mais dispositivos de usuário. Por exemplo, um usuário pode ter um computador desktop e um laptop. O Aranda Datasafe usa informações de perfil de usuário do Microsoft Windows para corresponder cada dispositivo a um usuário específico.

Configurações do usuário

Você pode visualizar os detalhes de seus usuários do Aranda Datasafe na página Usuários.

1. Clique em **Configurações**.

2. Na barra lateral, clique em **Usuários**.



A página Usuários exibe uma lista de usuários e fornece estas informações:

Campo	Descrição
Nome	O nome completo do usuário.
Usuário	O nome de usuário usado para fazer login no dispositivo do usuário.
E-mail	O endereço de e-mail do usuário.
Equipe	O computador ao qual o dispositivo do usuário está atribuído. Se um usuário tiver vários dispositivos, todos eles deverão ser atribuídos à mesma equipe.
Política	A política atribuída ao computador que usa o dispositivo do usuário. É essa Política que define quando o backup do dispositivo do usuário é feito, quais dados são copiados e protegidos e quais recursos de proteção e migração estão habilitados.
Equipamento	O número de computadores atribuídos ao repositório.
Dispositivos	O número de dispositivos dos quais o usuário fez backup e protegeu pelo Aranda Datasafe.
Dados	A quantidade de dados que o Aranda Datasafe fez backup para os dispositivos deste usuário.

Configurações de filtragem de usuário

Por padrão, a seção **Usuários** na página **Configurações** exibe informações para todos os usuários do Aranda Datasafe (que são baseados em perfis de usuário do Microsoft Windows). Mas, se necessário, você pode filtrar a seção **Usuários** para mostrar apenas informações que atendam a determinados critérios. Por exemplo, você pode filtrar a seção **Usuários** para mostrar apenas informações sobre um usuário específico.

Existem várias maneiras de filtrar a seção Usuário:

Use uma pesquisa para filtrar a lista de usuários

Mostrar ou ocultar colunas na lista de usuários.

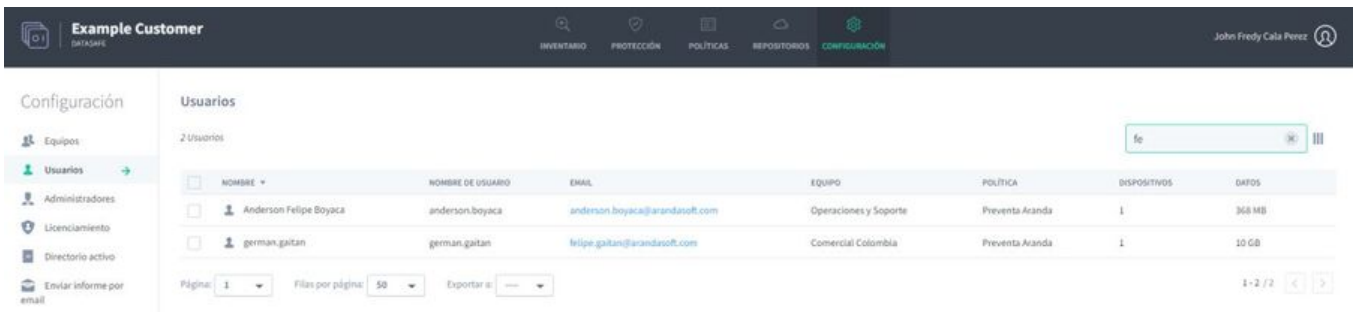
Use uma pesquisa para filtrar a lista de usuários

Você pode usar a função **pesquisar** para filtrar a lista de usuários para que ela inclua apenas usuários que tenham um nome específico (ou um nome parcial).

Para aplicar um filtro de pesquisa:

1. Clique no ícone de pesquisa acima da lista de usuários.

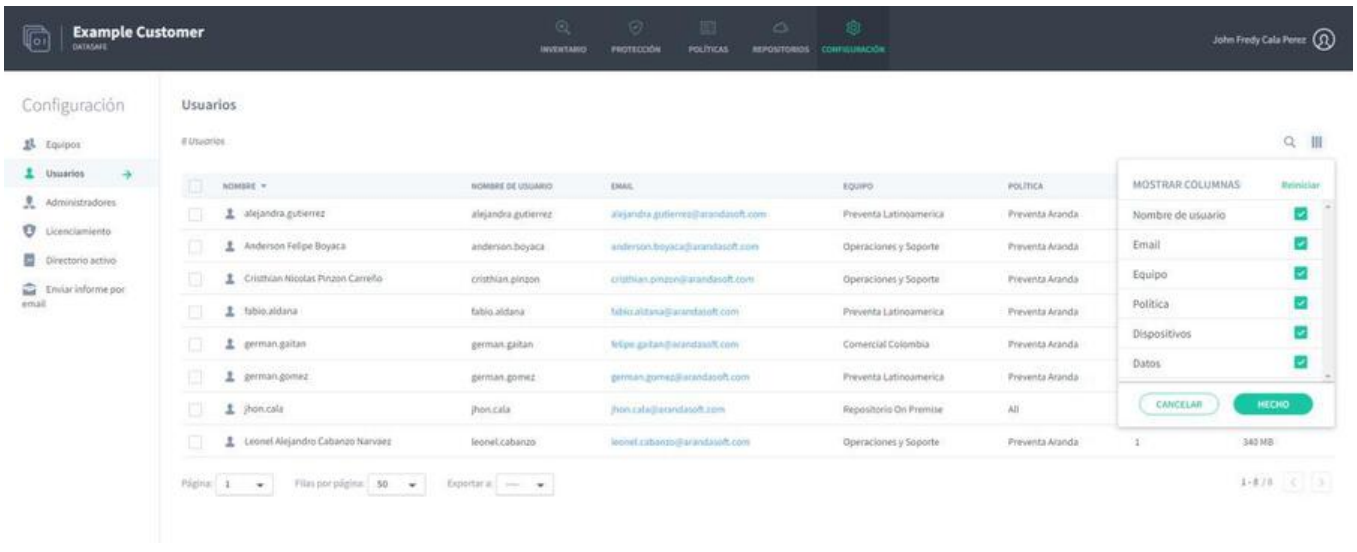
2. Insira os primeiros caracteres do valor de texto que deseja usar como filtro. O Aranda Datasafe aplica o filtro à medida que você digita, para que você possa fazer correspondências parciais ou inserir o valor de texto completo para ser mais específico.



Mostrar ou ocultar colunas na lista de usuários

Você pode optar por mostrar ou ocultar colunas na lista de usuários. Por exemplo, talvez você não se importe com o endereço de e-mail de cada usuário, portanto, pode ocultar a coluna E-mail.

Para mostrar/ocultar colunas, clique no ícone Colunas e escolha quais colunas incluir



Criar novo usuário

O Aranda Datasafe cria automaticamente novos usuários como parte do processo de descoberta. Não há necessidade de criar usuários manualmente.

Se você tiver um novo membro da equipe e precisar do Aranda Datasafe para fazer backup e proteger seus dispositivos, instale o Discovery Agent nos dispositivos. O Aranda Datasafe poderá então descobrir os dispositivos e conectar-se a eles.

Quando o Aranda Datasafe se conecta a um dispositivo, ele cria um usuário automaticamente, com base no perfil de usuário do Microsoft Windows do dispositivo.

Excluir usuário

Se você deseja remover um**usuário** do Aranda Datasafe, deve excluir todos os dispositivos desse usuário. Quando o Aranda Datasafe não possui dispositivos para um Usuário:

- Excluir esse usuário automaticamente
- Remova a licença do usuário e disponibilize-a para uso.

Para remover os dispositivos de um usuário (e também o usuário):

1. O primeiro passo é encontrar todos os dispositivos do usuário em uma lista de dispositivos. Para fazer isso, você pode usar a lista de dispositivos na página **Inventário** ou na página**Proteção**.

Clique em **Inventário**. ou:

Clique em **Proteção**.

2. Na seção da lista de dispositivos, clique no ícone**Pesquisar**.

3. Digite o nome do usuário na caixa de pesquisa. O Aranda Datasafe filtra a lista para que ela mostre apenas os dispositivos desse usuário.

4. Clique na caixa de seleção na parte superior da lista para selecionar todos os dispositivos do usuário.

5. Clique no ícone**Remover dispositivo** na parte inferior da lista de dispositivos.

6. Digite DELETE em maiúsculas e clique em**Excluir** para confirmar.

Conector do Active Directory

Conector do Active Directory

O Active Directory Connector (AD Connector) é um aplicativo que o Aranda Datasafe usa para autenticar suas contas de usuário. Ele se conecta ao seu Microsoft Active Directory e permite que o Aranda Datasafe:

- Identifique cada conta de usuário da Microsoft
- Identifique os dispositivos associados a cada conta de usuário da Microsoft.
- Crie automaticamente usuários e dispositivos correspondentes no Aranda Datasafe
- Autentique as conexões do dispositivo com o Aranda Datasafe.

Você deve instalar o AD Connector em um servidor Windows ingressado no domínio que esteja local em sua empresa. Você também deve registrar o conector do AD para que ele possa se conectar ao Aranda Datasafe.

Instalar e registrar o Active Directory Connector

O Active Directory Connector (AD Connector) é um aplicativo que o Aranda Datasafe usa para autenticar suas contas de usuário. Seus dados criptografados estão disponíveis apenas para usuários autorizados.

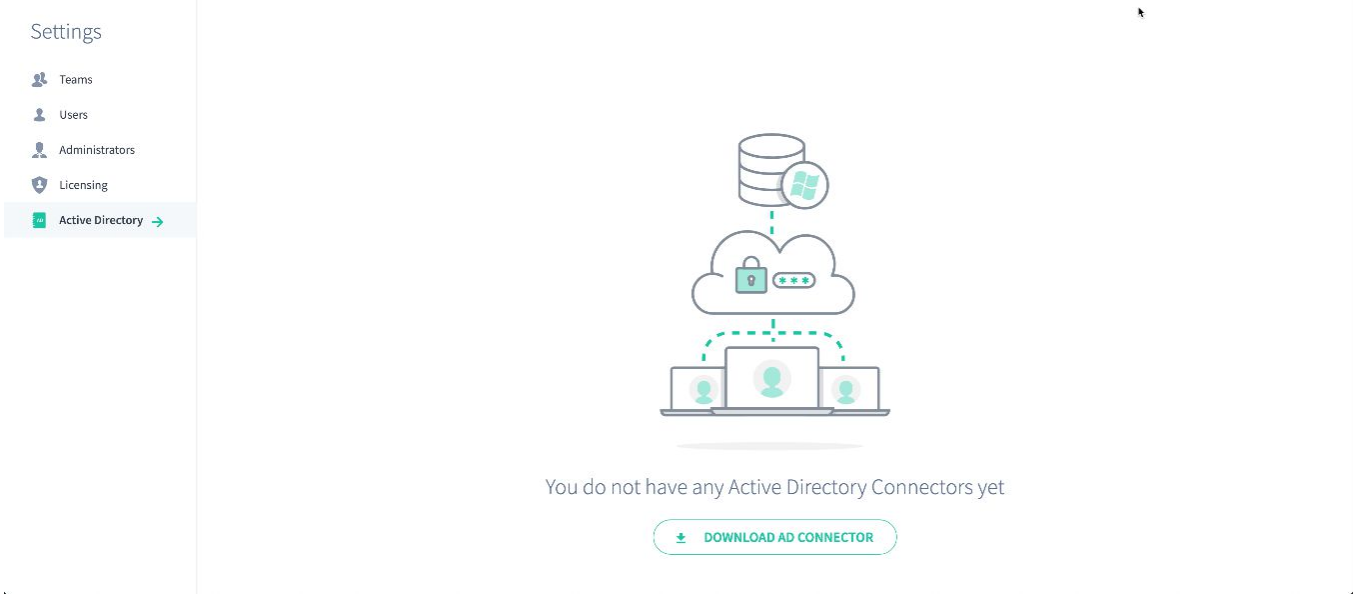
Você deve instalar o AD Connector em um servidor Windows ingressado no domínio que esteja local em sua empresa. Você também deve registrar o conector do AD para que ele possa se conectar ao Aranda Datasafe.

Para baixar, instalar e registrar o software AD Connector:

1. Clique em **Configurações**.

2. Clique em **Active Directory**.

3. Clique em **Baixar Ad Connector** para baixar o arquivo executável do adconnector. Copie este arquivo para o servidor local.



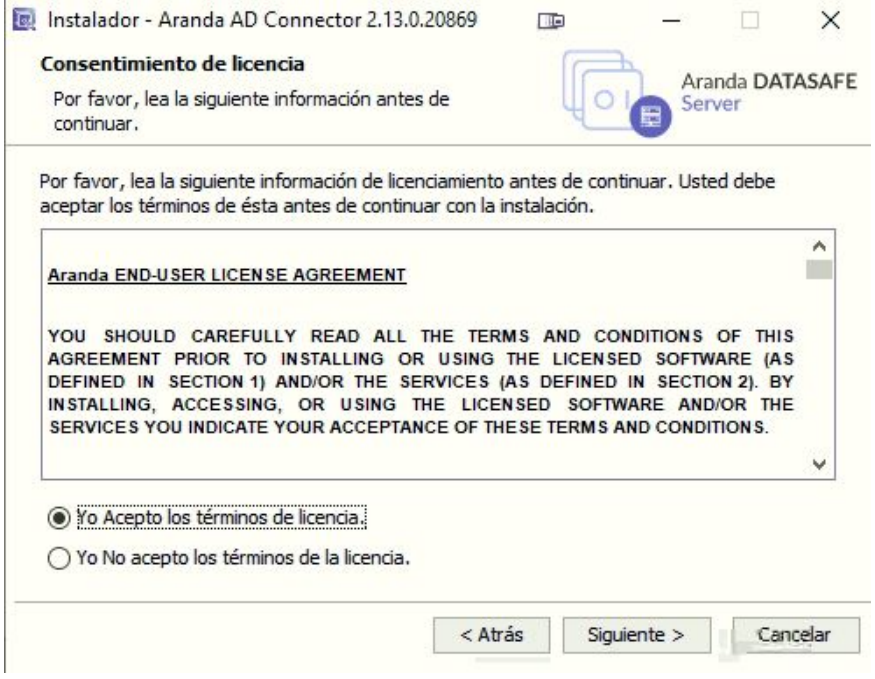
4. Faça login no servidor local (o servidor no qual o AD Connector será executado). Você deve fazer login por meio de uma conta de usuário administrador de domínio que tenha permissão para registrar um SPN (Nome de Serviço Principal) para conexões Kerberos.

5. Copie o arquivo executável do adconnector para o servidor e execute-o.

6. Siga as instruções na tela para instalar o conector AD. Você pode instalá-lo em qualquer diretório (o local padrão é a unidade C).

Quando você concluir as etapas de instalação, os arquivos começarão a ser extraídos e instalados. Quando os arquivos são instalados, o instalador pergunta se você deseja se registrar.

7. Certifique-se de que **Registre-se agora** esteja marcado e clique em **Avançar**.



8. Insira os detalhes do registro:

Campo	Descrição
Domínio	O nome do seu locatário do Aranda Datasafe. Geralmente, esse é o nome da sua organização e é a primeira parte do endereço do locatário do Aranda Datasafe.
Nome de usuário	Insira o nome de usuário de uma conta do Aranda Datasafe que tenha a função de Oficial de Segurança. Somente contas de usuário responsáveis pela segurança têm permissão para registrar um repositório.
Senha	Digite a senha da conta Aranda Datasafe.
Domínio	Digite o nome ou endereço IP do servidor que tem o software AD instalado.
Pseudônimo	Insira o nome do conector do AD como ele aparecerá no Aranda Datasafe. Recomendamos que você dê a ele um nome descritivo que seus usuários do Aranda Datasafe reconheçam.

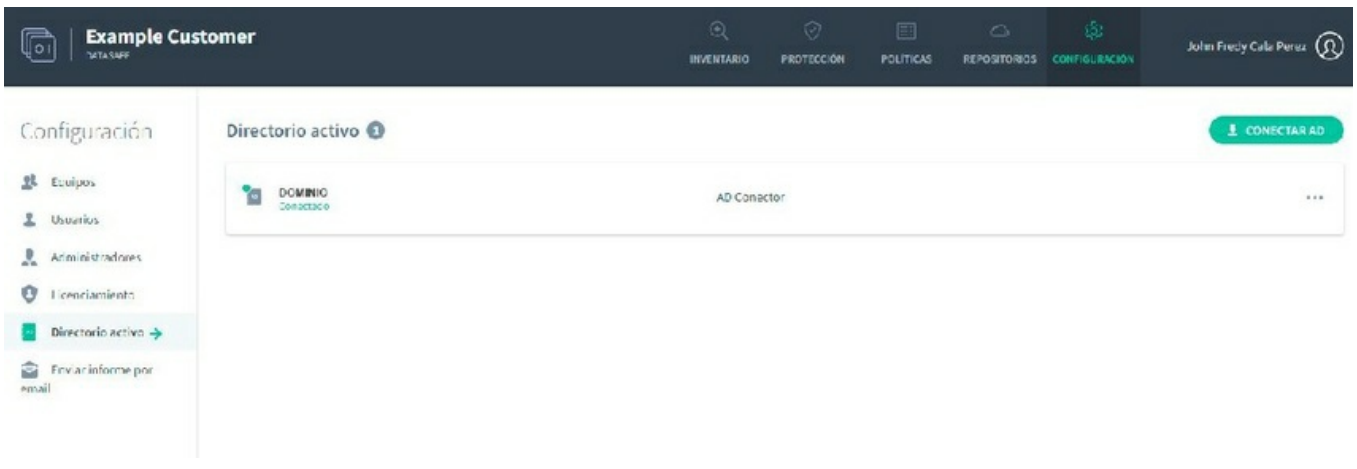
9. Clique em **Registrar**.

Remover o conector do Active Directory

Para remover um conector do AD:

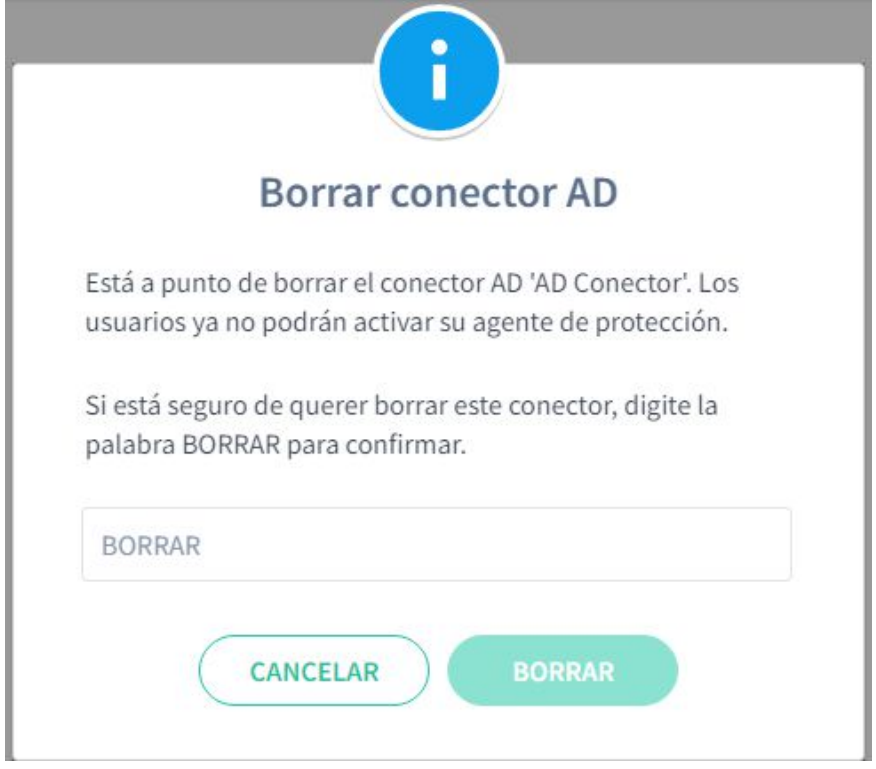
1. Clique em **Configurações**.

2. Clique em **Active Directory** na barra lateral.



3. Encontre o Active Directory que deseja excluir e clique no botão de opção (...) e clique em **Excluir**.

4. Digite CLEAR em letras maiúsculas na caixa de diálogo para confirmar.



5. Clique em **Excluir**.

Certificados

Certificados

O Aranda Datasafe exige que você tenha licenças para seus usuários. Ao adquirir um plano comercial, você recebe várias licenças com base em seus requisitos. Se esses requisitos mudarem, você poderá comprar mais licenças e adicioná-las ao seu plano.

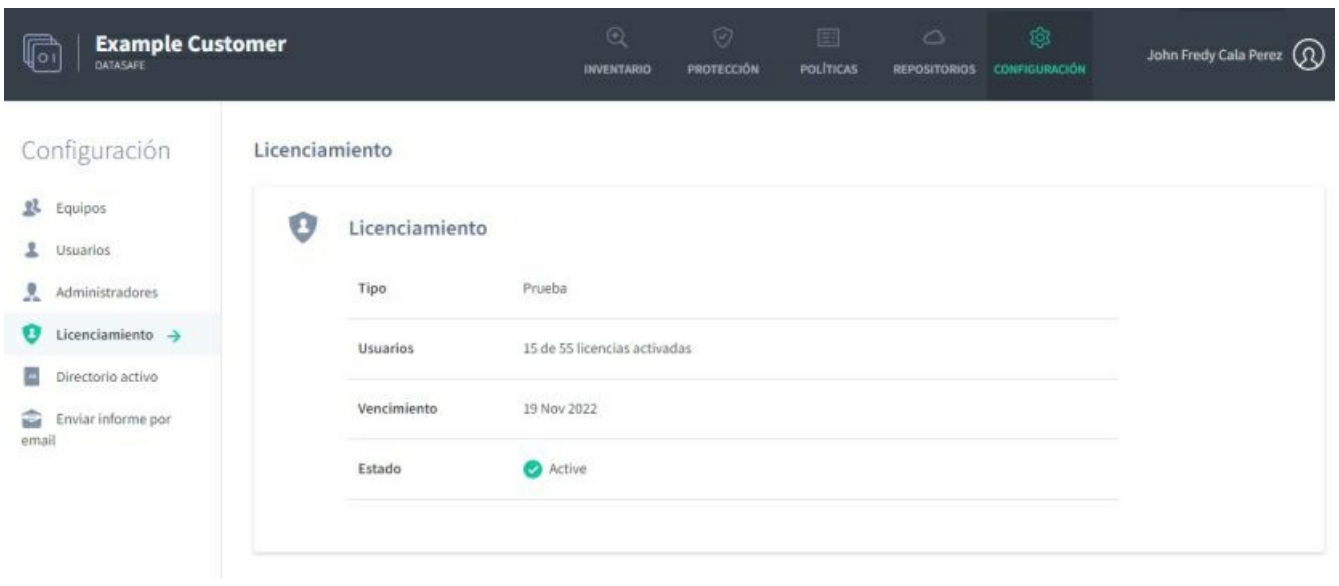
Você pode exibir informações sobre suas licenças no Página de licenciamento. Mostra o número de licenças disponíveis e o status da sua assinatura do Aranda Datasafe.

Configuração de licenciamento

Você pode exibir informações sobre seu plano e licenças disponíveis na página Licenciamento.

1. Clique em **Configurações**.

2. Clique em Licenças na barra lateral.



A página Licenciamento exibe:

Campo	Descrição
Tipo	Seu plano Aranda Datasafe.
	Comercial: No plano comercial, você pode usar o Aranda Datasafe para fazer backup e proteger seus dispositivos durante a duração da sua assinatura.
Usuários	O número de licenças que estão atualmente em uso e o número de licenças restantes disponíveis.
Expiração*	A data e a hora do término da sua assinatura do Aranda Datasafe.
Status	Mostra se sua assinatura do Aranda Datasafe está ativa ou expirada. Se sua assinatura expirar, seus dispositivos não serão mais copiados ou protegidos e, portanto, estarão em risco. Para assinar novamente, entre em contato com seu gerente de conta.

Backup e restauração

Backup e restauração

O Aranda Datasafe faz backup de seus dispositivos ativados automaticamente, em horários programados. Os dados são desduplicados e criptografados antes da transferência e permanecem criptografados durante a transferência e quando armazenados no repositório.

O que acontece antes que o backup ocorra?

Para iniciar o backup de um dispositivo, você precisará ativá-lo para proteção. Durante a ativação, o agente de proteção será baixado e instalado no dispositivo. O agente de proteção passará por um processo de autenticação antes que a indexação e os backups possam começar.

Antes do início do backup, o agente indexa o sistema de arquivos. O índice é criado uma vez e atualizado em tempo real à medida que os arquivos são adicionados, modificados ou excluídos do sistema de arquivos. A indexação em tempo real garante que uma verificação demorada e que consome recursos não seja necessária no momento do backup.

O que acontece durante um backup?

Durante um backup, o índice é referenciado para dados corporativos novos e alterados; Um instantâneo VSS é criado e os dados são desduplicados para garantir que apenas blocos de dados exclusivos sejam criptografados e transferidos do dispositivo do usuário para o repositório (área de armazenamento em seu servidor).

Backup automático

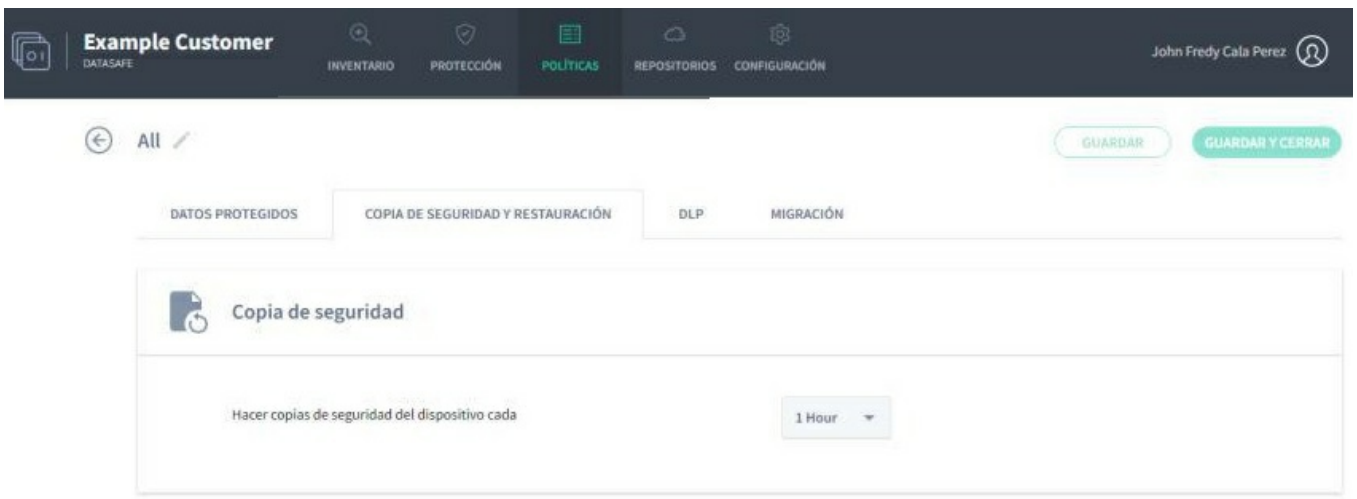
O Aranda Datasafe faz backup automático dos dados da empresa em seus dispositivos, desde que:

- O dispositivo está ativado
- O dispositivo está associado a um computador
- A equipe está associada a uma política e a um repositório.

O repositório define onde os dados de backup são armazenados.

A **Política** define:

- Quais dados de negociação são copiados
- Quando os backups são feitos.
- Quais recursos de prevenção contra perda de dados estão ativados.
- Se as configurações de perfil de usuário são copiadas para migrações de computador.



Seus dispositivos são automaticamente copiados e protegidos:

- **Logo após serem ativados pela primeira vez**. Isso geralmente leva cerca de 10 minutos, mas pode levar mais tempo, pois o backup só pode acontecer depois que o Agente de Proteção terminar a indexação.
- **Regularmente** de acordo com os intervalos programados estabelecidos nas Políticas.

Opções disponíveis: **A cada 1 hora	2 Horas	4 horas	8 horas**.

Você também pode fazer um Faça backup manualmente se desejar.

Executando o Aranda Data Safe Backup

Quando você tem dispositivos ativados no Aranda Datasafe, seus dados comerciais são protegidos automaticamente:

- Aproximadamente 10 minutos após a ativação inicial
- Regularmente, de acordo com o cronograma de backup (conforme definido na Política).

Você também pode fazer backup de um dispositivo manualmente, seja no Aranda Datasafe ou usando o Agente de Proteção localmente no dispositivo. Isso é útil se você precisar fazer backup de um dispositivo imediatamente e o próximo backup agendado não deve ser feito por algum tempo.

Abaixo, explicamos as várias maneiras de**executar um backup remoto no Aranda Datasafe**:

Executar um backup remoto na página de proteção.

Executar um backup remoto na página do dispositivo.

Execute um backup remoto na página de proteção

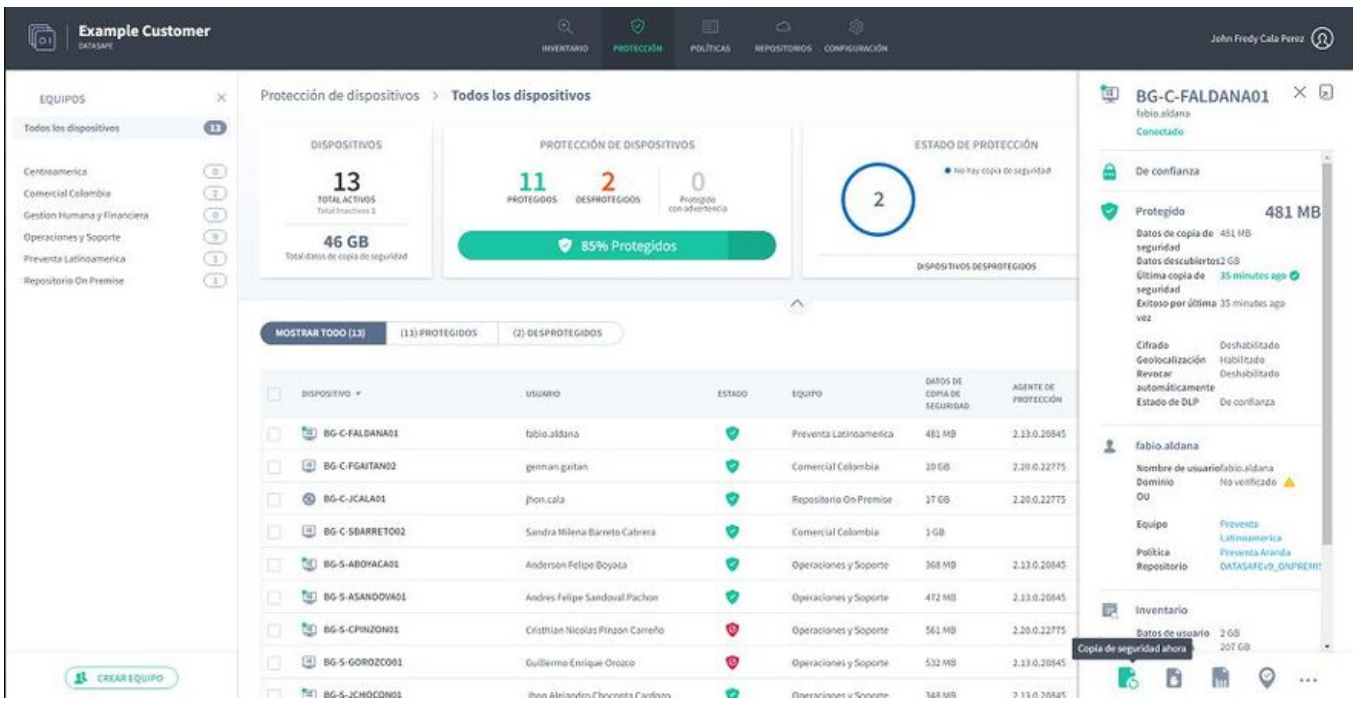
Para executar um backup na página**Proteção** do Aranda Datasafe:

1. Clique em**Proteção**.

2. Na lista de dispositivos, clique no dispositivo que deseja fazer backup. Seus detalhes aparecem em um painel lateral.

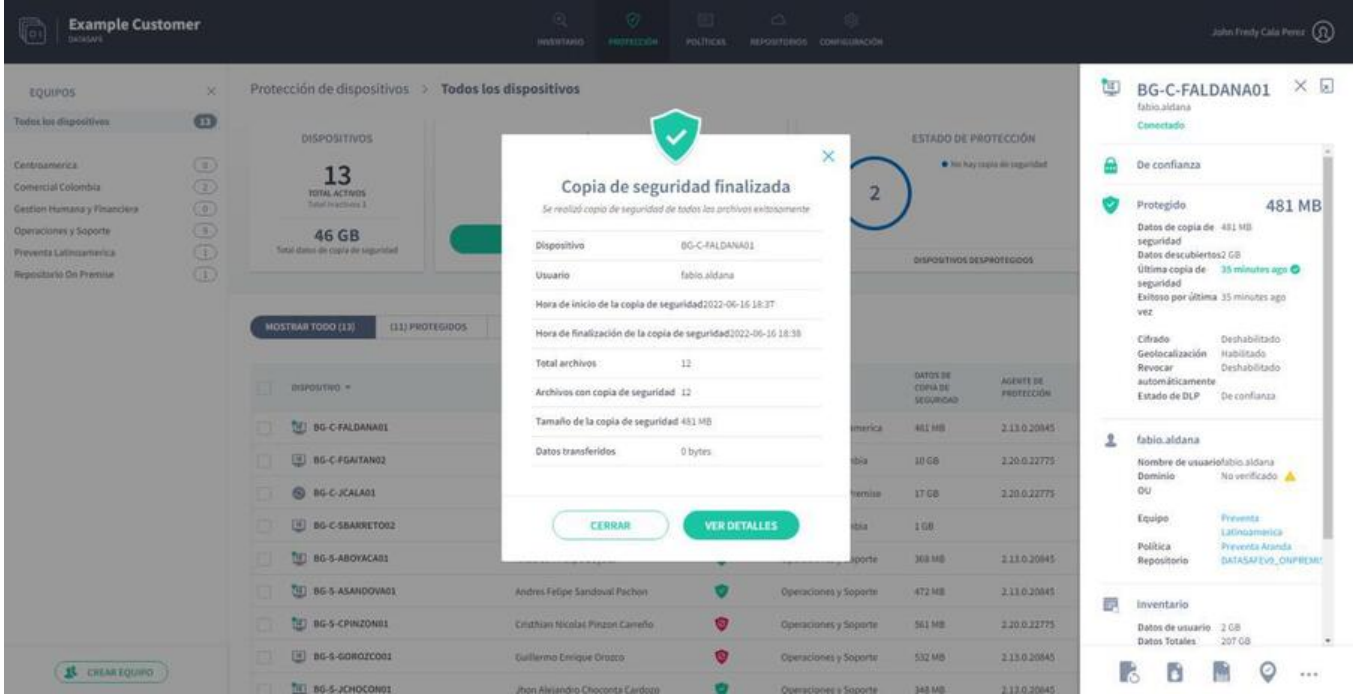
3. Clique no ícone**Fazer backup agora** na parte inferior do painel.

4. Uma mensagem aparece na parte inferior da tela para informar que a solicitação de backup foi bem-sucedida.

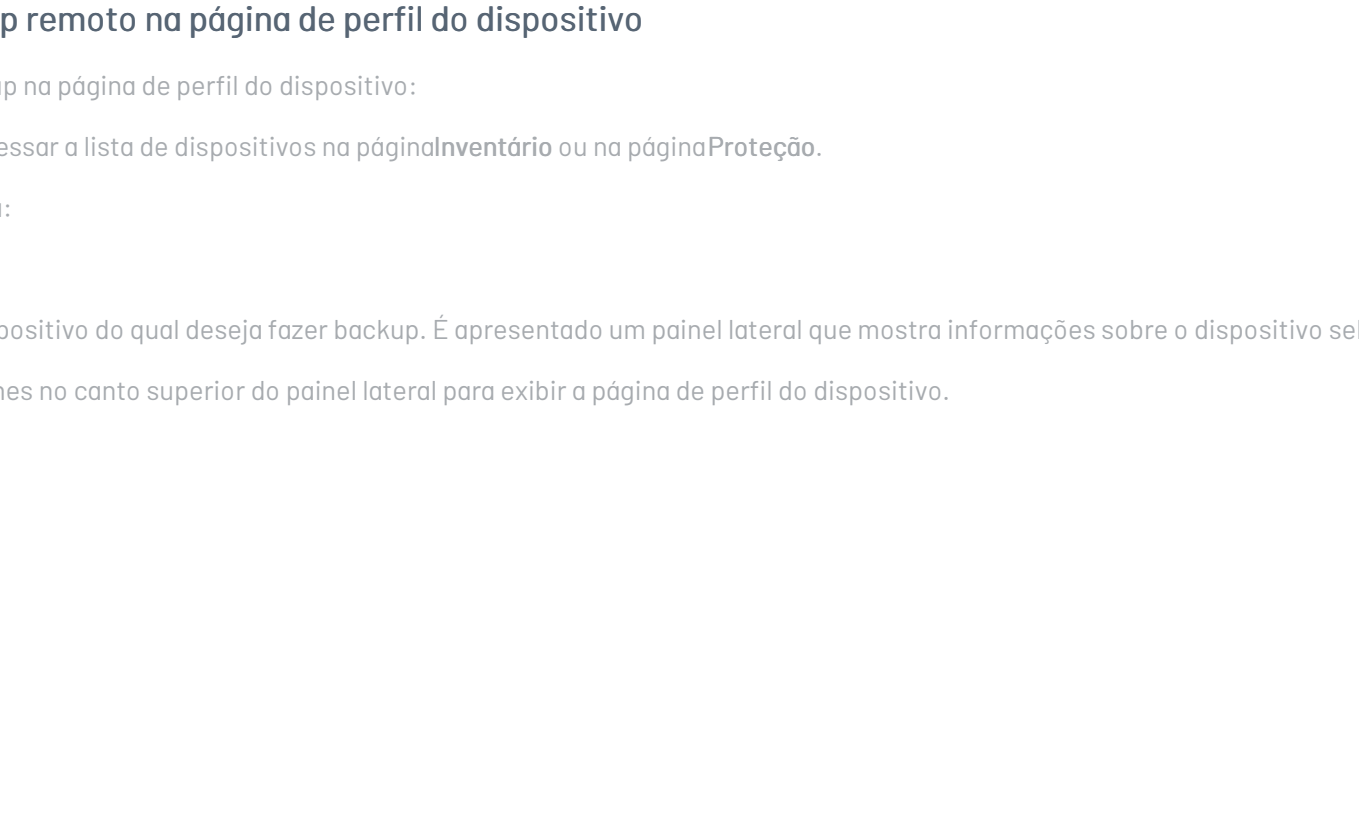


O software do Protection Agent (no dispositivo do usuário) usa a eliminação de duplicação para garantir que apenas dados novos ou alterados sejam copiados no repositório. A quantidade de tempo necessária para fazer backup de um dispositivo varia, dependendo da quantidade de dados que precisam ser indexados e copiados.

5. No painel lateral, clique no link ao lado da entrada**Último backup** para exibir um resumo do backup.



6. Para obter informações mais detalhadas sobre o backup, clique em**Exibir detalhes**. Em seguida, você pode exibir os detalhes do backup, o dispositivo, os arquivos que não puderam ser copiados e os dados de log.



Execute um backup remoto na página de perfil do dispositivo

Para executar um backup na página de perfil do dispositivo:

1. O primeiro passo é acessar a lista de dispositivos na página**Inventário** ou na página**Proteção**.

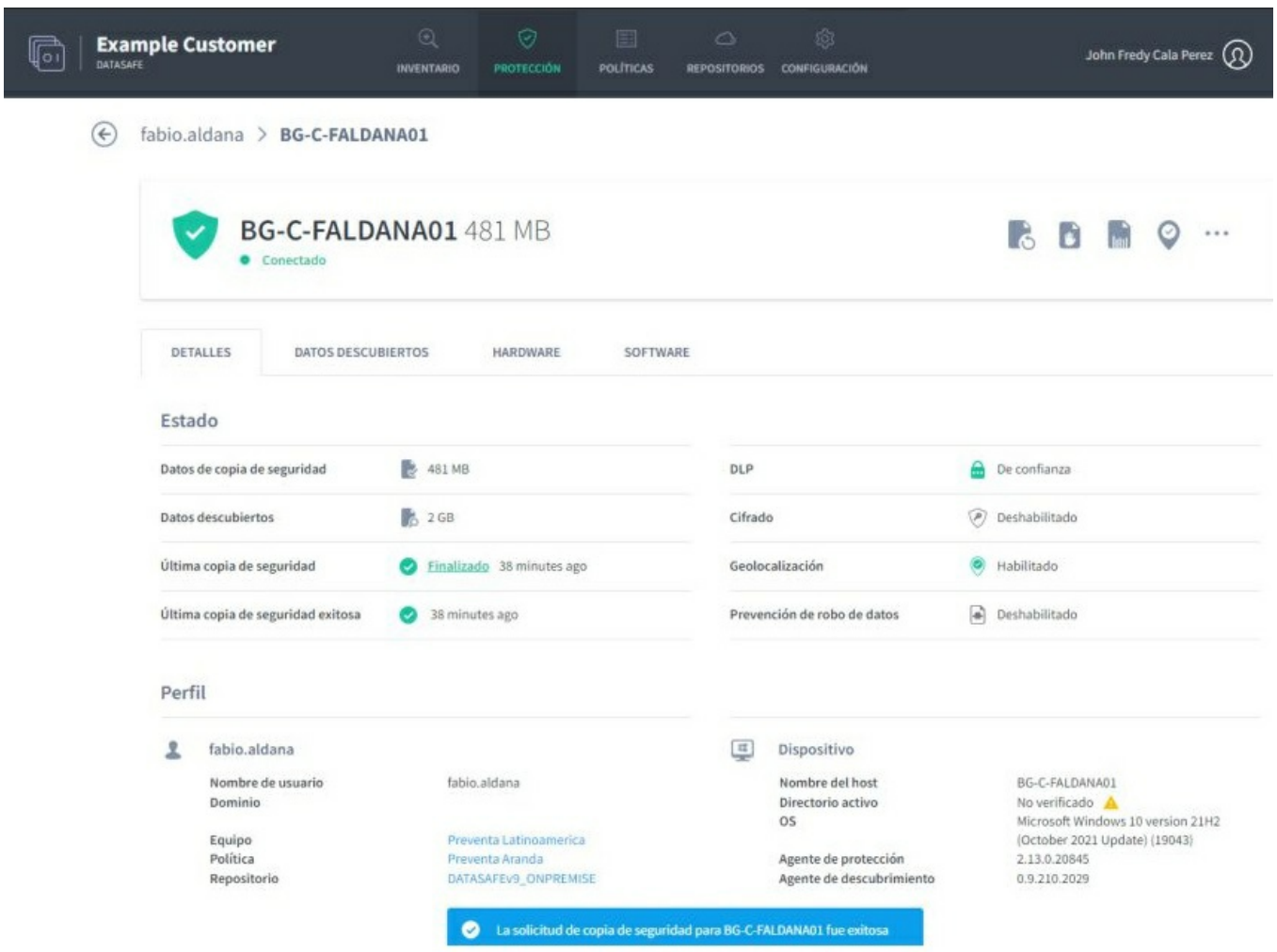
Clique em **Inventário**. Ou:

Clique em **Proteção**.

2. Na lista, clique no dispositivo do qual deseja fazer backup. É apresentado um painel lateral que mostra informações sobre o dispositivo selecionado.

3. Clique no ícone Detalhes no canto superior do painel lateral para exibir a página de perfil do dispositivo.

4. Na página de perfil do dispositivo, clique no ícone**Fazer backup agora**.

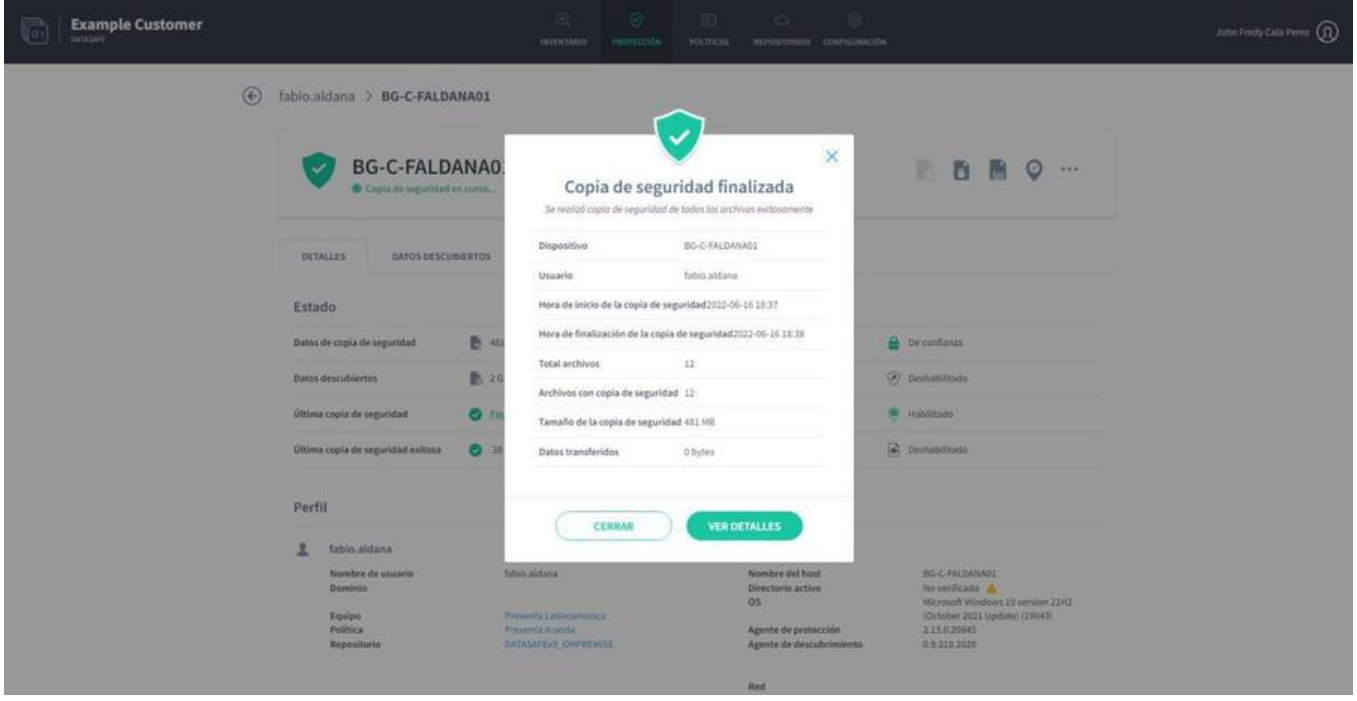


Uma mensagem é exibida na parte inferior da tela para informar que a solicitação de backup foi bem-sucedida.

O software do Protection Agent (no dispositivo do usuário) usa a eliminação de duplicação para garantir que apenas dados novos ou alterados sejam copiados no repositório. A quantidade de tempo necessária para fazer backup de um dispositivo varia, dependendo da quantidade de dados que precisam ser indexados e copiados.

5. Quando o backup estiver concluído, clique no link na entrada Último backup na guia Detalhes da página de perfil do dispositivo. O Aranda Datasafe exibe um resumo do backup.

6. Para obter informações mais detalhadas sobre o backup, clique em**Exibir detalhes**. Em seguida, você pode exibir os detalhes do backup, o dispositivo, os arquivos que não puderam ser copiados e os dados de log.



Executando o backup do agente

Existem três maneiras de fazer backup de seus dados no Aranda Datasafe:

1. O Aranda Datasafe faz backup de seus dispositivos ativados automaticamente, nos intervalos definidos nas Políticas para seus dispositivos (consulte Agendar backups automáticos).

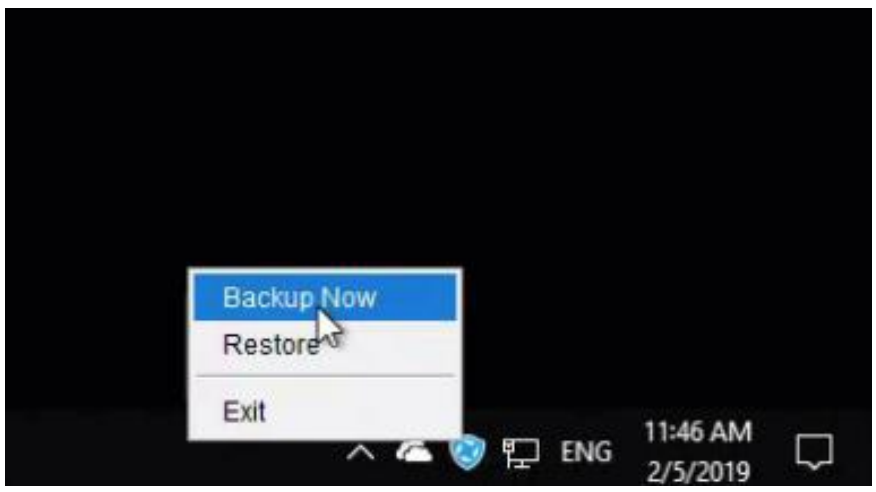
2. Você pode iniciar um backup manual remotamente do Aranda Datasafe (consulte Executar um backup remoto do Aranda Datasafe).

3. Você pode iniciar um backup manual de um dispositivo local ativado (veja abaixo).

Cada dispositivo ativado deve ter o software do Agente de Proteção instalado. Esse agente é necessário se você for executar um backup manual de um dispositivo local.

1. Clique com o botão direito do mouse no ícone do Protection Agent na bandeja do sistema do Windows.

2. Clique em Fazer backup agora para iniciar um backup.



Detalhes e logs de backup

Se a página Proteção mostrar que você tem dispositivos desprotegidos ou dispositivos protegidos com um aviso, você poderá encontrar mais informações no último log de eventos de backup do dispositivo. O Aranda Datasafe mantém um registro da última tentativa de backup para cada dispositivo conectado.

Para visualizar o histórico de backup e os registros de um dispositivo:

1. Clique em **Proteção**.

2. Na lista Dispositivos, clique em um dispositivo para exibir os detalhes do dispositivo em um painel deslizante.

3. Clique no ícone Exibir no canto superior do painel deslizante para exibir a página de perfil do dispositivo.

4. Na página Dispositivo, clique no link na entrada **Último backup** (na guia Detalhes).

5. Na caixa de diálogo de resumo do backup, clique em **Exibir detalhes** para exibir o log de backup do dispositivo.

6. Expanda as seções de log de backup para visualizar os detalhes do último backup.

Restaurar dispositivo

Importante: Você só pode restaurar dados do usuário e informações de perfil se os dados do usuário tiverem sido copiados para o Aranda Datasafe.

Se o Aranda Datasafe tiver backups de dados em máquinas protegidas, você poderá restaurá-los a qualquer momento. Normalmente, você usaria o recurso de restauração se:

- Você excluiu acidentalmente um arquivo protegido e deseja adicioná-lo novamente ao seu dispositivo
- Você tem um novo dispositivo e deseja baixar os dados protegidos que estavam anteriormente em um dispositivo diferente. Por exemplo, se você estiver substituindo um laptop antigo, poderá usar **Restaurar** para adicionar os arquivos protegidos do laptop antigo ao novo laptop.

Se a política tiver **migração** habilitada e a opção **Perfis de Usuário do Microsoft Windows** estiver selecionada, você também poderá restaurar as configurações do perfil de usuário.

Para **restaurar** arquivos em um dispositivo:

1. Faça login no dispositivo que receberá o backup dos dados do Aranda Datasafe.

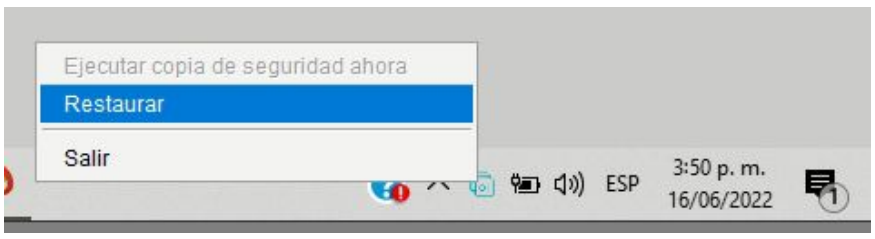
Se o seu dispositivo já tiver o Discovery Agent instalado, ignore as etapas 2 e 3 e continue a partir da etapa 4.

Se você precisar restaurar dados para um novo dispositivo ou um dispositivo que não tenha sido protegido pelo Aranda Datasafe antes, será necessário instalar o Discovery Agent. Continue a partir da etapa 2.

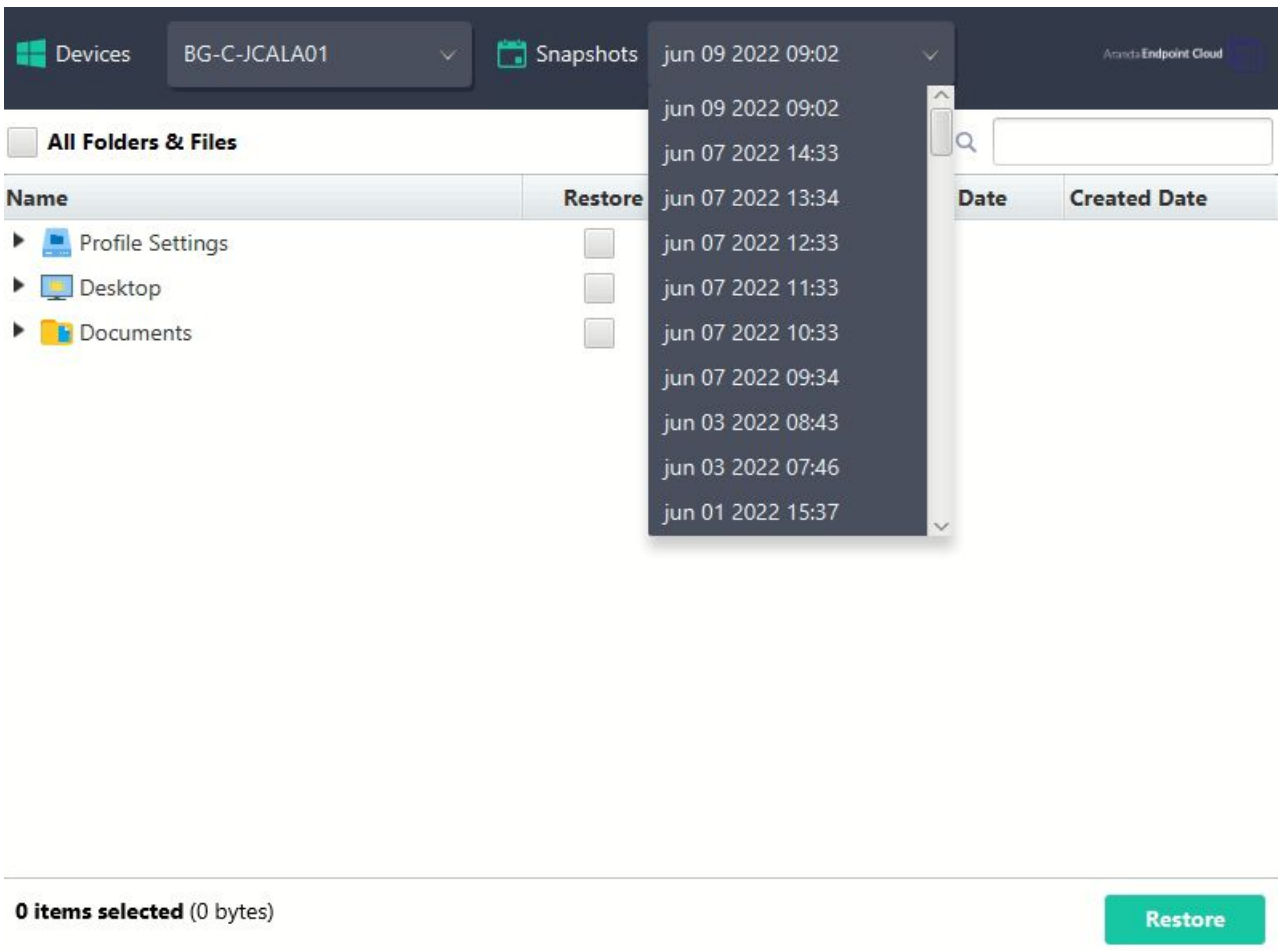
2. Instale o Discovery Agent no dispositivo, para que o Aranda Datasafe possa detectá-lo. Para obter mais informações, consulte Instalação e implantação do Discovery Agent.

3. No Aranda Datasafe, ative o novo dispositivo. Para obter mais informações, consulte Ativando seus dispositivos.

4. Na bandeja do sistema do Windows, clique com o botão direito do mouse no ícone do Agente de Proteção e selecione **Restaurar**.



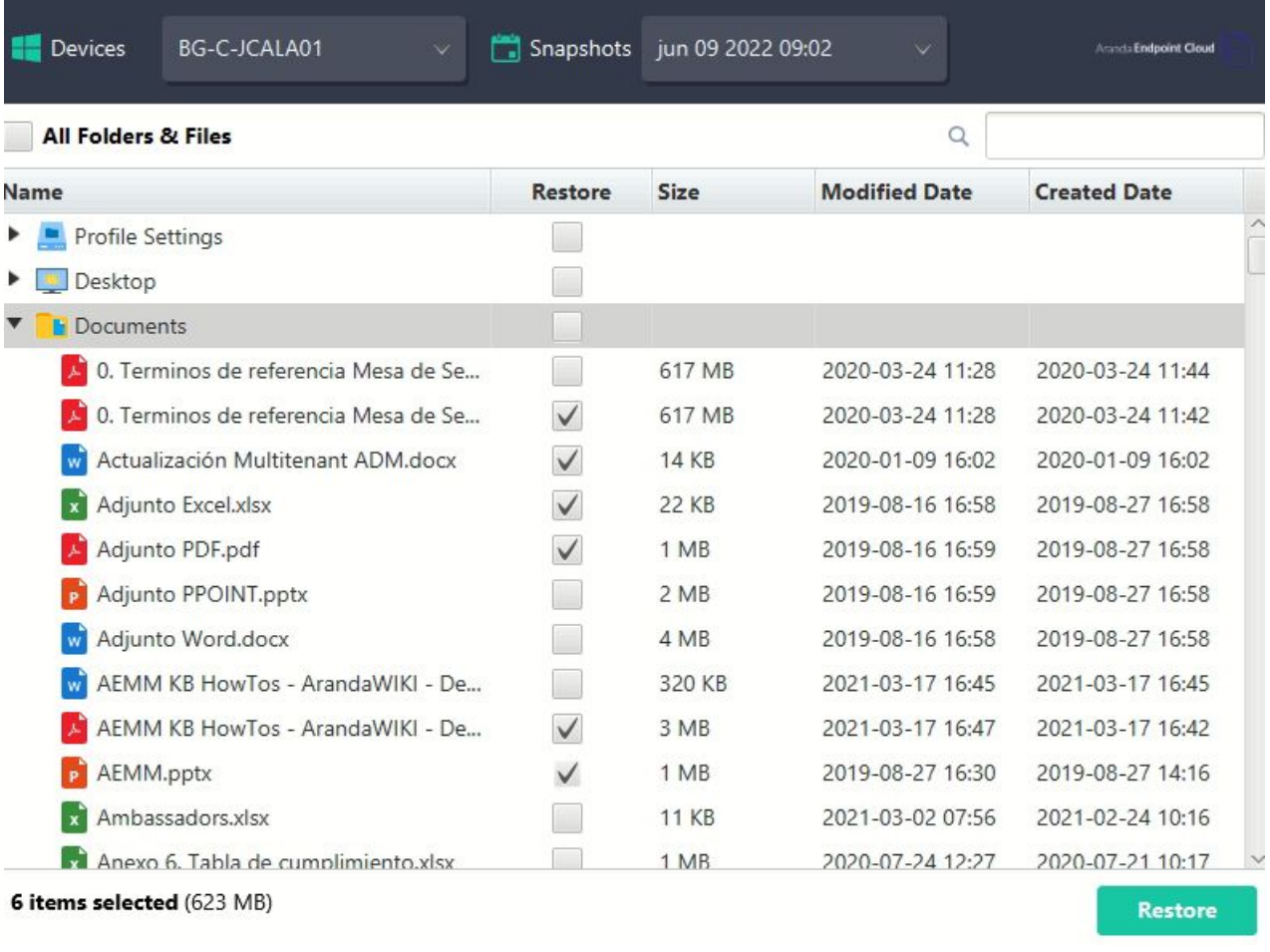
5. Na parte superior do Agente Aranda, escolha o dispositivo e o instantâneo associado que você deseja migrar para o novo dispositivo. O instantâneo é um registro dos dados de um dispositivo em um ponto específico no tempo, e você pode escolher qualquer um dos horários mostrados na lista.



6. Escolha quais arquivos deseja restaurar. Você pode escolher **Todas as pastas e arquivos**, todos os **arquivos da área de trabalho**, todos os documentos** ou todos os arquivos em volumes (unidades). Como alternativa, você pode selecionar arquivos individuais.

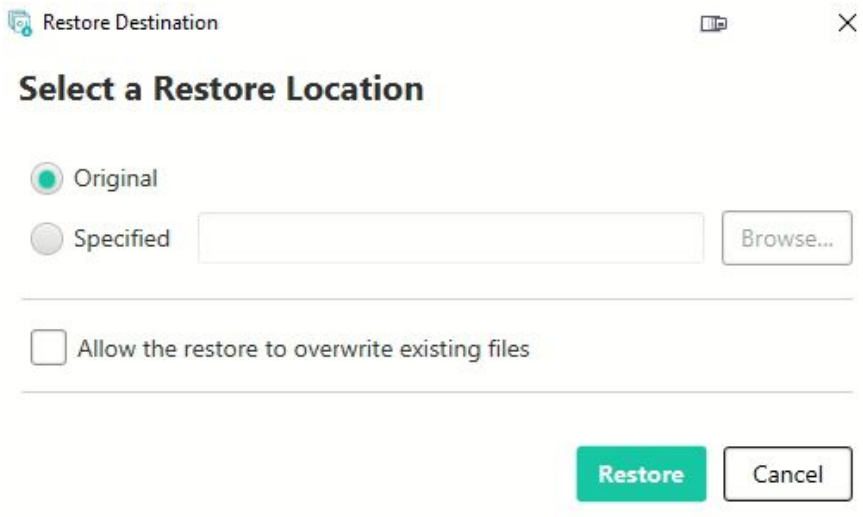
Se a política tiver **migração** habilitada e a opção **Perfis de Usuário do Microsoft Windows** estiver selecionada, você também poderá restaurar os dados do perfil do usuário. Selecione a opção **Configurações de perfil** para restaurar essas configurações.

Se o recurso de migração estiver desativado ou os perfis de usuário do Microsoft Windows não estiverem selecionados, você só poderá optar por restaurar os dados de backup.



7. Selecione **Restaurar**.

8. Escolha o local de restauração dos arquivos. Se você escolher**Original**, os arquivos serão enviados para o mesmo local que tinham no dispositivo anterior. Ou você pode escolher um local **especificado** diferente, se preferir.



9. Selecione **Restaurar**.

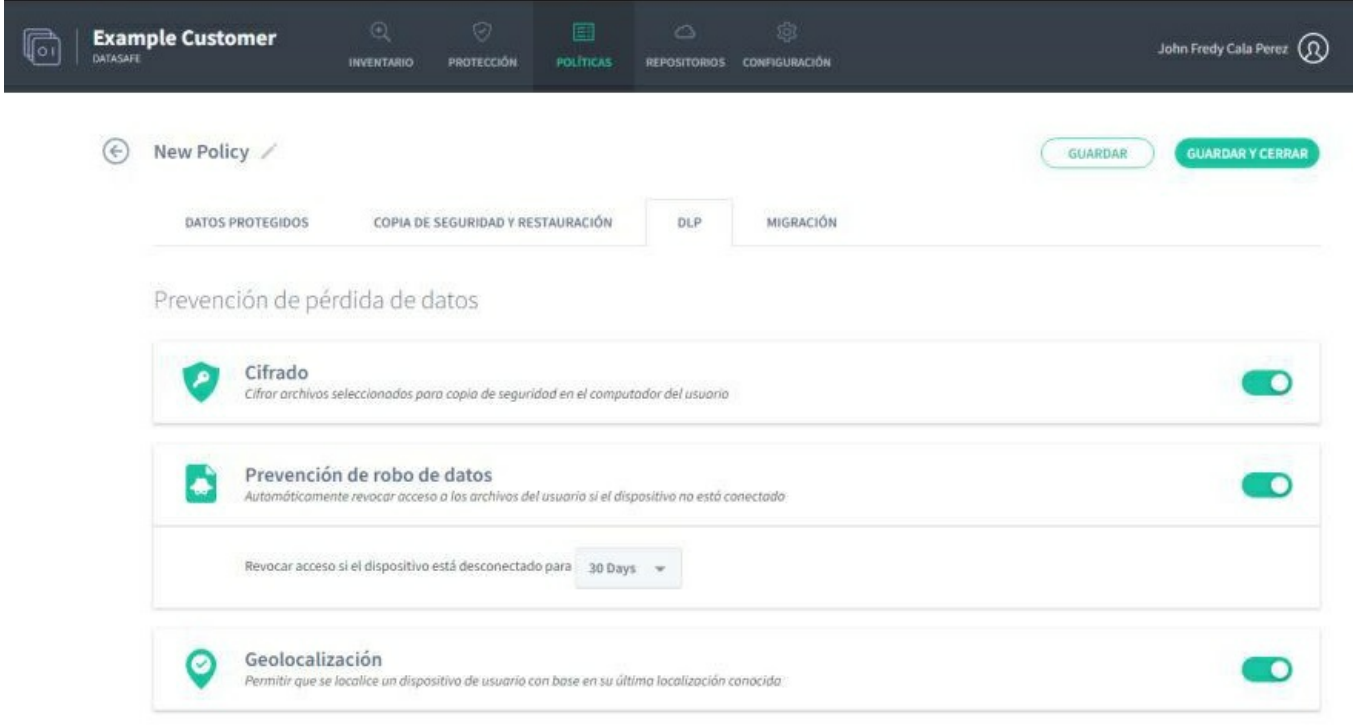
Os dados selecionados são baixados do Aranda Datasafe para o seu dispositivo. Se você escolheu arquivos da área de trabalho, eles aparecerão na área de trabalho.

Se você estiver restaurando dados de backup e configurações de perfil de usuário, a restauração será concluída em duas fases separadas.

Prevenção contra perda de dados

Prevenção contra perda de dados

O Aranda Datasafe possui muitos recursos de Prevenção de Perda de Dados (DLP) projetados para proteger os dados da sua empresa em caso de perda ou roubo de um de seus dispositivos.



Os recursos DLP permitem que você:

- Ative a criptografia de arquivos local. Isso criptografa os dados em seus dispositivos de usuário para garantir que a segurança e o acesso aos dados sejam controlados. Para obter mais informações, consulte Ativar criptografia local.
- Tenha prevenção automática de roubo de dados. Se um dispositivo for desconectado do Aranda Datasafe por um determinado período de tempo, o Agente Aranda impedirá o acesso aos dados criptografados no dispositivo. (Isso só se aplica quando a criptografia local está habilitada) Para obter mais informações, consulte Habilite a prevenção contra roubo de dados).
- Use a geolocalização para encontrar a última localização conhecida do dispositivo, com base em seu sinal wi-fi (consulteEncontrar dispositivos com geolocalização).
- Use o Aranda Datasafe paraApagar um dispositivo com segurança para que seus dados não existam mais no dispositivo.
- Use o Aranda Datasafe paraRevogar acesso para dados criptografados no dispositivo online (aplica-se apenas quando a criptografia local está ativada). Quando um dispositivo é revogado, seus dados criptografados não estão disponíveis, mas podem ser Cancelar se você quiser disponibilizar seus dados novamente.

Você pode ativar ou desativar os recursos DLP para cada política (consulte Ativar recursos de prevenção contra perda de dados).

Se um dos seus dispositivos estiver ausente ou roubado, consulte Se um dispositivo for perdido ou roubado.

Dispositivo perdido ou roubado

Se um dispositivo protegido pelo Aranda Datasafe for perdido ou roubado, você poderá:

Encontre o dispositivo

Se a Política do Dispositivo tiver a Geolocalização habilitada, você poderá usar o Aranda Datasafe para encontrar a última localização conhecida do dispositivo. A localização é mostrada no Aranda Datasafe em um mapa incorporado do Google. Esse recurso usa as conexões Wi-Fi do dispositivo para identificar o último local conhecido e, portanto, requer que o dispositivo esteja habilitado para Wi-Fi.

Para obter mais informações sobre geolocalização, consulteEncontrar dispositivos com geolocalização.

Revogue o dispositivo*

Se a política do dispositivo tiver a criptografia local habilitada, você poderá revogar o dispositivo. Essa pode ser uma boa opção se você suspeitar que um dispositivo foi perdido em vez de roubado.

Com uma revogação, você diz ao Aranda Datasafe para remover remotamente o certificado de criptografia do dispositivo. Assim que o agente recebe a instrução, o certificado é excluído e os dados criptografados no dispositivo não podem ser acessados ou usados. Portanto, qualquer pessoa que use o dispositivo não poderá acessar seus dados.

Você tem a opção de substituir a revogação posteriormente. A revogação colocará o certificado de criptografia de volta no dispositivo para disponibilizar os dados criptografados novamente.

Para obter mais informações, consulte:

- Revogar um dispositivo
- Revogar um dispositivo

Limpeza do dispositivo

Você pode usar o Aranda Datasafe para realizar uma "limpeza forense" do dispositivo. Apagar com segurança exclui os dados do seu dispositivo. Envolve uma

revogação do certificado de criptografia e uma série de exclusões que excluem os dados e, em seguida, os limpam novamente para remover quaisquer vestígios de seus dados.

Para obter mais informações, consulte Limpar um dispositivo remotamente.

⚐ >**Observação:** Você pode configurar o Aranda Datasafe para revogar automaticamente um dispositivo se o dispositivo não se conectar ao Aranda Datasafe dentro de um determinado período de tempo.

Ativar recursos de prevenção

Você pode editar uma política e ativar ou desativar cada um dos recursos DLP (Prevenção contra perda de dados) conforme necessário. Mas lembre-se de que as configurações de política se aplicam a todos os computadores que usam a política.

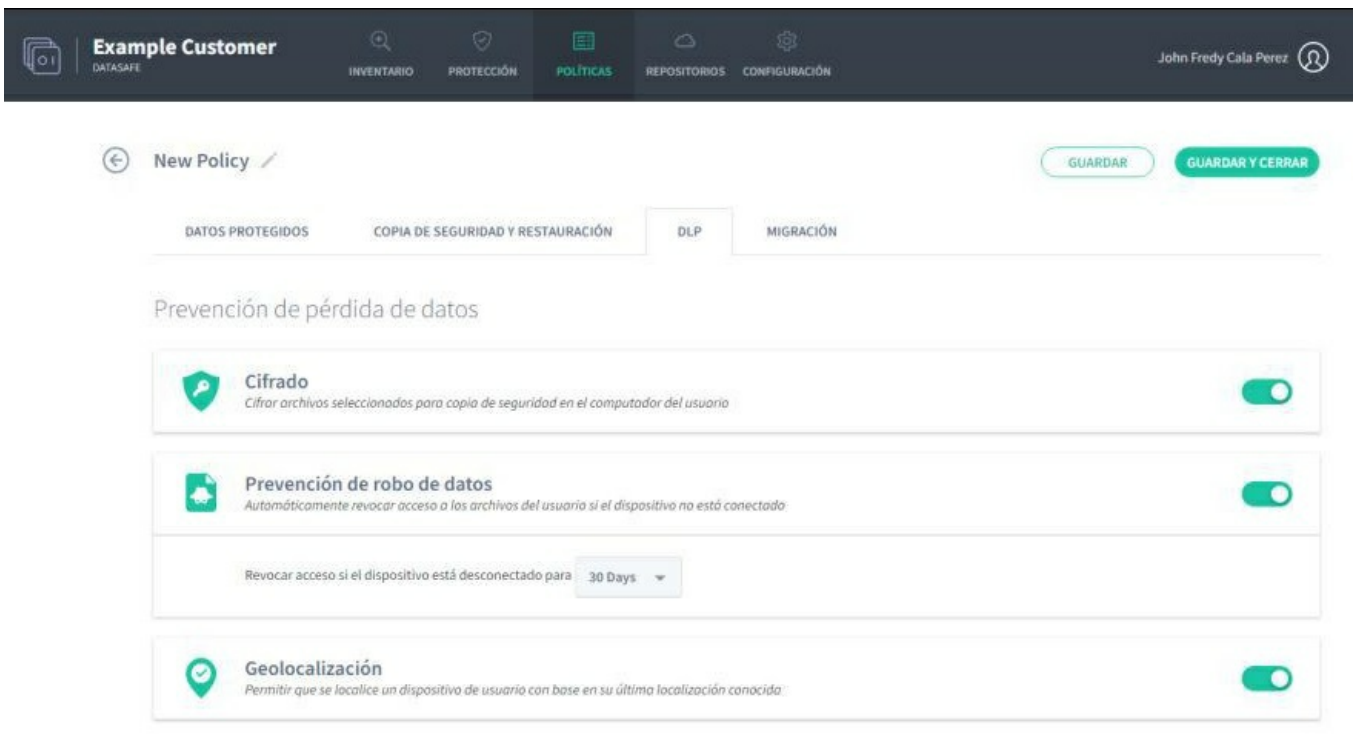
1. Clique em **Políticas**.

2. Clique na Política que deseja editar.

3. Clique na guia **DLP**.

4. Use os controles deslizantes para ativar ou desativar cada recurso DLP (verde está ativado, cinza está desativado).

5. Clique em **Salvar** ou **Salvar e fechar**.



Localizar dispositivos com geolocalização

Você pode usar a geolocalização para encontrar a última localização conhecida de um dispositivo, desde que:

- O dispositivo tem WI-FI ativado
- O recurso de **geolocalização** está habilitado na política (usada pela equipe do dispositivo).

Para descobrir o último local conhecido, o Aranda Datasafe se conecta ao Google Maps. A localização é estimada com base em:

- As coordenadas dos últimos pontos de acesso WI-FI que seu dispositivo localizou
- A intensidade do sinal do seu dispositivo para o ponto de acesso.

A localização é estimada com base no sinal WI-FI, não é necessário GPS.

Para usar a geolocalização do Aranda Datasafe para encontrar um dispositivo:

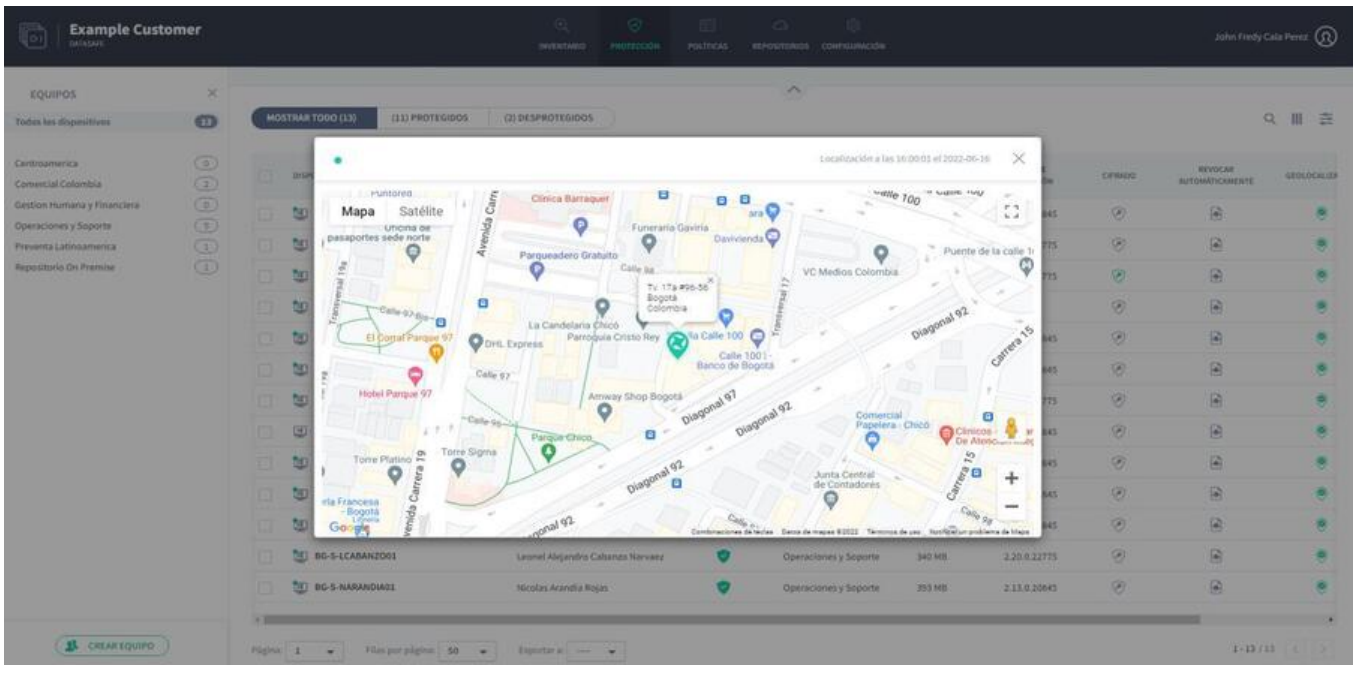
1. Clique em **Inventário** ou **Proteção**.

2. Na lista de dispositivos, clique no dispositivo que deseja localizar. Seu painel deslizante aparece.

3. Clique no ícone **Geolocalizar**.

O último local conhecido é mostrado em um mapa do Google. Você pode ampliar, diminuir o zoom e mostrar a visualização de satélite.

⚐ >Observação:** O ícone de geolocalização também está disponível na página de perfil do dispositivo (na página Inventário ou Proteção, exiba o painel deslizante do dispositivo e clique no ícone de detalhes da exibição para exibir a página de perfil do dispositivo).



Revogar acesso ao dispositivo

Se você habilitar a criptografia local em uma política, cada dispositivo que usa essa política receberá um certificado de criptografia. Quando um usuário faz logon em um dispositivo, ele só pode acessar os dados criptografados se o certificado estiver em vigor.

Se um dispositivo for perdido ou roubado, você pode usar o Aranda Datasafe para limpar remotamente o certificado do dispositivo. Depois que o certificado for excluído, qualquer pessoa, incluindo o usuário conectado, não poderá acessar os dados criptografados no dispositivo (já que o certificado não está no dispositivo).

Usar o Aranda Datasafe para excluir um certificado é conhecido como "revogar um dispositivo".

Para revogar um dispositivo:

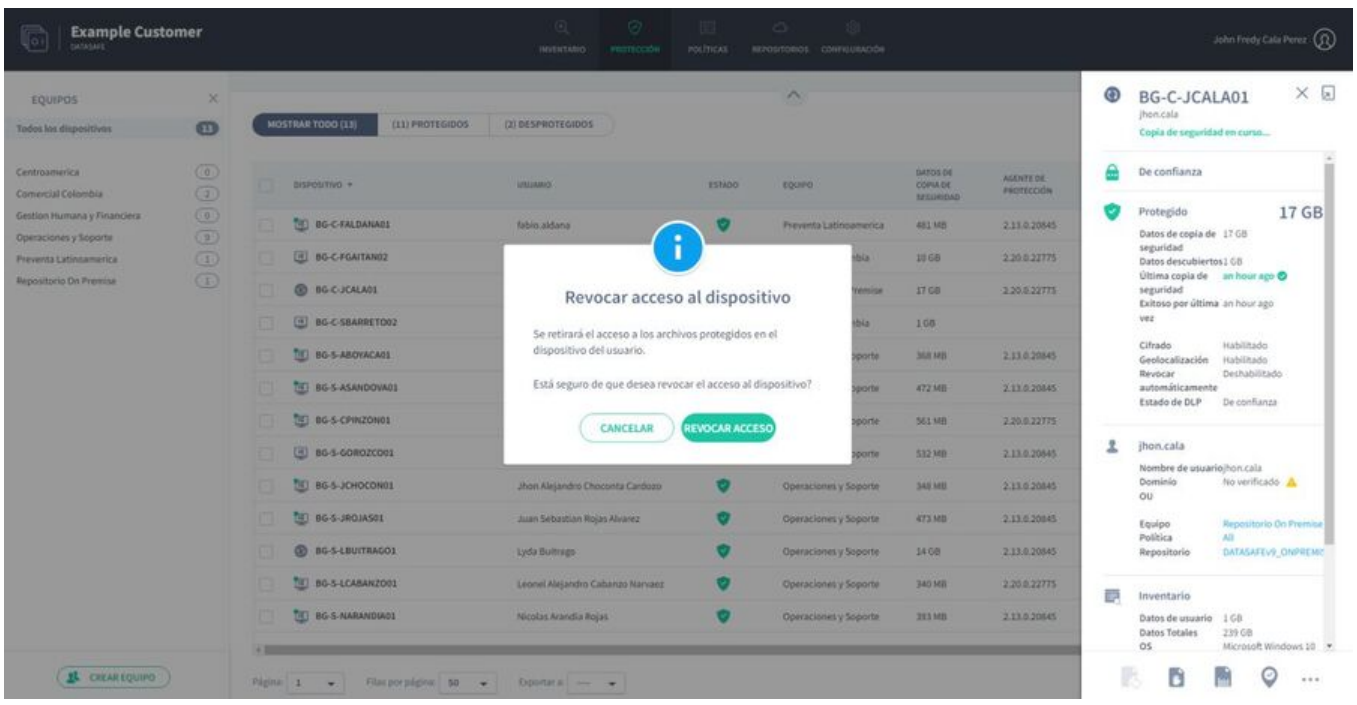
1. Clique em **Inventário** ou **Proteção**.

2. Na lista de dispositivos, clique no dispositivo que deseja revogar. O painel deslizante do seu dispositivo é exibido.

3. Clique no ícone **Revogar dispositivo**.

⚐ > Observação: O ícone Revogar dispositivo também está disponível na página de perfil do dispositivo (na página Inventário ou Proteção, exiba o painel lateral do dispositivo e clique no ícone de exibição de detalhes para exibir a página de perfil do dispositivo).

4. Clique em Revogar para confirmar. A solicitação para revogar o dispositivo é feita. Você pode cancelar a solicitação de revogação, se necessário (exiba o painel deslizante do dispositivo ou a página do dispositivo e clique no ícone Cancelar revogação).



⚐ > Observação: Se a revogação automática estiver habilitada em uma política, o Aranda Datasafe revogará automaticamente o certificado de qualquer dispositivo protegido que não se conecte ao Aranda Datasafe dentro de um período de 30 dias. (Você pode alterar o período de revogação automática nas configurações de política.)

Exclusão remota no dispositivo

Se você deseja excluir arquivos de um dispositivo que está ausente ou roubado, pode usar o recurso **Apagar**. Isso remove completamente os arquivos protegidos do dispositivo (ao contrário de Revogar, que deixa os arquivos no lugar, mas os torna inacessíveis).

Com uma limpeza, use o Aranda Datasafe para realizar um "apagamento forense" remoto, que remove arquivos protegidos no dispositivo. Como parte do "apagamento forense", o Aranda Datasafe remove o certificado de criptografia e executa uma série de exclusões adicionais para remover completamente quaisquer vestígios dos dados protegidos do dispositivo.

Para apagar um dispositivo:

1. Clique em **Inventário** ou **Proteção**.

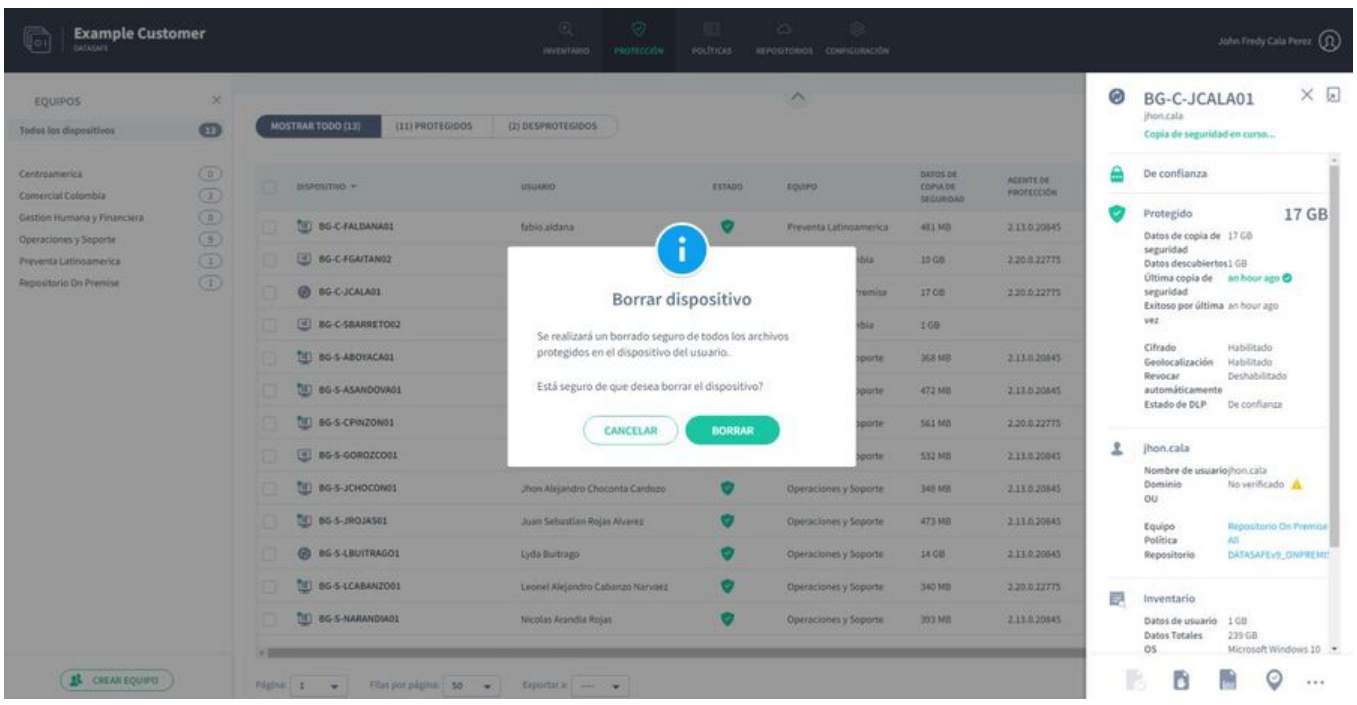
2. Na lista de dispositivos, clique no dispositivo que deseja apagar.

3. Clique no ícone **Excluir**.

4. Clique em **Excluir** para confirmar. A limpeza é definida como pendente e, após um pequeno atraso, a limpeza começa. Enquanto a limpeza estiver pendente, você pode cancelá-la (clique no ícone **Cancelar apagar** no painel deslizante do dispositivo ou na página Dispositivo). Quando a limpeza for iniciada, ela não poderá ser cancelada.

A quantidade de tempo que leva para concluir o apagamento varia, dependendo do tamanho e da velocidade do disco.

⚐ > Observação: O ícone de limpeza também está disponível na página de perfil do dispositivo (na página Inventário ou Proteção, exiba o painel deslizante do dispositivo e clique no ícone de detalhes da exibição para exibir a página de perfil do dispositivo).



Substituir revogação de dispositivo

No Aranda Datasafe, você pode revogar um dispositivo para que seus arquivos protegidos fiquem inacessíveis. Isso é para manter seus dados seguros em caso de perda ou roubo de um dispositivo. Se o dispositivo for encontrado, você poderá tornar os dados acessíveis novamente usando **Substituir**.

Com uma substituição de revogação, o Aranda Datasafe coloca o certificado de criptografia de volta no dispositivo revogado. Depois que o certificado estiver no dispositivo, ele não poderá ser revogado e seus dados protegidos poderão ser acessados.

Para revogar um dispositivo:

1. Clique em **Inventário** ou **Proteção**.

2. Na lista de dispositivos, clique no dispositivo que deseja revogar. O painel deslizante do seu dispositivo é exibido.

3. Clique no ícone **Cancelar revogação do dispositivo**.

4. Clique em **Cancelar revogação** para confirmar. A solicitação para revogar o dispositivo é feita e a revogação está pendente. Quando o Aranda Datasafe conclui o aplicativo, a revogação é concluída.

Enquanto a revogação estiver pendente, você pode cancelar a solicitação de revogação, se necessário (exiba o painel deslizante do dispositivo ou a página do dispositivo e clique no ícone **Cancelar Cancelamento de Revogação**).

Status de prevenção contra perda de dados

Você pode exibir o status de **DLP** na seção **Proteção**. Mostra o número de dispositivos que têm recursos de criptografia local, revogação automática e geolocalização habilitados (na Política).

O status DLP também é exibido na lista de dispositivos na parte inferior da seção **Proteção**.

Migração remota

Migração remota

Nossa solução de migração remota de dispositivos transfere todos os dados do usuário e configurações de perfil para a nova máquina, enquanto o usuário trabalha. A transferência de dados é totalmente segura e você não corre o risco de perder nenhum arquivo do usuário.

A equipe de TI pode gerenciá-lo remotamente e os usuários podem simplesmente começar a usar a nova máquina com todas as suas configurações e arquivos

exatamente como estavam em seu computador antigo.

- Ative e monitore remotamente várias migrações do Aranda Datasafe
- Migração de dispositivo para dispositivo (sem necessidade de armazenamento adicional no repositório)
- Melhor descoberta de caminho de rede
- Abrir/fechar automaticamente o firewall do Windows
- Migrações ao vivo (inicial completa e atualizações para o seguinte)
- Capacidade de repetição de conexão
- Compactação e criptografia
- Migrar todos os dados (incluindo comerciais e pessoais)
- Migração de acesso direto para novos locais
- Migrar locais de unidade de nuvem (não configuração)

- Migração de perfil
    - Configurações da barra de tarefas, opções de pasta do Windows, unidades de rede
    - Microsoft Outlook: Todas as contas de e-mail, arquivos PST, assinatura de e-mail.

Preparação para migração remota

Antes de migrar, as seguintes verificações são necessárias:

As máquinas de origem e destino devem estar preparadas

- Ambas as máquinas devem estar no status **Ativo** e visíveis na janela **Proteção** no Aranda Datasafe.
- O usuário relevante deve fazer login em ambas as máquinas.
- A máquina de destino deve ter o Windows e os aplicativos instalados antes da migração. Muitos clientes usam uma imagem padrão da empresa para suas máquinas.

Preparando o dispositivo de destino

- Deve haver tamanho de disco suficiente no dispositivo de destino.
- É importante que a configuração ou partição do disco seja a mesma em ambos os dispositivos. Se o dispositivo de origem tiver um C:\&D://volume, por exemplo, e o dispositivo de destino tiver apenas um volume C:\, a migração dos dados para D:\ falhará.
- Certifique-se de que aplicativos como MS Office, antivírus e outros aplicativos da empresa estejam instalados antes de executar a migração. As informações de **Inventário** no Aranda Datasafe mostrarão todos os aplicativos instalados no dispositivo **Origem**.
- Descubra e ative o dispositivo de destino no Aranda Datasafe se ele ainda não estiver ativo e visível na janela Proteção.

O que posso esperar da migração?

O recurso de migração remota completa copiará todos os dados do usuário e configurações de perfil para o dispositivo de destino.

O que será incluído nas configurações do perfil?

- Perfil de e-mail para Microsoft Outlook
- Assinaturas de e-mail
- Arquivos de armazenamento de e-mail (arquivos PST)
- Localizações de unidades mapeadas
- Impressoras de rede
- Visualizações de pastas personalizadas
- Preferências da barra de tarefas

O que será excluído da migração?

-Aplicativos

- Arquivo interno exclui como executáveis, arquivos do sistema e arquivos temporários
- Os arquivos bloqueados serão excluídos
- Discos e volumes que não existem no dispositivo de destino
- A migração falhará se o tamanho do disco de destino for menor
- Impressoras conectadas localmente não serão incluídas
- O plano de fundo da área de trabalho não será migrado

Executando a migração remota

Inicie uma migração do Aranda Datasafe

1. Navegue até Proteção no Aranda Datasafe.

2. Use a função de pesquisa no painel da lista de dispositivos e procure o usuário que deseja migrar.

3. A pesquisa deve resultar em pelo menos dois dispositivos para o usuário. O dispositivo atual e o novo dispositivo

4. Clique no dispositivo de destino para abrir o painel lateral.

5. Clique nos 3 pontos no canto inferior direito do painel lateral e selecione Migrar.

6. Selecione o dispositivo do qual migrar no menu suspenso e continue.

7. A migração começará e mostrará o progresso.

Monitoramento

Depois de iniciar a migração, o administrador pode continuar monitorando o progresso do Aranda Datasafe. A janela pode fechar enquanto outras tarefas de gerenciamento estão sendo executadas.

O administrador pode verificar o progresso da migração a qualquer momento, clicando em qualquer um dos dispositivos envolvidos na migração e abrindo os detalhes do evento no painel lateral.

Executar uma migração de atualização

Depois que a migração remota completa inicial for concluída, há mais algumas etapas antes de entregar o dispositivo de destino ao usuário:

- Caso um usuário esteja trabalhando na máquina de origem durante a execução da migração, alguns arquivos podem estar bloqueados. Isso ficará visível nos detalhes do evento de migração.
- É importante que o usuário feche todos os aplicativos durante a migração de atualização (posteriormente).
- No Aranda Datasafe você pode iniciar outra migração. Isso migrará todos os dados que estavam em uso pelo usuário no momento da execução inicial da migração.
- Depois que a migração de atualização for concluída com êxito, você poderá executar um logout/login para aplicar as configurações de perfil ao novo dispositivo.
- Certifique-se de aplicar outras configurações que não são cobertas pelo recurso de migração remota completa.
- Dê o novo dispositivo ao usuário e confirme com ele se tudo foi migrado.

Detalhes do evento

Quando a migração remota completa for concluída, você poderá exibir os resultados e os detalhes do evento de migração. Selecione o dispositivo de destino no Aranda Datasafe e clique no nome do dispositivo ao lado de Migrado de.

As seguintes informações serão exibidas:

- Horários de início e término
- Número de arquivos migrados
- Tamanho da migração
- Arquivos bem-sucedidos versus com falha com motivos de falha

Migração

O recurso de migração do Aranda Datasafe facilita a transferência das configurações do perfil do usuário de um dispositivo para outro. O uso do recurso de migração pode economizar muito tempo e esforço quando você precisar atualizar ou substituir seus dispositivos.

Migrando configurações de perfil

Com o recurso de migração de configurações de perfil, você pode fazer backup dos dados do usuário e das configurações de perfil em um dispositivo no Aranda Datasafe. Em seguida, você pode restaurá-los em outro dispositivo. Isso torna mais fácil e rápido transferir dados comuns do usuário, como atalhos da área de trabalho, arquivos da área de trabalho, documentos etc.

Para usar o recurso de migração, você deve [habilitá-lo na Política] que o dispositivo que deseja substituir usa.

Quando a migração estiver habilitada, o Aranda Datasafe fará backup dos dados do usuário e das configurações do perfil. Isso ocorre ao mesmo tempo que o próximo backup de dados corporativos (conforme definido na Política).

Quando os dados e as configurações de perfil do usuário tiverem sido copiados, você poderá restaurá-los em um novo dispositivo.

Exemplo: Digamos que você tenha um laptop com backup e protegido pelo Aranda Datasafe. O laptop será substituído por um modelo mais novo.
Use o recurso de migração para fazer backup dos dados do usuário e das configurações de perfil do laptop atual.

Quando o novo laptop chegar, você descobrirá e ativará o dispositivo no Aranda Datasafe. Em seguida, use o recurso Restaurar para transferir os dados do usuário e as configurações de perfil do laptop antigo do Aranda Datasafe para o novo laptop.

Seu novo laptop é atualizado com dados do usuário e configurações de perfil (perfil e assinaturas do Outlook, unidades de rede mapeadas e várias configurações de pasta e barra de tarefas, etc.).

Ativar recurso de migração de perfil de usuário

Você pode usar o recurso de migração de perfil de usuário no Aranda Datasafe para fazer backup das informações de perfil de usuário do Windows em um dispositivo. Você pode então transferir as informações para um dispositivo diferente executando uma restauração.

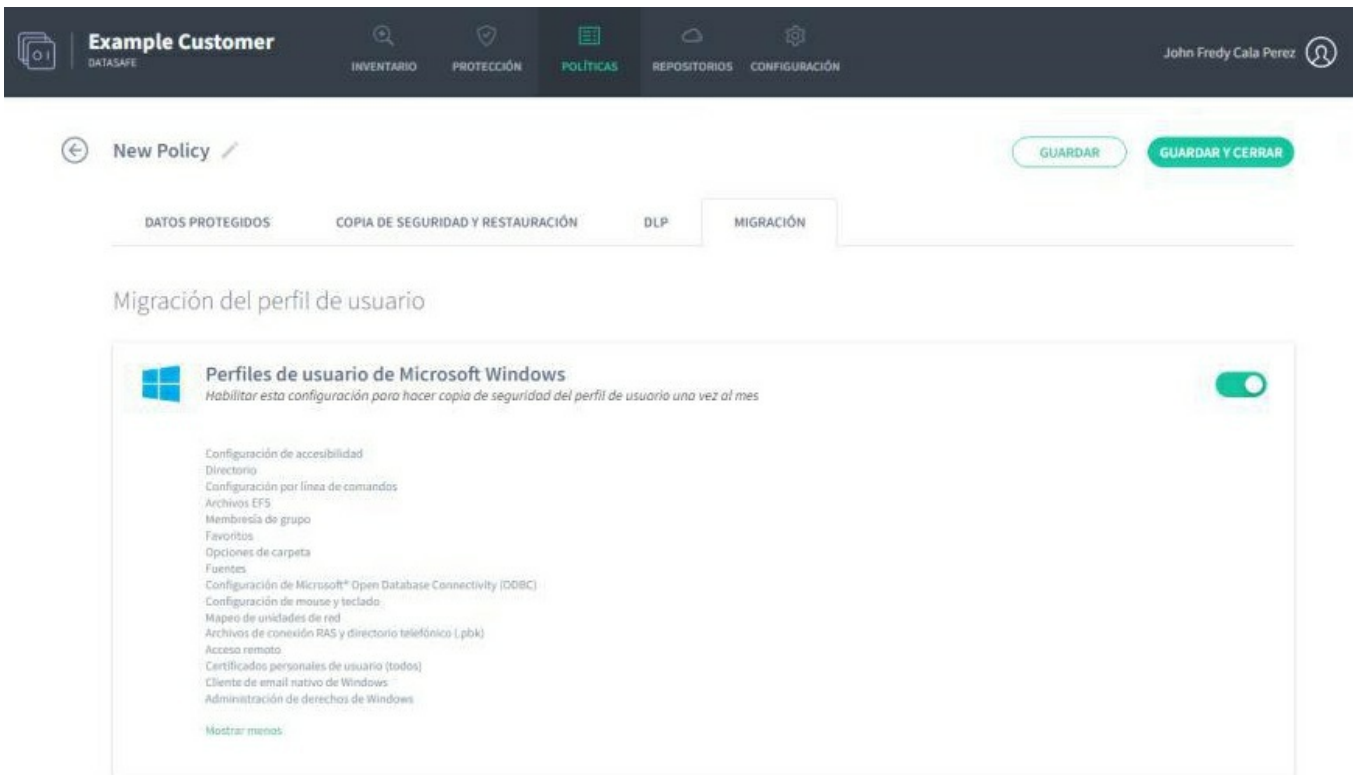
Para usar a migração de perfil, ative-a na Política usada pelo dispositivo do qual você deseja fazer backup:

1. Clique em **Políticas**.

2. Edite a política associada ao computador ao qual o dispositivo pertence.

3. Clique em **Migração**.

4. Use o controle deslizante para ativar a migração de perfil para perfis de usuário do Microsoft Windows. (Verde está ativado, cinza está desativado.)



4. Clique no link **Mostrar mais** para ver uma lista completa das informações do perfil de usuário do Windows que serão copiadas. Inclui layout da barra de tarefas, unidades de rede mapeadas, opções de pasta, contas de e-mail, arquivos pst anexados anteriormente e assinaturas de e-mail.

5. Clique em Salvar e Fechar.

O Aranda Datasafe fará backup dos dados do usuário e das configurações de perfil em todos os dispositivos associados a esta Política. O backup do perfil será executado quando o próximo backup dos dados corporativos for feito (conforme agendado na Política). Ele será executado uma vez a cada 30 dias para garantir que seja atualizado regularmente.

Quando um backup for feito, você poderá migrar o[Configurando para um novo dispositivo](#) .

Desativar recurso de migração de perfil de usuário

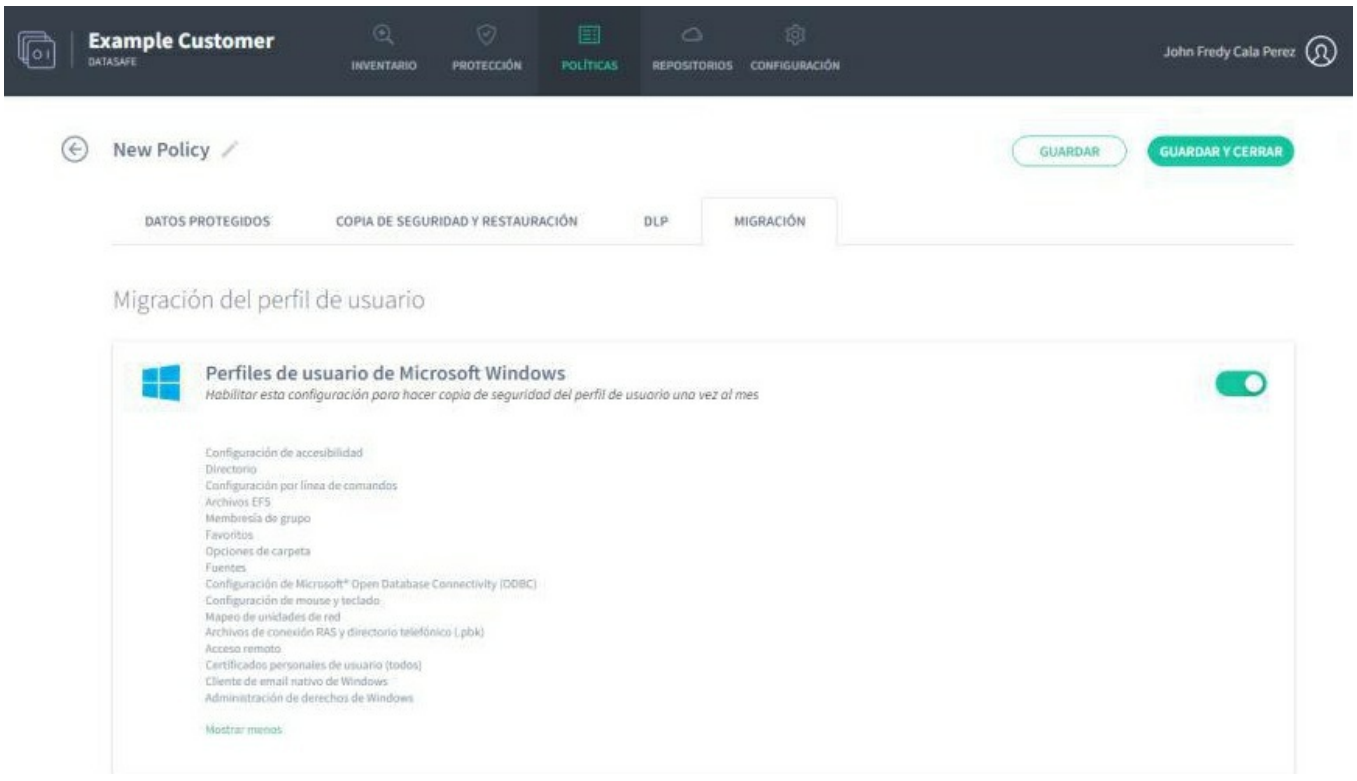
Para desativar o recurso de migração de perfil de usuário para que o Aranda Datasafe não faça backup dos dados de perfil de usuário do Windows:

1. Clique em **Políticas**.

2. Edite a política associada ao computador ao qual o dispositivo pertence.

3. Clique em **Migração**.

4. Use o controle deslizante para desativar a migração de perfil para perfis de usuário do Microsoft Windows. (O cinza está desligado, o verde está desligado.)



5. Clique em Salvar e Fechar.

O Aranda Datasafe **não** fará backup dos dados e perfis do usuário em todos os dispositivos associados a esta Política.

Migrar dados de perfil de usuário para o dispositivo

Se você tiver habilitado a migração em uma política, poderá usar a restauração para transferir dados de perfil de usuário do Windows (e dados de backup) de um dispositivo antigo para um novo dispositivo (via Aranda Datasafe).

⚐ > Observação: você só pode restaurar os dados do perfil do usuário de outro dispositivo se a migração estiver ativada e o backup do dispositivo "antigo" tiver sido feito. Para saber como habilitar o recurso de migração, consulte Habilitar o recurso de migração.

Para **restaurar** arquivos em um dispositivo:

1. Faça login no novo dispositivo.

Se o seu dispositivo já tiver o Discovery Agent instalado, ignore as etapas 2 e 3 e continue a partir da etapa 4.

Se você precisar restaurar dados para um novo dispositivo ou um dispositivo que não tenha sido protegido pelo Aranda Datasafe antes, será necessário instalar o Discovery Agent. Continue a partir da etapa 2.

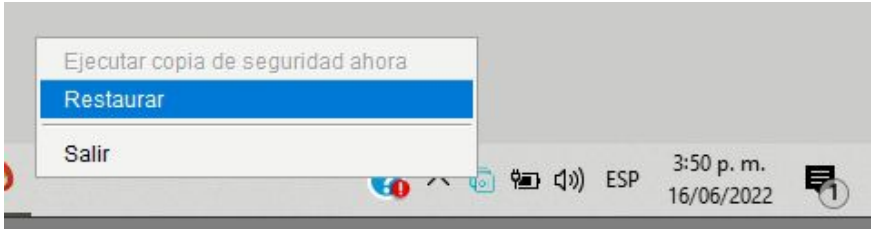
2. Instale o Discovery Agent no dispositivo, para que o Aranda Datasafe possa detectá-lo. Para obter mais informações, consulteInstalação e implantação do Discovery Agent.

3. Na Aranda Datasafe, Ative o novo dispositivo.

Para obter mais informações, consulte Ativando seus dispositivos.

⚐ > Nota: O Aranda Datasafe usa a conta de usuário do Windows no novo dispositivo para identificar qual dispositivo antigo está sendo substituído. Atribui automaticamente o novo dispositivo à mesma equipe e perfil do dispositivo antigo.

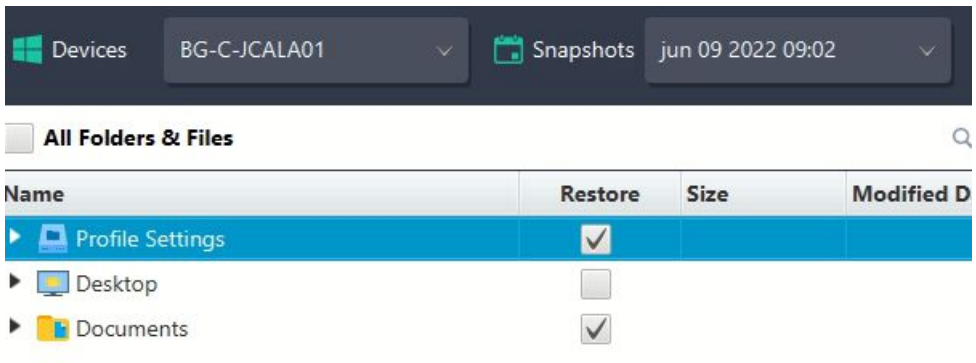
4. Na barra de tarefas do Windows, clique com o botão direito do mouse no ícone do Agente de Proteção e selecione Restaurar.

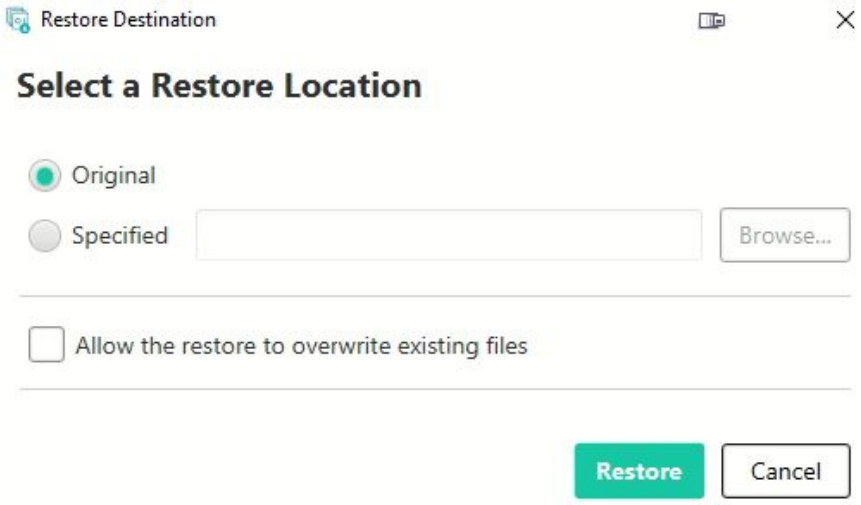


⚐ > Observação: Se o ícone do Agente de Proteção não for exibido, encontre o aplicativo Agente de Proteção no seu dispositivo e inicie-o.

5. Escolha os dados que deseja migrar e o local dos dados migrados.

- Use a opção Dispositivos para escolher o dispositivo "antigo" que possui os dados que você deseja migrar para o "novo" dispositivo.
- Use a opção Snapshots para escolher o snapshot que deseja migrar para o novo dispositivo. Um instantâneo é um registro dos dados de um dispositivo em um ponto específico no tempo. Na maioria dos casos, você desejará selecionar o instantâneo mais recente.
- Use as caixas de seleção Restaurar para escolher os dados a serem migrados. Selecione todos os dados que deseja restaurar e também as Configurações de Perfil (Perfil de Usuário do Windows).
- Clique em Restaurar.
- Escolha Restaurar local para os dados migrados no novo dispositivo. Você pode escolher Original para migrar os dados para o mesmo local que tinha no dispositivo anterior ou escolher Especificado para definir um local diferente.





1. Clique em Restaurar.

Os dados do usuário selecionados e as informações do perfil são baixados do Aranda Datasafe para o seu novo dispositivo. Se você escolheu arquivos da área de trabalho, eles aparecerão na área de trabalho.