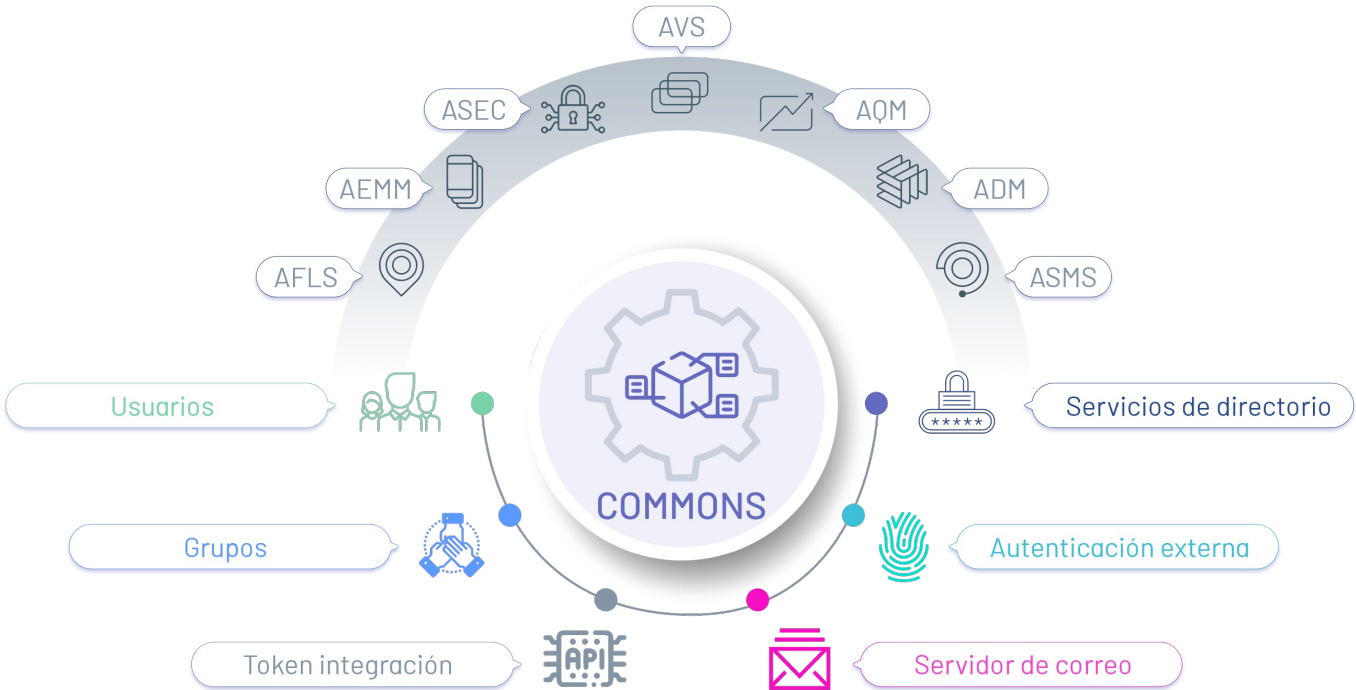




Configuración de Commons

Nos processos de configuração das diferentes aplicações Aranda, existem conceitos e funcionalidades transversais que permitem a racionalização e partilha de dados relacionados para cada projeto.

Aranda COMMONS é uma biblioteca que compartilha componentes ou módulos transversais para os processos gerais de configuração dos produtos Aranda, como ASEC, AVS, AFLS, ADM, AQM.



2. Módulos

Os seguintes módulos de configuração comuns integram-se nativamente às nossas soluções:

Módulos comuns	Implementado em:
	 
	 
	 
	   
	   
	

Para quem é este Manual?

Este manual foi desenvolvido para usuários de produtos Aranda que compartilham diferentes módulos de configuração transversal Aranda COMMON.

O que é a nossa documentação?

Módulos de configuração

Módulos comuns

O administrador geral do console Web poderá executar as seguintes tarefas de configuração de passagem:



1. Usuários

Neste módulo você poderá configurar os usuários responsáveis pelos diferentes processos de gestão dos produtos Aranda. Essas configurações só podem ser feitas por um usuário com uma função de administrador. Além disso, você pode associar grupos e funções.

Para obter mais informações, consulte o [Gerenciamento de usuários ↗](#).

2. Grupos de usuários

Neste módulo, você poderá configurar e gerenciar grupos de usuários para realizar a atribuição de funções de maneira mais eficiente.

Para obter mais informações, consulte o [Gestão de ↗ Grupos](#).

3. Servidor de e-mail

Neste módulo você poderá configurar um provedor de e-mail para a operação dos produtos Aranda; As notificações serão enviadas aos usuários deste servidor. O e-mail está configurado para poder executar a recuperação de senha para usuários que foram criados manualmente (não se aplica àqueles que são importados).

Para obter mais informações, consulte o [Gerenciamento de servidor de ↗ e-mail](#).

4. Serviços de Diretório

Neste módulo, você pode definir os serviços de diretório que podem ser usados em um aplicativo Aranda, como o protocolo de acesso ao diretório leve LDAP, que permite configurar a conexão com outros diretórios de negócios ou com o serviço de diretório Azure Active Directory

Para obter mais informações, consulte o [Serviços de diretório ↗ de gerenciamento](#).

5. Provedores de autenticação

Neste módulo, você pode definir os provedores de autenticação externa, que seguem o padrão SAML (Security Assertion Markup Language) para executar a autenticação do usuário no aplicativo. e subsequente e notificação sobre o status da validação.

Para obter mais informações, consulte o [Gerenciamento do provedor de ↗ autenticação](#).

6. Tokens de integração

Neste módulo, você poderá realizar a configuração de conexão da API e adicionar detalhes para a criação do Token. Esse token permite que as APIs do produto que o requer sejam consumidas, a partir de aplicações externas, sem a necessidade de credenciais de autenticação.

Para obter mais informações, consulte o [Gerenciamento de token de integração ↗](#).

Ambiente Commons

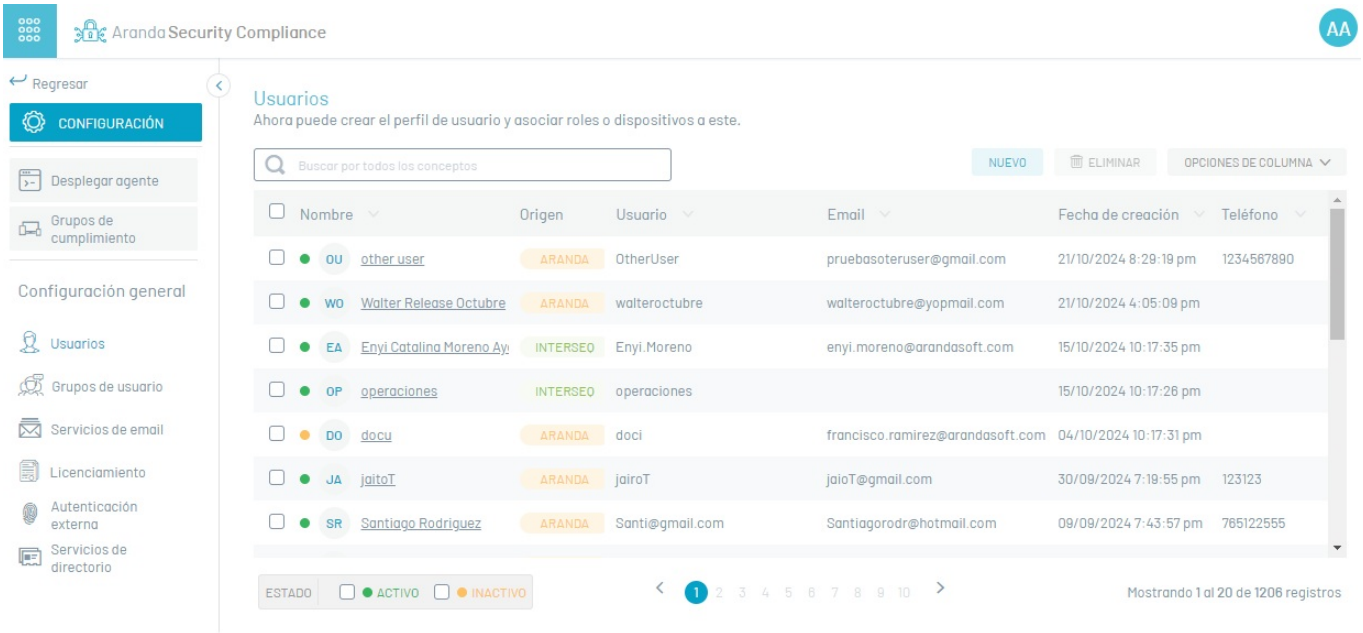
O gerenciamento e a configuração dos processos de configuração para diferentes aplicativos Aranda são realizados a partir de um ambiente web com opções e ações compartilhadas.

Visualize o ambiente

1. Após o login, faça login no console da Web do produto com o conjunto de funções (administrador, especialista, usuários).

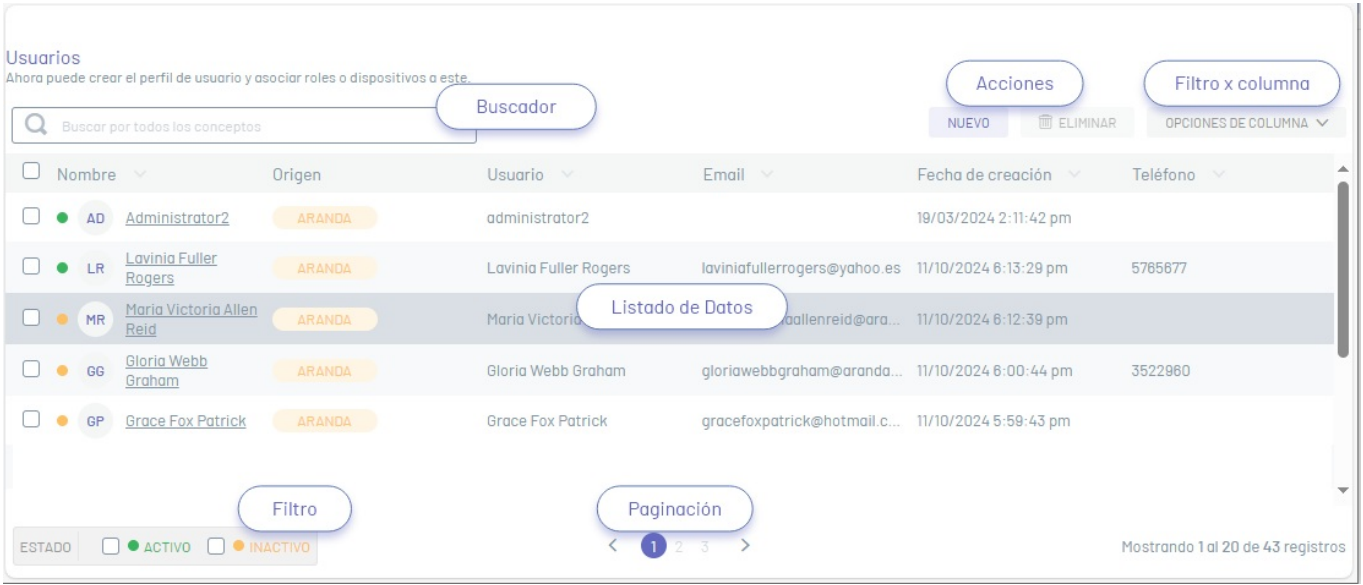
2. No menu principal do produto Aranda, no menu Configuração, selecione o respectivo módulo (Usuários, Servidor de e-mail, Autenticação externa, Serviços de diretório, Tokens de integração) e, ao fazê-lo, habilite a visualização de informações com os dados relacionados.

Exemplo: Na imagem a seguir você pode ver a seção de configuração do produto Aranda Security, com os módulos comuns usados.



Commons/Módulos do Ambiente

3. Na visualização de informações do módulo comum selecionado (Usuários, Servidor de Correio, Serviços de Diretório, Autenticação Externa) você pode encontrar ações transversais que complementam as tarefas de gerenciamento, como:



Abaixo estão as opções disponíveis e os módulos comuns onde são usados:

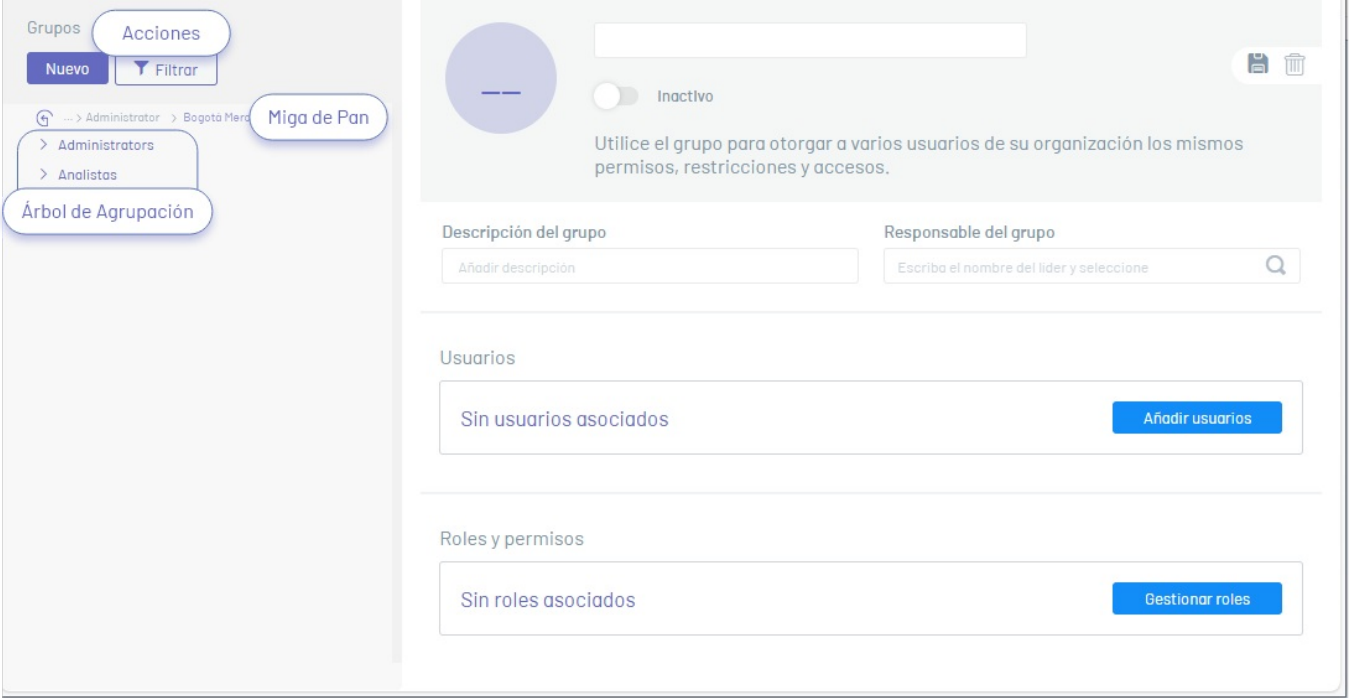
Opção	Descrição	Módulos comuns
Procurar	Ele permite que você pesquise a lista de usuários de acordo com os critérios de pesquisa. Você pode pesquisar pelo nome dos campos definidos de cada conceito associado.	    
Listagem de dados	Esta seção agrupa as informações dos registros encontrados por módulo ou item selecionado. As informações apresentadas são agrupadas em colunas com os dados inseridos. Ao selecionar o registro na lista disponível, você poderá visualizar e editar os dados associados ou excluir o registro.	    

	Este botão define a ação para criar um registro para cada conceito de gerenciamento de produtos da Aranda. A ativação desta ação permite que uma janela preencha as informações relacionadas.	
Novo		
	Este botão define a ação para excluir um registro que já foi criado nos processos de gerenciamento.	
Eliminar		
	Permite mostrar ou ocultar opções da lista.	
Filtrar por coluna		
	As opções de coluna do módulo de usuários são: Nome, origem, usuário, e-mail, data de criação e telefone.	
	Ele permite que você navegue entre as páginas da lista de registros de usuário encontrados.	
Paginação		
	Permite filtrar pelo status ativo ou inativo de usuários ou provedores de autenticação.	
Filtrar por status		
	No módulo Tokens de Integração, você permite filtrar pelo status atual ou expirado dos tokens de conexão de API criados.	
	Este botão	
Segurança		
	define a ação para executar o Configurações do reCAPTCHA para usá-lo no momento da autenticação do usuário.	

Módulo de Ambiente/Grupos do Commons

4. Na visão de informações do módulo comum selecionado (Grupos), é possível encontrar ações que complementam as tarefas de gerenciamento.

5. Na estrutura semelhante a uma árvore para grupos de usuários, é possível identificar os seguintes componentes:



Opção	Descrição	Módulos comuns
Novo	Este botão	
		
Filtro	Define a ação para criar um registro de Grupos de Usuários. A ativação desta ação permite que uma janela preencha as informações relacionadas.	
	Este botão	
Árvore de agrupamento	Define a ação para executar uma pesquisa avançada em toda a árvore de grupos. A ativação desta ação permite que uma janela preencha as informações relacionadas	
	Esta seção exibe os grupos e subgrupos definidos.	
Eliminar	Este botão	
		
	Define a ação para excluir um registro de grupo já criado	
	Este ícone	

Farinha de rosca

Exibe o local atual na árvore de grupo.

Este botão

Adicionar usuários

Añadir usuarios

Define a ação para associar usuários a um grupo estabelecido.

Este botão

Gerenciar funções

Gestionar roles

Define a ação para associar funções a um grupo estabelecido.

Módulo de Usuários

Gerenciamento de usuários

Ver usuários

1. Na visualização Informações de usuários, você pode visualizar a lista de usuários registrados ou importados, agrupados por dados como:

Usuarios

Ahora puede crear el perfil de usuario y asociar roles o dispositivos a este.

Q

Buscar por todos los conceptos

NUEVO

ELIMINAR

OPCIONES DE COLUMNA

☐	Nombre	Origen	Usuario	Email	Fecha de creación	Teléfono
☐	AD Administrator2	ARANDA	administrator2		19/03/2024 7:11:42 pm	
☐	LR Lavinia Fuller Rogers	ARANDA	Lavinia Fuller Rogers	laviniafullerrogers@yahoo.es	11/10/2024 11:13:29 pm	5765677
☐	MR Maria Victoria Allen Reid	ARANDA	Maria Victoria Allen Reid	mariavictoriaallenreid@aran...	11/10/2024 11:12:39 pm	
☐	GG Gloria Webb Graham	ARANDA	Gloria Webb Graham	gloriawebbgraham@arandas...	11/10/2024 11:00:44 pm	3522960

ESTADO

☐ ACTIVO

☐ INACTIVO

<

1

2

3

>

Mostrando 1 al 20 de 43 registros

Campo	Tipo de campo	Descrição
Nome	Texto	Nome com o qual o usuário se identifica.
Origem	Texto	Indica a origem pela qual o usuário foi criado
Utilizador	Texto	Nome usado pelo usuário para acessar o aplicativo.
Email	Texto	E-mail do usuário para receber informações.
Data de criação	Seletor	Indica se o usuário está ativo ou inativo.
Telefone	Texto	Número de telefone do usuário.

📌 Nota: A coluna Origem indica o nome do serviço de diretório que importou o usuário; se o nome da fonte for Aranda São usuários que não foram importados, mas foram criados diretamente dessa interface.

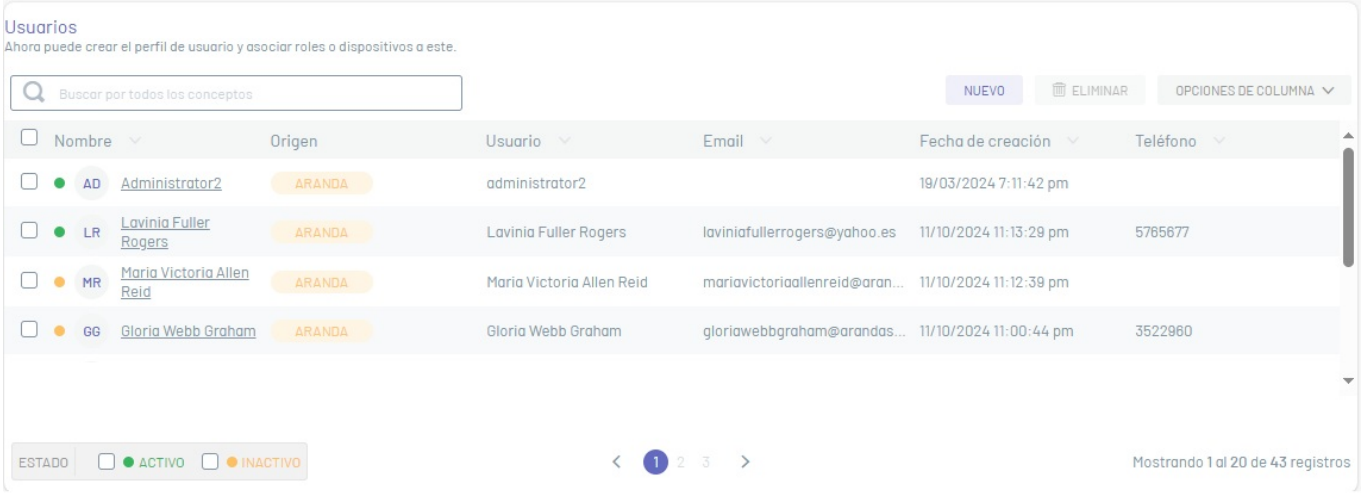
2. Na visualização de informações do usuário, você terá ações de gerenciamento de informações e organização habilitadas.[Visualização de informações no ambiente do Commons](#)

Links Relacionados:

- [Criar usuários](#)
- [Editar usuários](#)
- [Excluir usuários](#)

Criar usuários

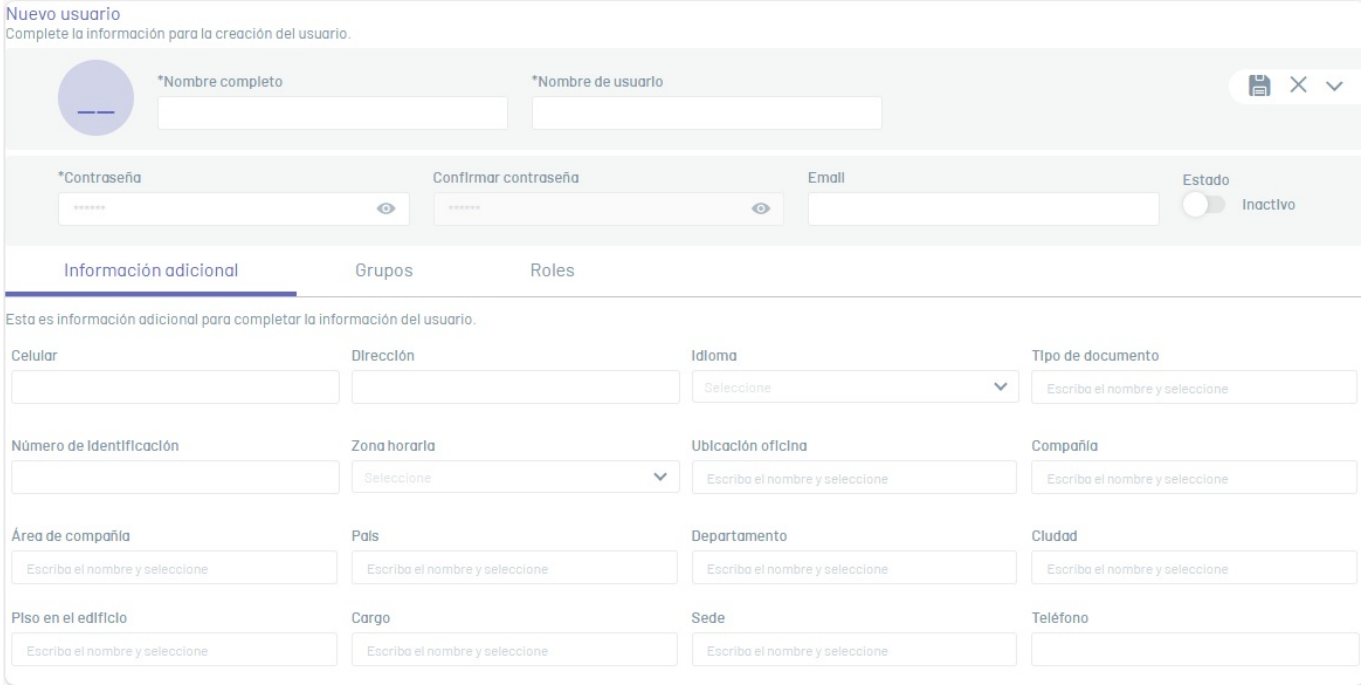
1. Para criar um novo usuário, na visualização de informações do usuário, clique no ícone Novo.



Nota: No podrá crear un usuario con el mismo nombre de usuario a menos que pertenezca a otro proveedor de autenticación.

Fatos básicos

2. Na janela habilitada, você poderá preencher os dados básicos do usuário, informações adicionais, associação de grupos e funções.
3. Nos dados básicos do usuário, você pode inserir campos como nome, senha, e-mail e status. Cada um dos campos do usuário deve levar em conta o [Especificações para campos comuns](#)



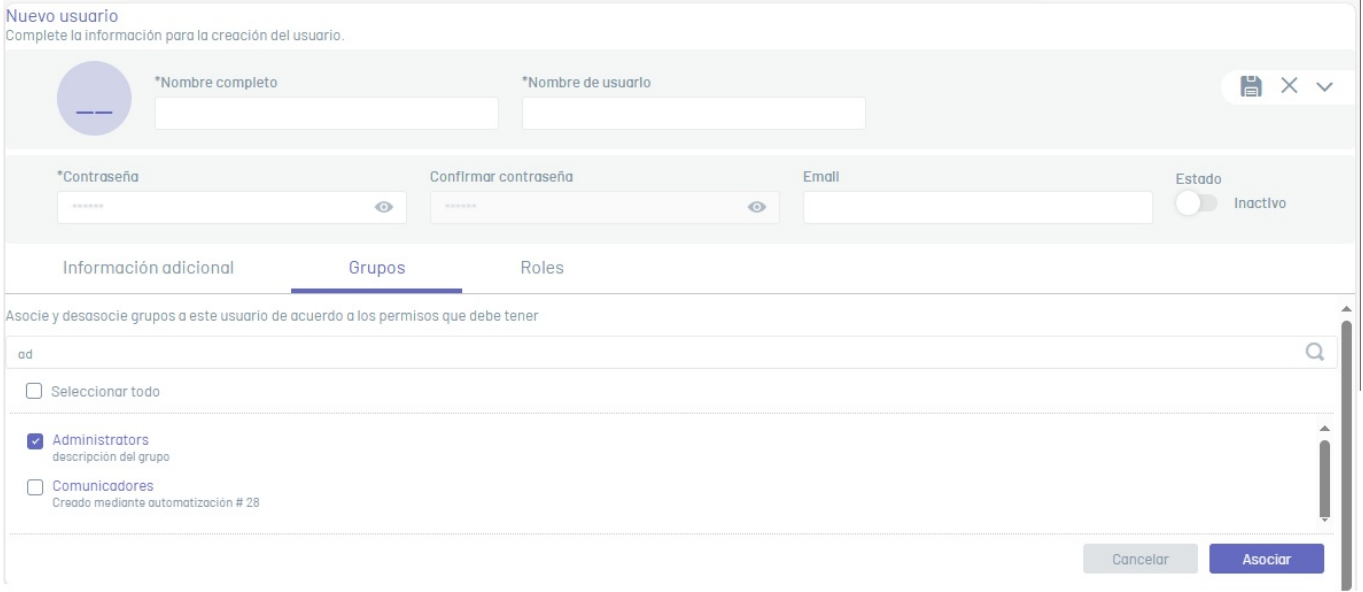
Informações adicionais

4. No Informações adicionais Insira os seguintes campos: Número de telefone celular, endereço, idioma, telefone, entre outros. Cada um dos campos do usuário deve levar em conta o [Especificações para campos](#)

Nota: As informações adicionais do usuário são opcionais e não são necessárias para a criação do usuário.

Associação e dissociação de grupos

4. No Grupos, no campo de pesquisa para associar grupos, você pode relacionar o usuário, o(s) Grupo(s) de Usuários necessário(s).
5. Selecione um ou todos os grupos necessários e clique no botão Associar.



6. Os grupos associados podem ser exibidos na lista de grupos de usuários. 7. Para pesquisar grupos que pertencem ao usuário, você pode usar a barra de pesquisa de grupos de usuários. Grupos no estado brinco Eles não permitem filtragem ou pesquisa por texto.

8. Para desassociar um grupo, selecione um registro na lista de grupos de usuários e clique no botão Desassociar.

Información adicional

Grupos

Roles

Asocie y desasocie grupos a este usuario de acuerdo a los permisos que debe tener

o

Q

Grupos de usuario

Q

Buscar por todos los conceptos

DESASOCIAR

☐ Nombre	Descripción	
☒ Arquitectos	Creado mediante automatización # 8	Pendiente
☒ Asesores	Creado mediante automatización # 32	Pendiente
☐ Administrators	descripción del grupo	

ESTADO

☐ ACTIVO

☐ INACTIVO

<

1

>

Mostrando 1 al 1 de 1 registros

Nota:

- Todas as funções no grupo serão herdadas para os usuários que pertencem a esse grupo.
- Somente os grupos que não são importados e estão ativos aparecerão na lista.
- Se as alterações não tiverem sido salvas, uma coluna aparecerá com a mensagem Brinco o que significa que as alterações não foram salvas e ainda não pertencem ao usuário.

Associação e dissociação de papéis

9. No Papéis, no campo de pesquisa para associar funções, você pode associar as funções ao usuário selecionado, de acordo com as permissões definidas.

10. Selecione uma ou todas as funções que deseja relacionar e clique no botão Associar.

A

*Nombre completo

Administrator2

*Nombre de usuario

administrator2

Guardar

X

▼

*Contraseña

Confirmar contraseña

Email

Estado

Activo

Información adicional

Grupos

Roles

admin

☐ Seleccionar todo

☒ Administrator prueba

Administrator

☐ Administrator Role

Administrator Role

☒ Aproval Administrator

Aproval Administrator

Cancelar

Asociar

11. As funções associadas podem ser exibidas na lista de funções de usuário. 12. Para desanexar uma função, selecione um registro na lista de funções do usuário e clique no ícone Desassociar.

Información adicional

Grupos

Roles

Asocie y desasocie roles a este usuario de acuerdo a los permisos que debe tener

o

Q

Roles asociados

Q

Buscar por todos los conceptos

DESASOCIAR

☐ Nombre	Descripción	
☐ Alert Manager	Alert Manager	Pendiente
Administrator prueba	Administrator	
CManager	CManager	

Nota: : Se a função estiver no Brinco É porque as informações do usuário não foram salvas e, portanto, não foram associadas ao usuário.

11. Quando terminar de configurar o novo usuário, clique no botão Salvar



para confirmar as alterações feitas.

Nota: : Todos os usuários criados por este meio são do tipo Aranda, esse valor é exibido no Origen na lista de usuários.

12. Se o usuário pertencer a um grupo, o grupo herdará as funções do grupo. Cada função é identificada pelo



e só pode ser desassociado removendo o usuário do grupo.

Roles asociados

Q

Buscar por todos los conceptos

DESASOCIAR

☐	Nombre	Descripción
☐	Accounting Manager prueba	Accounting Manager
☒	Administrator prueba	Administrator
☐	Administrator Role	Administrator Role
☐	All Change Viewer	All Change Viewer

Editar usuários

1. Para modificar um usuário, na exibição de informações do usuário, selecione um registro na lista de usuários existentes.

Usuarios

Ahora puede crear el perfil de usuario y asociar roles o dispositivos a este.

Q

Buscar por todos los conceptos

NUEVO

ELIMINAR

OPCIONES DE COLUMNA

☐	Nombre	Origen	Usuario	Email	Fecha de creación	Teléfono
☐	AD Administrator2	ARANDA	administrator2		19/03/2024 7:11:42 pm	
☐	LR Lavinia Fuller Rogers	ARANDA	Lavinia Fuller Rogers	laviniafullerrogers@yahoo...	11/10/2024 11:13:29 pm	5765677
☐	MR Maria Victoria Allen Reid	ARANDA	Maria Victoria Allen Reid	mariavictoriaallenreid@ar...	11/10/2024 11:12:39 pm	

ESTADO

☐ ACTIVO ☐ INACTIVO

<

1

2

3

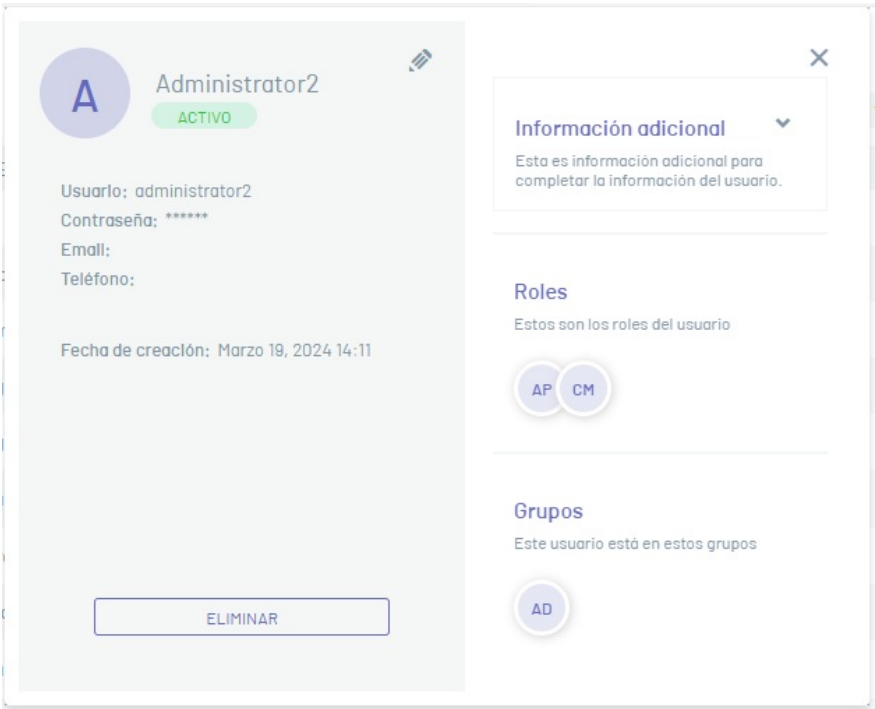
>

Mostrando 1 al 20 de 43 registros

2. Na visualização de detalhes do usuário, clique no ícone Editar



e modifique as informações necessárias.



2. Na janela Edição do usuário você poderá atualizar as informações básicas e adicionais do usuário; bem como os grupos e funções associados ao usuário.

Edición de usuario

Complete la información para la edición del usuario.

A

*Nombre completo

Administrator2

*Nombre de usuario

administrator2

*Contraseña

👁

Confirmar contraseña

👁

Email

Estado

Activo

Información adicional

Grupos

Roles

Esta es información adicional para completar la información del usuario.

Celular

Dirección

Idioma

Seleccione

Tipo de documento

Escriba el nombre y seleccione

Número de Identificación

Zona horaria

(UTC-01:00) Azores

Ubicación oficina

Escriba el nombre y seleccione

Compañía

Escriba el nombre y seleccione

Área de compañía

Escriba el nombre y seleccione

País

Escriba el nombre y seleccione

Departamento

Escriba el nombre y seleccione

Ciudad

Escriba el nombre y seleccione

Piso en el edificio

Escriba el nombre y seleccione

Cargo

Escriba el nombre y seleccione

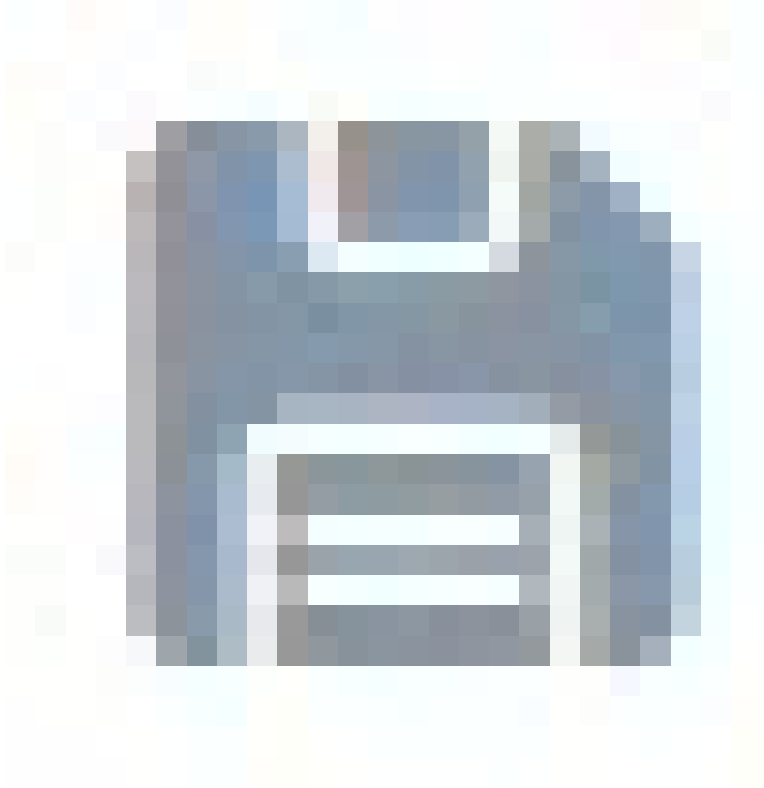
Sede

Escriba el nombre y seleccione

Teléfono

📌 Nota: Somente usuários do provedor Aranda podem ser modificados. Os usuários importados permitem apenas associar e desassociar funções, modificando os campos de estado, idioma e fuso horário.

3. Quando terminar de editar o usuário, clique no botão Salvar



para confirmar as alterações feitas.

Desbloquear usuário

Nota: Quando um usuário é bloqueado por exceder as tentativas de senha permitidas, na visualização de detalhes do usuário, uma mensagem de aviso é ativada e o DESBLOQUEAR. Ao executar esta ação, o usuário bloqueado poderá fazer login novamente.

Adamaris Navarro
ACTIVO

Fecha de creación: 19 de Julio de 2021 9:26

Nombre completo: Adolfo Valdez

Usuario: pgomez

Contraseña: *****

E-mail: pgomez@hotmail.com

Origen: Aranda

ELIMINAR

Información adicional

Esta es información adicional para completar la información del usuario.

Roles
Estos son los roles del usuario
AD ES US PO +2

Grupos
Este usuario esta en estos grupos
J DA PO +2

Usuario bloqueado por exceder los intentos permitidos de contraseña.

DESBLOQUEAR

Excluir usuários

1. Na visualização de informações do usuário, selecione um ou mais registros na lista de usuários existentes e clique no botão Eliminar para limpar as informações associadas.

Usuarios						
Ahora puede crear el perfil de usuario y asociar roles o dispositivos a este.						
Buscar por todos los conceptos				NUEVO	ELIMINAR	OPCIONES DE COLUMNA
☐	Nombre	Origen	Usuario	Email	Fecha de creación	Teléfono
☒	EM Eileen Powell Moss191	Ldap Simulac...	Eileen Powell Moss191	eileenpowellmoss191@aranda...	09/01/2021 9:44:27 am	
☒	GL Gloria Jennings Larson852	Ldap Simulac...	Gloria Jennings Larson852	gloriajenningslarson852@ara...	15/03/2023 4:19:53 pm	6019368459
☐	AA APPLICATION ADMINISTRATOR	ARANDA	administrator		19/03/2024 7:11:42 pm	
ESTADO ☐ ACTIVO ☐ INACTIVO < 1 2 3 > Mostrando 41 al 43 de 43 registros						

2. Você poderá exibir uma mensagem de confirmação para validar a ação de exclusão.

Nota:

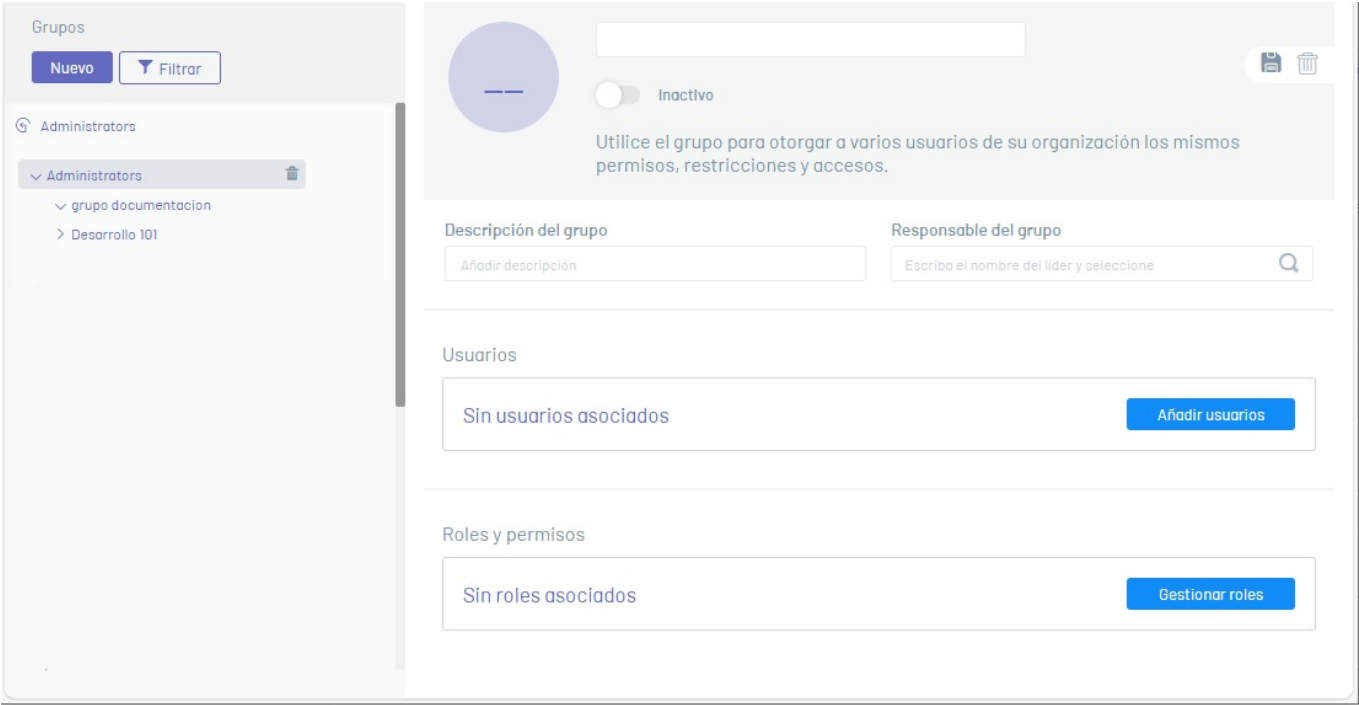
- Um usuário excluído não pode ser restaurado.
- Se o usuário tiver registros associados no banco de dados, a exclusão falhará.
- Os usuários com a função de Administrador e conectados não poderão ser excluídos.
- Se você excluir usuários Importados, na próxima sincronização do Serviço de Diretório, é possível acreditar novamente.

Módulo Grupos

Gestão de Grupos

Exibir grupos de usuários

1. Na visualização de informações Grupos de usuários, você pode exibir uma estrutura semelhante a uma árvore com os grupos e subgrupos de usuários registrados ou importados.
2. Ao selecionar o nome de um grupo, você pode exibir as informações dos subgrupos relacionados. Na visualização de informações, você pode visualizar as informações do grupo em três seções:
- Informação básica: São apresentadas informações básicas do grupo, como nome, status, descrição do grupo e do líder do grupo; Você também poderá editar informações relacionadas.
 - Usuários: Nesta seção, você pode gerenciar usuários para o grupo de usuários.
 - Funções e permissões: nesta seção, você pode gerenciar as funções no grupo de usuários.

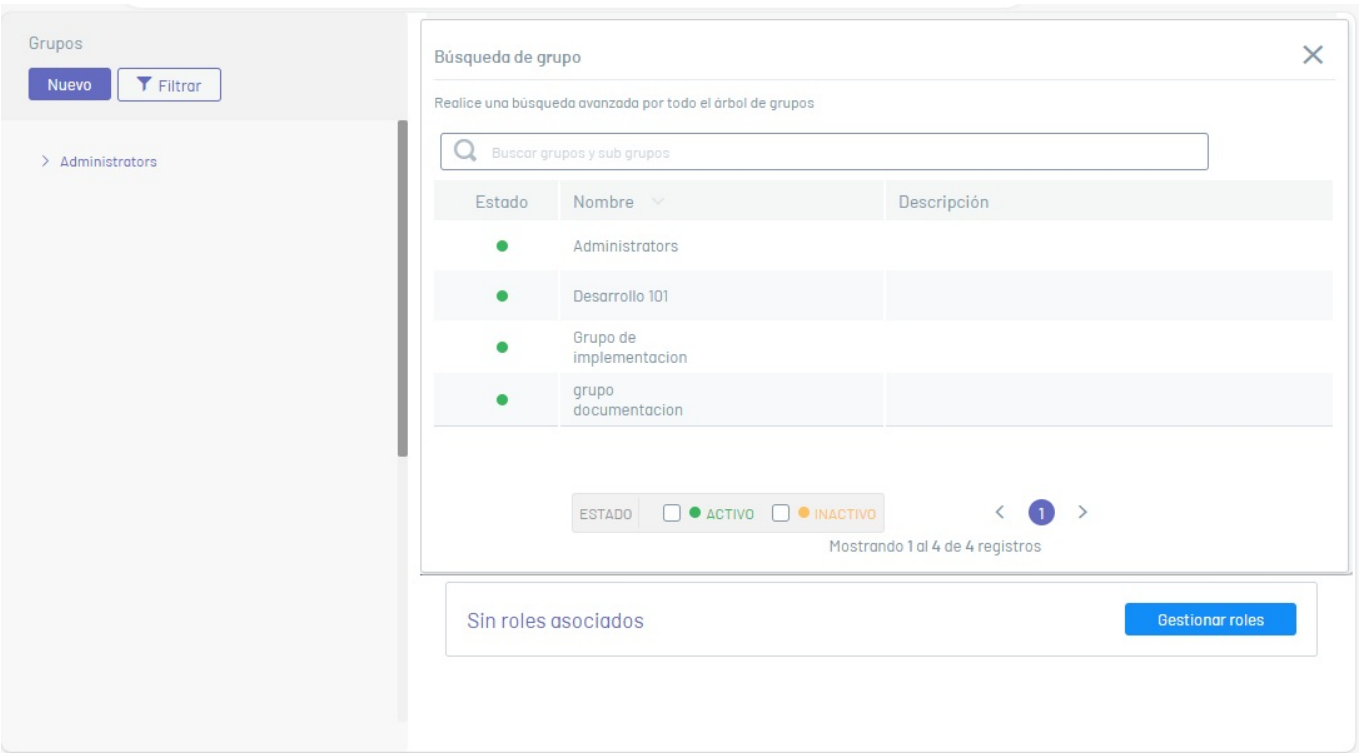


📌 Nota: Mesmo que um grupo esteja desabilitado, ele será exibido na árvore.

2. Na visualização de informações do grupo, você terá ações de gerenciamento e organização de informações habilitadas.
- [Visualização de informações no ambiente do Commons](#)

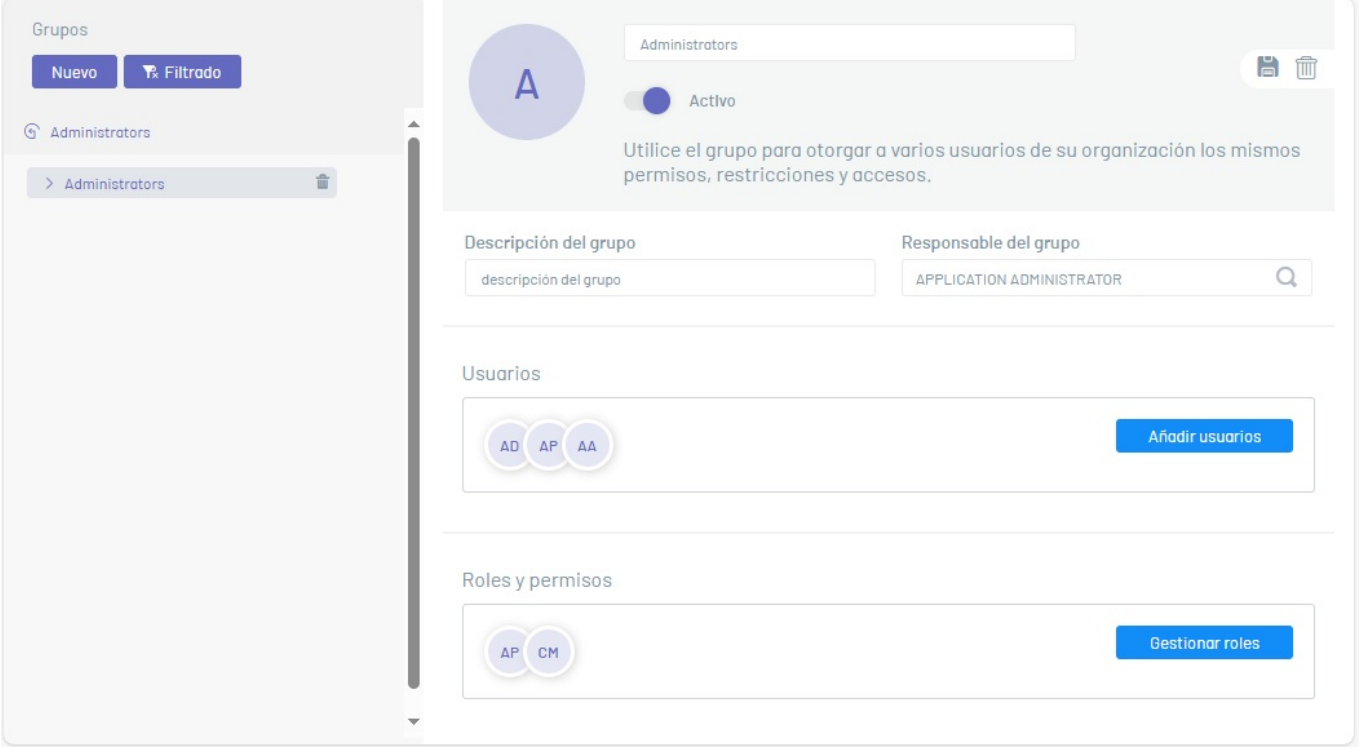
Filtragem de grupo

1. Na exibição de informações do grupo de usuários, selecione o ícone Filtro.
2. A janela está ativada Pesquisa de grupo onde você pode fazer a consulta necessária; No campo Pesquisar, insira uma palavra-chave.



3. Selecione um registro dos grupos encontrados na pesquisa. Isso ativa a janela de detalhes do grupo.
4. Na visualização Informações do Grupo de Usuários, você pode limpar as informações filtradas clicando no botão





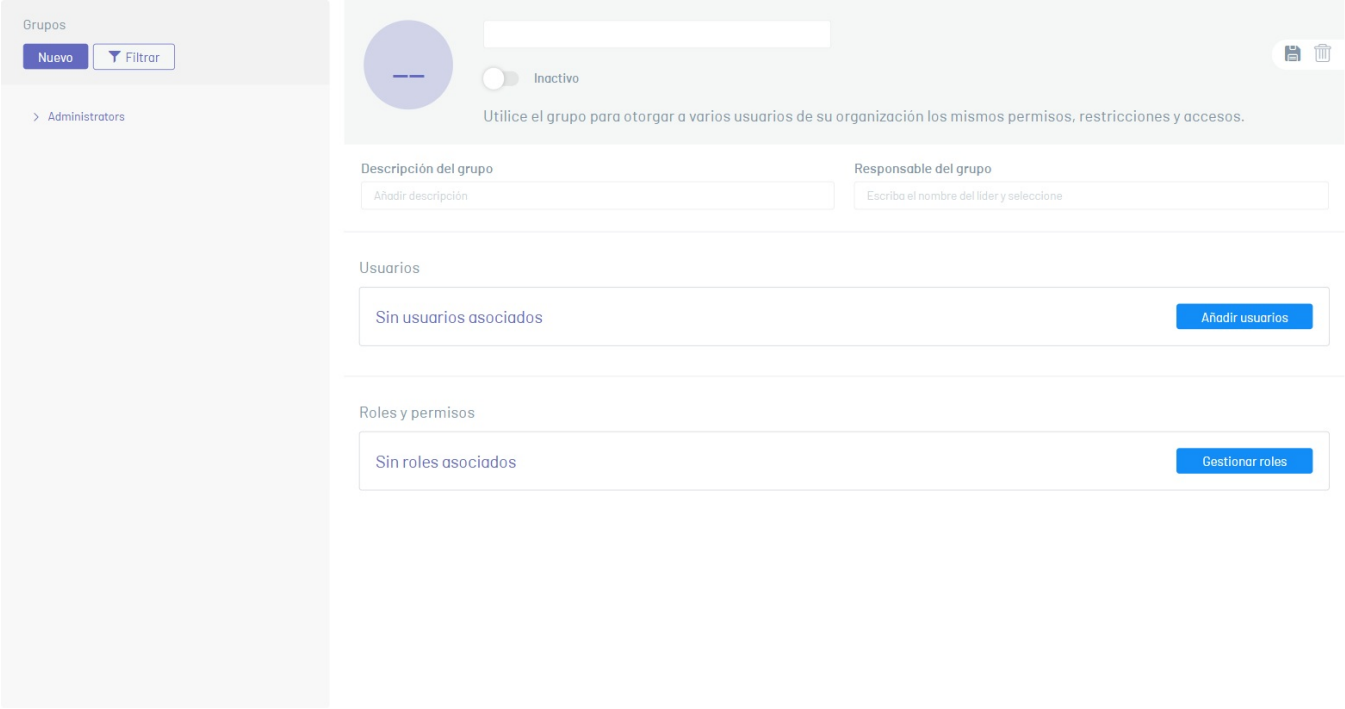
Links Relacionados:

- [Criar grupos](#)
- [Editar grupos](#)
- [Excluir grupos](#)

Criar grupos

Fatos básicos

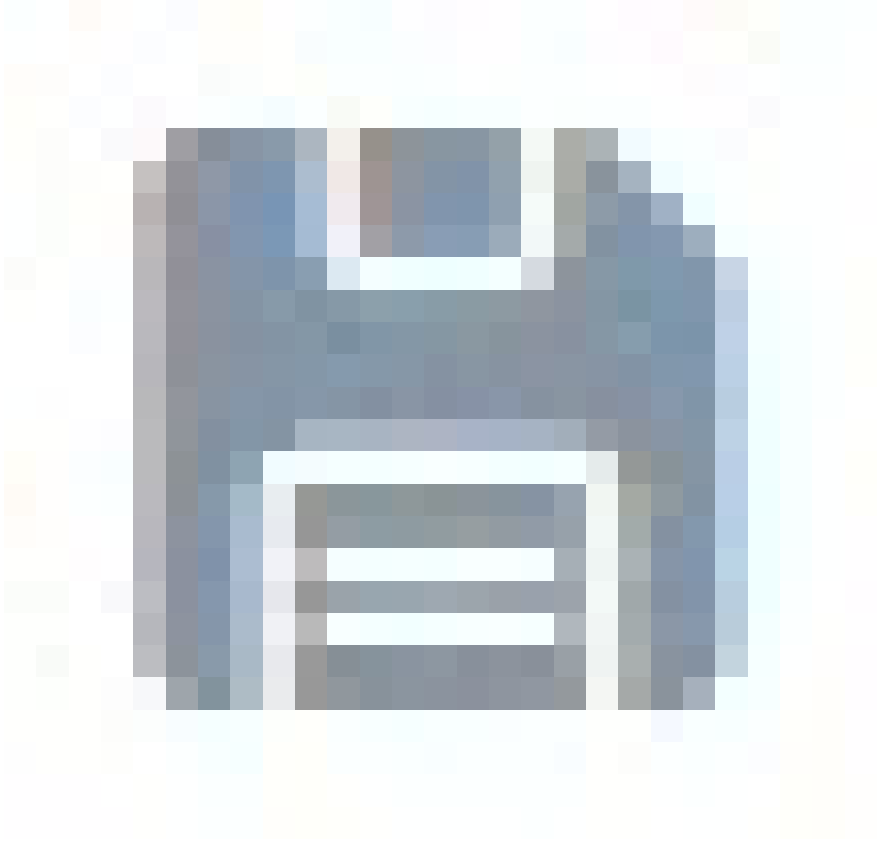
1. Para a criação de um grupo sem hierarquia superior, ele deve estar localizado na raiz da árvore; Na visualização de informações, você pode visualizar o formulário para preencher as informações necessárias (informações básicas, usuários associados e funções).
2. Se o grupo a ser criado deve pertencer a outro grupo, clique no grupo pai desejado e clique no botão Novo e preencha as informações necessárias. Cada um dos campos do grupo deve levar em conta o [Especificações para campos comuns](#).



Nota:

- Os grupos importados não podem ser criados, pois são informações coletadas do diretório de serviços.
- Você pode criar quantos subgrupos precisar. Os subgrupos (grupos filhos) não herdam usuários ou funções do grupo pai (grupo pai).
- Dois grupos não podem ter o mesmo nome se estiverem no mesmo nível hierárquico.

3. Quando terminar de configurar o novo grupo, clique no botão Salvar



para confirmar as alterações feitas. 4. Uma vez criado o grupo de usuários, a mensagem confirmando a criação do grupo será exibida e sua localização será exibida na árvore

Associar e desassociar usuários ao grupo

6. Para adicionar usuários, na exibição de informações de um grupo de usuários, na seção Usuários, selecione o Adicionar usuários.

Inactivo

Utilice el grupo para otorgar a varios usuarios de su organización los mismos permisos, restricciones y accesos.

Descripción del grupo

Añadir descripción

Responsable del grupo

Escriba el nombre del líder y seleccione

Usuarios

AD

AA

Añadir usuarios

Roles y permisos

Sin roles asociados

Gestionar roles

7. A janela está ativada Gerenciar usuários, onde você pode visualizar e adicionar os usuários necessários para o grupo definido. No campo de pesquisa, insira o nome do usuário desejado e selecione o usuário a ser adicionado na lista de resultados. 8. Quando terminar, clique no botão Associar.

Gestionar Usuarios

Asocie aquí usuarios para esta agrupación

ad

☐ Seleccionar todo

☒ Administrator2

☒ APPLICATION ADMINISTRATOR

Cancelar

Asociar

Usuarios asociados

Buscar por todos los conceptos

DESASOCIAR

☐

Nombre completo

Usuario

Email

Fecha de creación

Teléfono

Pendiente

No hay información

📌 Anotações:

- Você só poderá listar usuários ativos. Os usuários adicionados ficarão com as funções do grupo.
- Uma vez associados, os usuários são deixados em um estado Brinco até que o grupo seja salvo

Gestionar Usuarios

Asocie aquí usuarios para esta agrupación

a

Q

Usuarios asociados

Q

Buscar por todos los conceptos

DESASOCIAR

☐	Nombre completo	Usuario	Email	Fecha de creación	Teléfono	Pendiente
☐	Administrator2	administrator2		19/03/2024 2:11:42 pm		Pendiente
☐	APPLICATION ADMINISTRATOR	administrator		19/03/2024 2:11:42 pm		Pendiente

9. Para remover um usuário de um grupo, na seção Gerenciar usuários Selecione um ou mais registros na lista de usuários e clique no botão Desassociar. Confirme que deseja desassociar usuários clicando no ícone Aceitar.

Associando e desassociando funções

10. Para adicionar funções, na exibição de informações de um grupo de usuários, na seção Funções e Permissões, selecione o Gerenciar funções.

Inactivo

Utilice el grupo para otorgar a varios usuarios de su organización los mismos permisos, restricciones y accesos.

Descripción del grupo

Añadir descripción

Responsable del grupo

Escriba el nombre del líder y seleccione

Usuarios

AD

AA

Añadir usuarios

Roles y permisos

Sin roles asociados

Gestionar roles

11. A janela está ativada Gerenciar funções, onde você pode exibir e adicionar as funções necessárias para o grupo definido. No campo de pesquisa, insira o nome da função necessária e, na lista de resultados, selecione a função a ser adicionada.

Nota: Somente funções ativas são listadas.

12. Quando terminar, clique em Associar.

Gestionar Roles

Asocie aquí los roles para esta agrupación

Escriba el nombre del rol y seleccione...

Q

☐ Seleccionar todo

☒ Administrator Role

☒ Alert Manager

Cancelar

Asociar

Roles asociados

Q

Buscar por todos los conceptos

DESASOCIAR

☐	Nombre	Descripción
No hay información		

Nota: O status da função é pendente até que as alterações sejam salvas.

Gestionar Roles

Asocie aquí los roles para esta agrupación

a

Q

Roles asociados

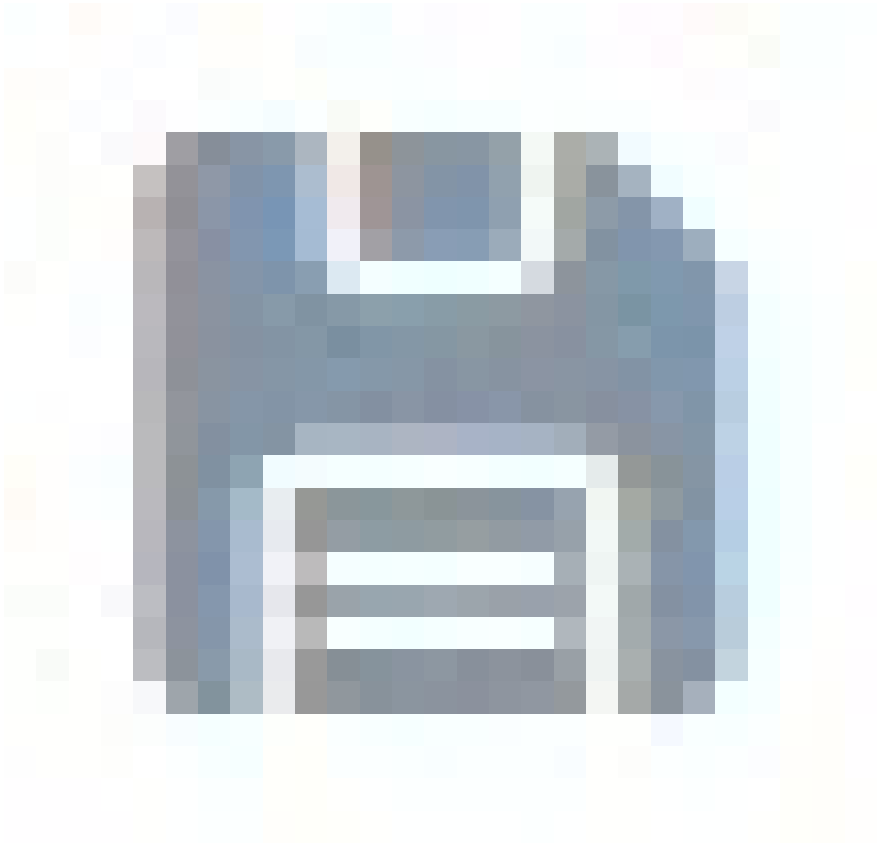
Q

Buscar por todos los conceptos

DESASOCIAR

☐	Nombre	Descripción	
☒	Administrator Role	Administrator Role	Pendiente
☐	All Incidents Viewer	All Incidents Viewer	Pendiente

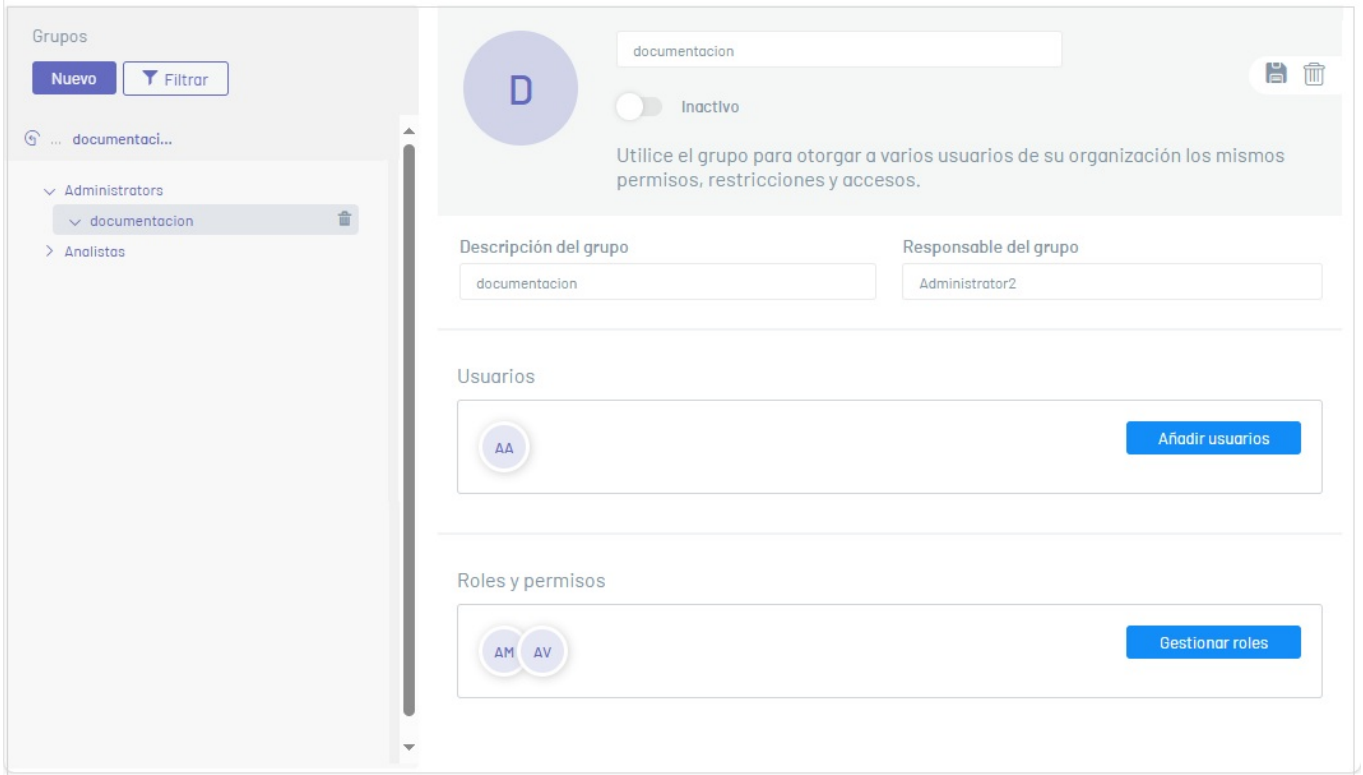
13. Para desanexar funções de um grupo, no Gerenciar funções Selecione um ou mais registros na lista de funções e clique no botão Desassociar. Confirme que deseja desassociar usuários clicando no ícone Aceitar. 14. Quando terminar de configurar o novo grupo, clique no botão Salvar



para confirmar as alterações feitas.

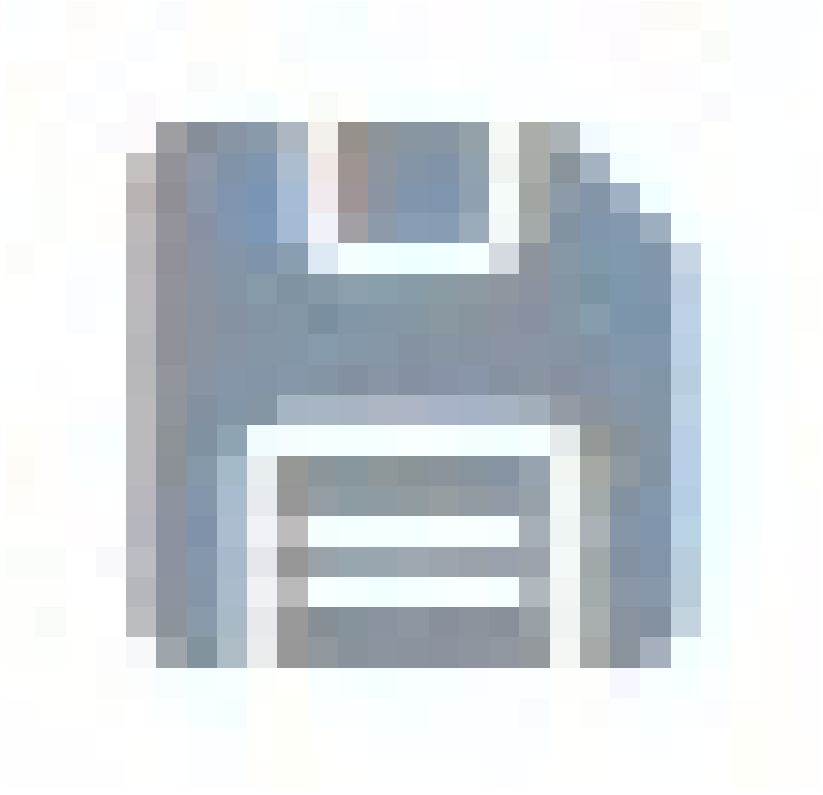
Editar a partir de grupos

1. Para modificar um grupo ou subgrupo, na exibição de informações do grupo de usuários, selecione um registro na árvore de agrupamento; Você poderá visualizar os detalhes do grupo e modificar as informações necessárias.



📌 Nota: Se o grupo for importado de um Active Directory, você só poderá modificar as funções e o status de um grupo. Os usuários não poderão editar

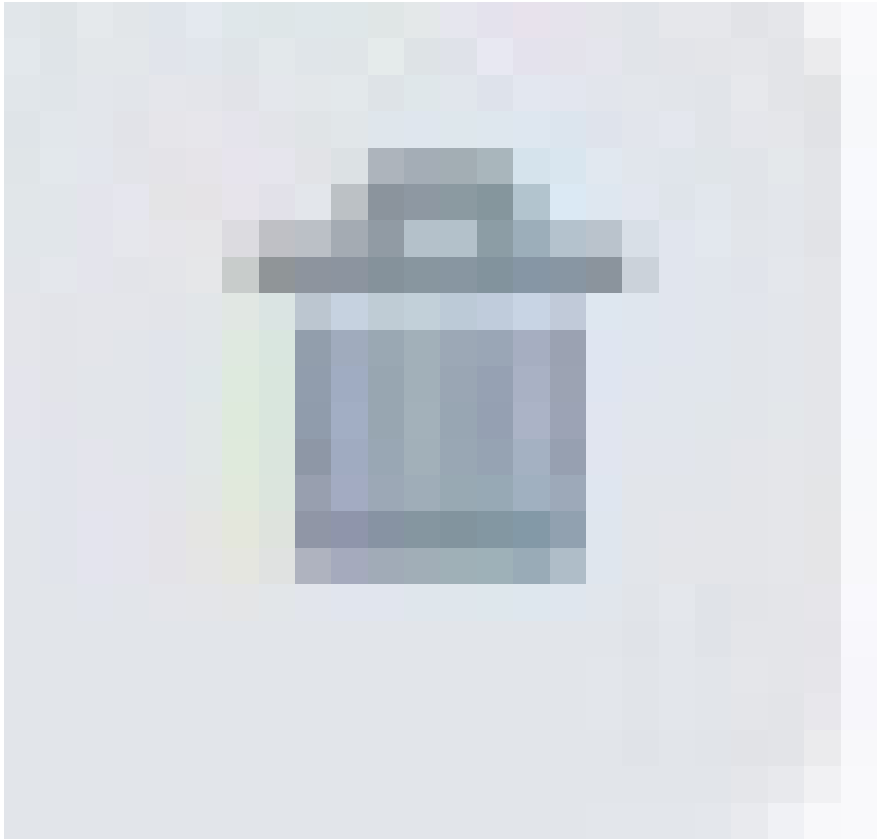
2. Quando terminar de editar o grupo, clique no botão Salvar



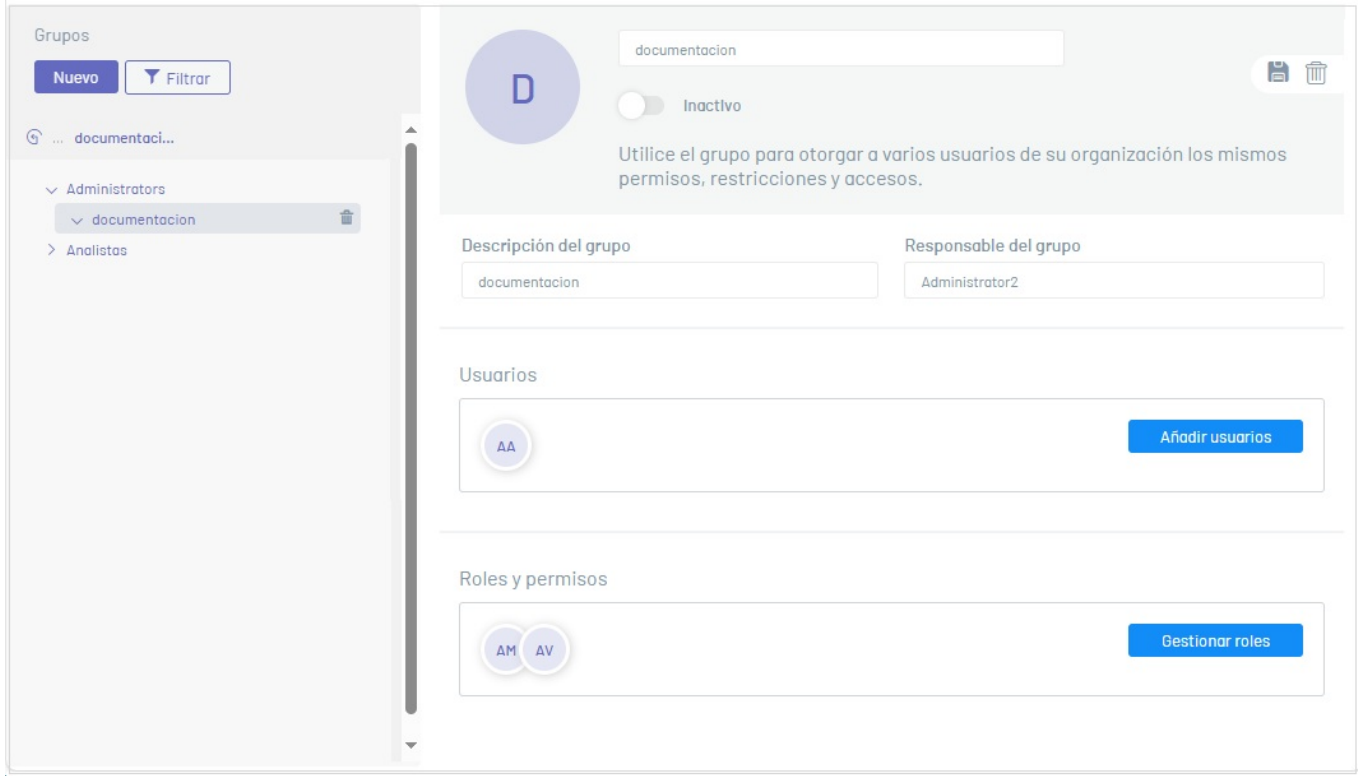
para confirmar as alterações feitas.

Remover de grupos

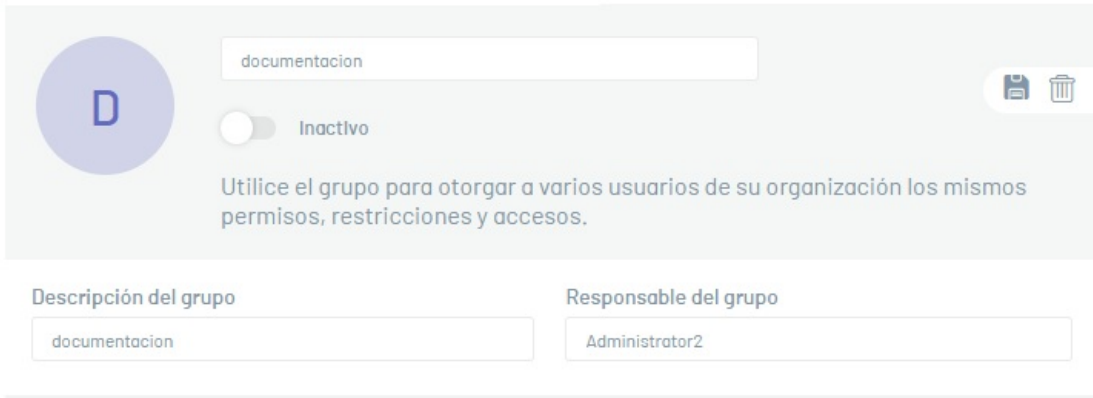
1. Na exibição de informações do grupo de usuários, selecione um registro na árvore de agrupamento e clique no botão Eliminar



para limpar as informações associadas.



2. Como alternativa, na vista de detalhes do grupo selecionado, clique no botão Eliminar para limpar as informações associadas.

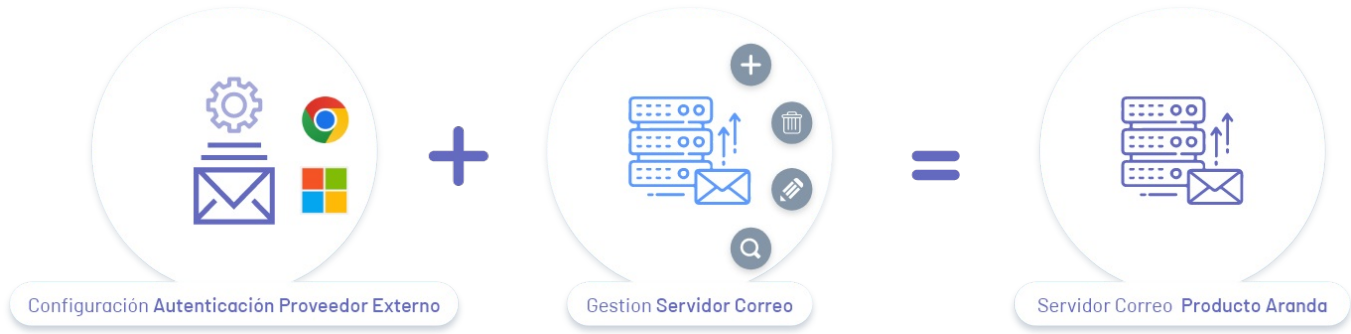


3. Você poderá exibir uma mensagem de confirmação para validar a ação de exclusão.

📌 Nota:

- Quando você exclui um grupo, se for um grupo pai, os subgrupos que pertencem a ele serão excluídos.
- Usuários e funções não serão excluídos se o grupo for excluído.
- Se você quiser excluir apenas um subgrupo, deverá selecionar o subgrupo a ser excluído.
- Os grupos importados podem ser excluídos. No entanto, há uma chance de que o grupo seja importado de volta do diretório de serviço.

Configuração preliminar do servidor de e-mail



1. Configuração de provedores de servidor de terceiros

Configure provedores de terceiros (Microsoft Azure, Google) para processos de autenticação de servidor de email.

Para obter mais informações, consulte o [Autenticação Oauth/Microsoft ↔ Modern](#).

Para obter mais informações, consulte o [Autenticação moderna Oauth/Google ↔](#).

2. Gerenciamento de módulo de servidor de e-mail

No módulo Servidor de e-mail, você pode criar, atualizar e excluir configurações de servidor de e-mail para notificações que serão enviadas aos usuários a partir do console da Web.

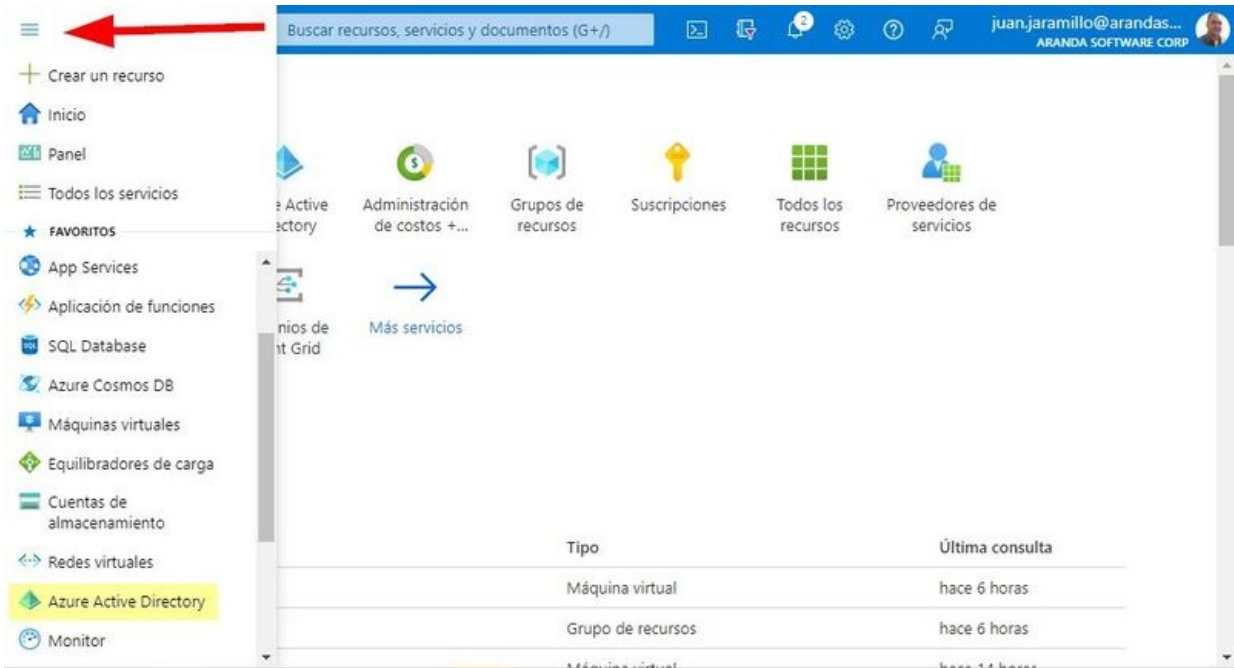
Para obter mais informações, consulte o [Gerenciamento de servidor de ↔ e-mail](#).

Autenticação OAuth 2.0/Microsoft

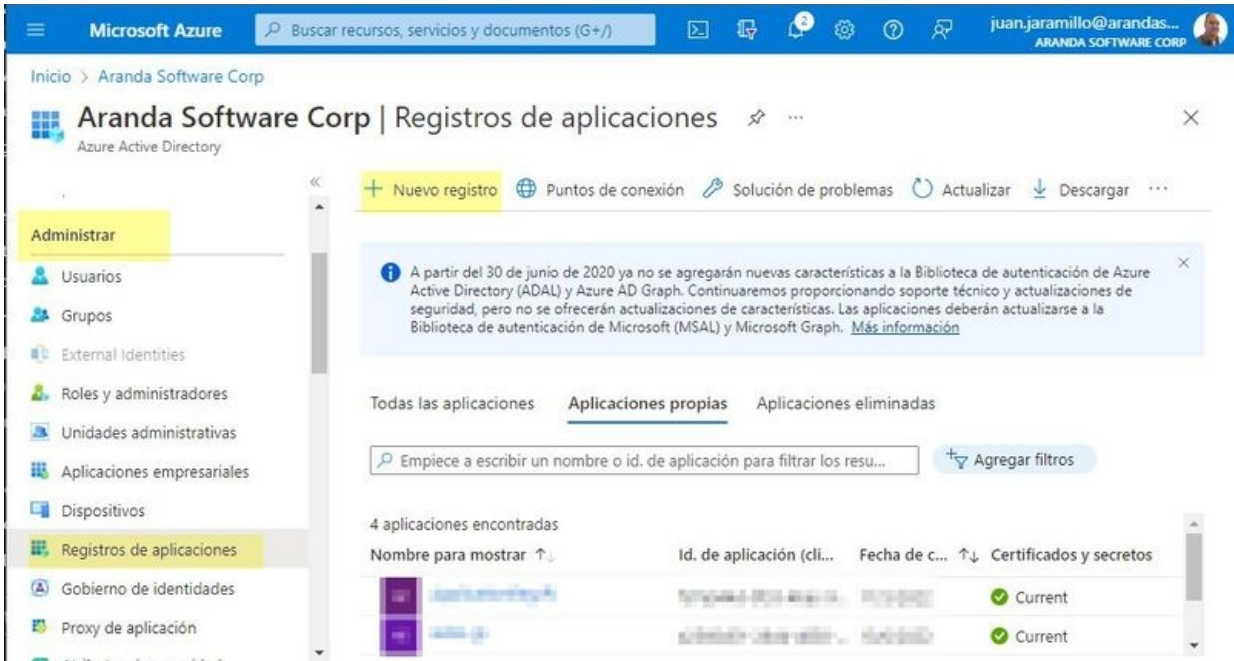
Criando um aplicativo no Azure

► Requisitos Autenticación Azure: ►

1. Acessar o portal do Azure [Veja o Microsoft Azure](#) , pesquise e selecione Azure Active Directory.



2. . No Administrar Pesquise e selecione Logs do aplicativoclique Novo Cadastro.



3. O campo de nome é preenchido e a opção desejada é selecionada em (Tipos de conta suportados), clique em Registro.

Microsoft Azure

Buscar recursos, servicios y documentos (G+/)

Inicio > Aranda Software Corp | Registros de aplicaciones >

Registrar una aplicación

* Nombre

Nombre para mostrar accesible por los usuarios de esta aplicación. Se puede cambiar posteriormente.

Nombre de la Aplicación

Tipos de cuenta compatibles

¿Quién puede usar esta aplicación o acceder a esta API?

☒ Solo cuentas de este directorio organizativo (solo de Aranda Software Corp: inquilino único)

☐ Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino)

☐ Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino) y cuentas de Microsoft personales (como Skype o Xbox)

Al continuar, acepta las directivas de la plataforma Microsoft.

Registrar

4. Depois que seu aplicativo estiver registrado, salve os seguintes dados necessários para a configuração nos aplicativos Aranda.

- ID do aplicativo (cliente) -> ID do cliente.

Clique na opção (Endpoints).

- Ponto de extremidade de autorização do OAuth 2.0 (v2) - URL de autorização >.
- Ponto de extremidade do token OAuth 2.0 (v2) - URL do token >.

Microsoft Azure

Buscar recursos, servicios y documentos (G+/)

Inicio > Aranda Softv

Normbre

Buscar (Ctrl+/)

Eliminar Puntos de conexión Características en versión preliminar

¿Tiene un segundo? Nos encantaría conocer su opinión sobre la plataforma de identidad de Microsoft (anteriormente Azure AD para desarrolladores).

Información esencial

Nombre para mostrar: AutModerna

Id. de aplicación (cliente): [ID]

Identificador de objeto: [ID]

Id. de directorio (inquilino): [ID]

Tipos de cuenta compatibles: Solo mi organización

Credenciales de cliente

0 certificado_1secreto

URI de redirección: 2 web_0 SPA_0 cliente público

URI de id. de aplicación: Agregar un URI de id. de aplicación

Aplicación administrada en directorio local: AutModerna

Puntos de conexión

Punto de conexión de autorización de OAuth 2.0 (v2): https://login.microsoftonline.com/[ID]/oauth2/v2.0/authorize

Punto de conexión de token de OAuth 2.0 (v2): https://login.microsoftonline.com/[ID]/oauth2/v2.0/token

Punto de conexión de autorización de OAuth 2.0 (v1): https://login.microsoftonline.com/[ID]/oauth2/authorize

Punto de conexión de token de OAuth 2.0 (v1): https://login.microsoftonline.com/[ID]/oauth2/token

Documento de metadatos de OpenID Connect: https://login.microsoftonline.com/[ID]/.well-known/openid-configuration

Punto de conexión de la API de Microsoft Graph: https://graph.microsoft.com

Documento de metadatos de federación: https://login.microsoftonline.com/[ID]/federationmetadata/2007-06/federationmetadata.xml

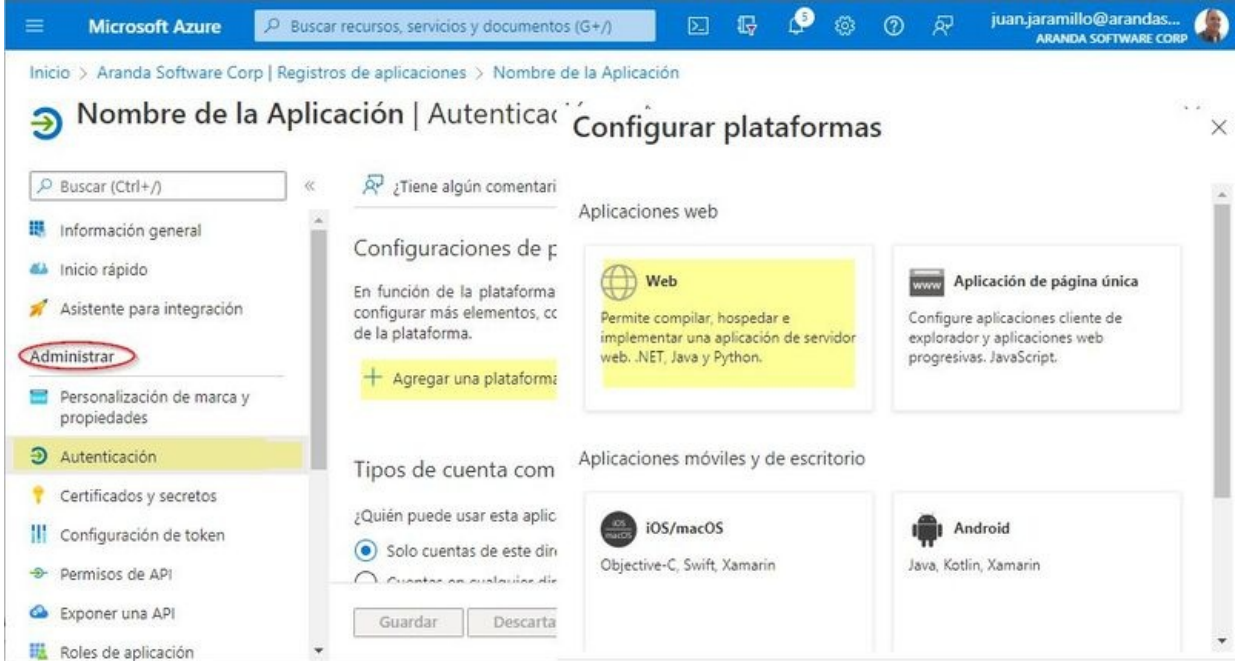
Copiar al Portapapeles

Configurar seu aplicativo no portal do Azure

Quando você tiver o aplicativo criado e tiver os dados salvos, prossiga para configurar o aplicativo da seguinte maneira:

Como configurar a autenticação

1. Você insere o portal do Azure > Menu > do Azure Active Directory > Logs de Aplicativos > seleciona o aplicativo criado na lista que aparece no modo de exibição.
2. No Administrar Pesquise e selecione Autenticação > então em Adicionar uma plataforma, selecione o ícone Teia.



3. Para o produto Gerenciamento de serviços Aranda ASMS Preencha o URIs de redirecionamento como segue:

- Servidor de saída: [https://\[dominio\]/\[Administração do Site\]/Principal/Páginas/OauthToken.aspx](https://[dominio]/[Administração do Site]/Principal/Páginas/OauthToken.aspx)
- Servidor de entrada (Case Creator): (<http://localhost>) e executar o [Proceso de geração manual de token](#) (Carteiro).

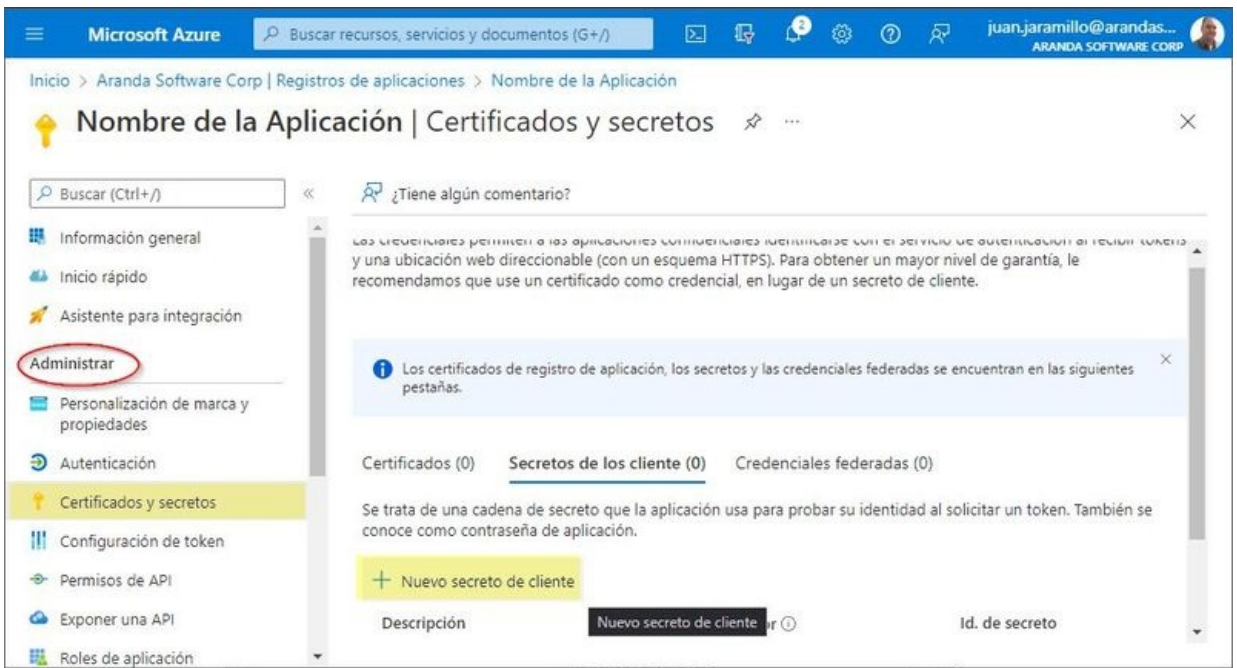
- Substitua o [domínio] conforme apropriado e, em seguida, selecione Configurar.
- Substituir [Administração do site] pelo nome do diretório ou aplicativo do site de administração.
- Nota: Esse nome diferencia maiúsculas de minúsculas e deve ser escrito conforme configurado.

4. Para outros produtos Aranda, o Redirecionamento Url é: (<https://localhost/smtp>) e deve executar o [Proceso de geração manual de token](#) (Carteiro).

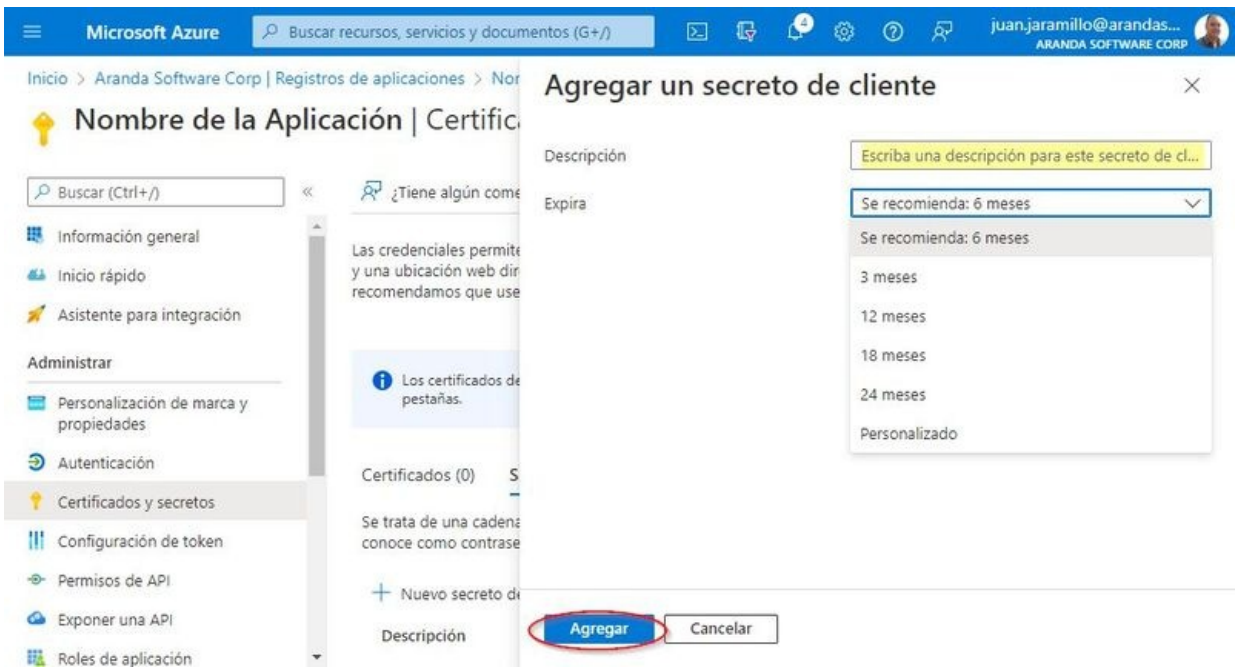
Criação do Segredo

1. Para criar o segredo, insira o portal do Azure > Menu > do Azure Active Directory > Logs de Aplicativos > selecione o aplicativo criado na lista que aparece no modo de exibição.

2. No Administrar Pesquise e selecione Certificados e segredos > Em seguida, clique em Novo segredo do cliente.

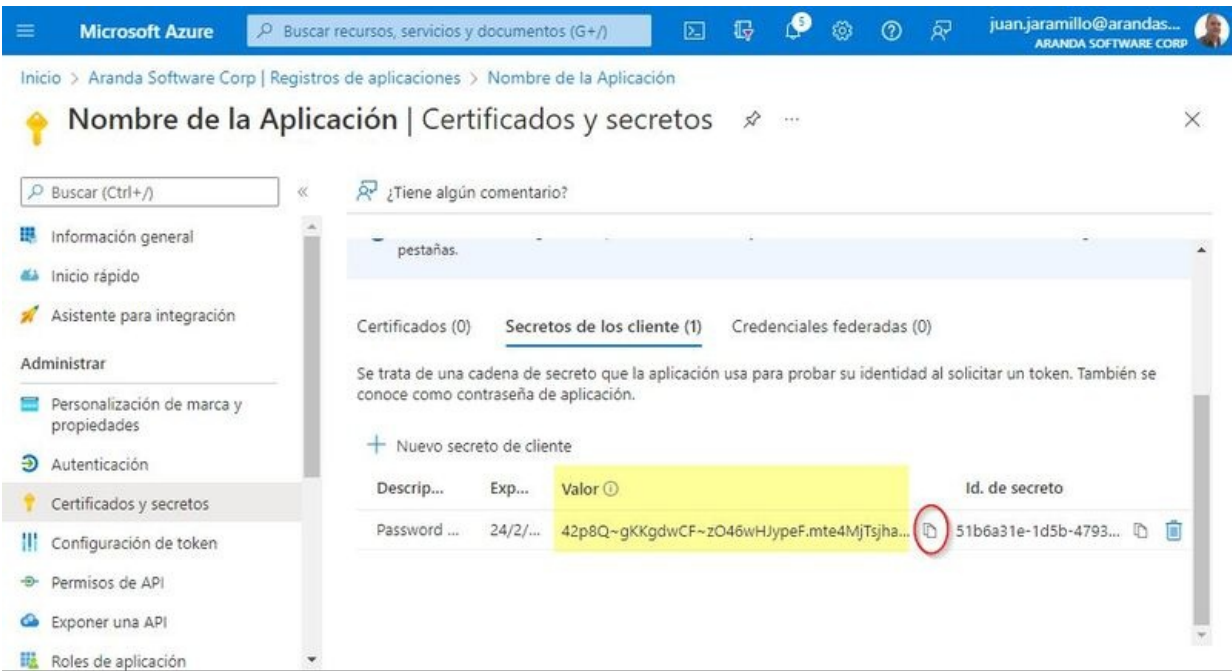


3. Na audiência Adicionar um segredo do cliente Preencha o campo Descrição, configure o Expira que corresponde à duração do sigilo. Em seguida, selecione Adicionar (É importante sempre ter essa duração em mente, pois, quando expirar, se não for atualizada, a autenticação falhará.)



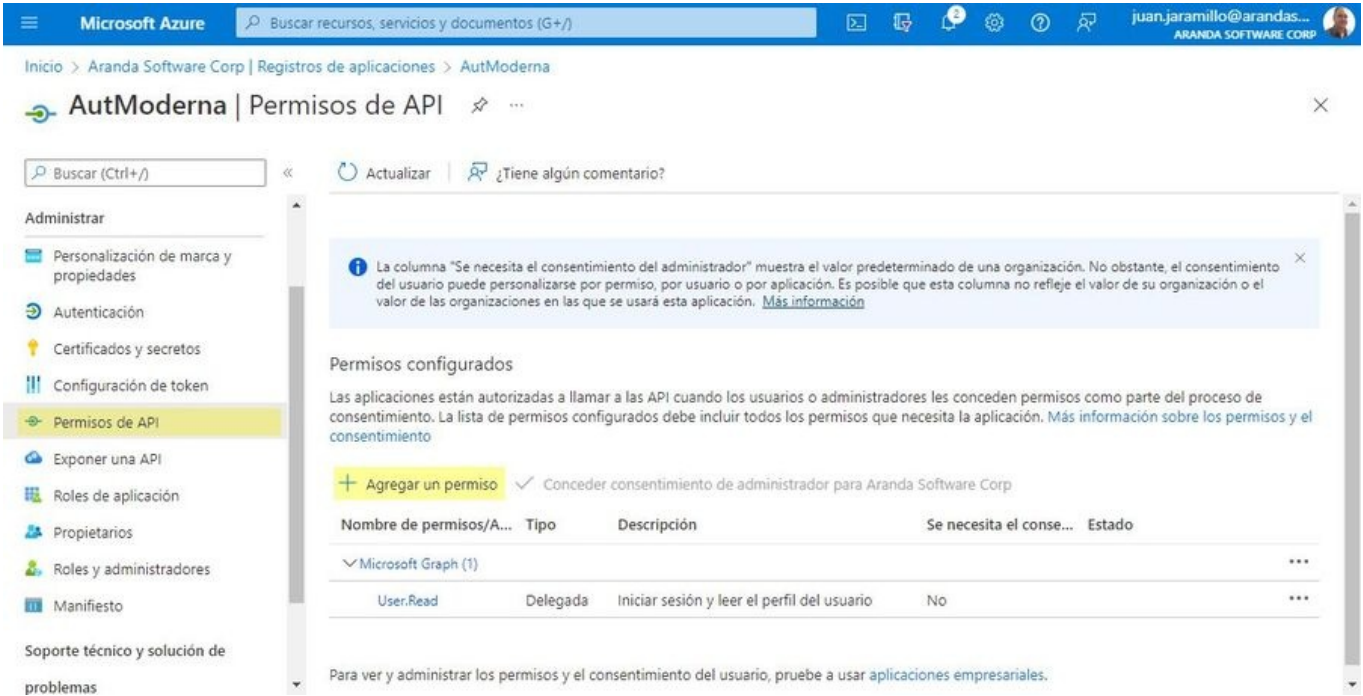
4. O valor do segredo só é visível quando ele é criado, portanto, ele deve ser salvo para uso posterior e retido para as configurações necessárias nos produtos Aranda.

- Valor do segredo do cliente -> segredo do cliente.

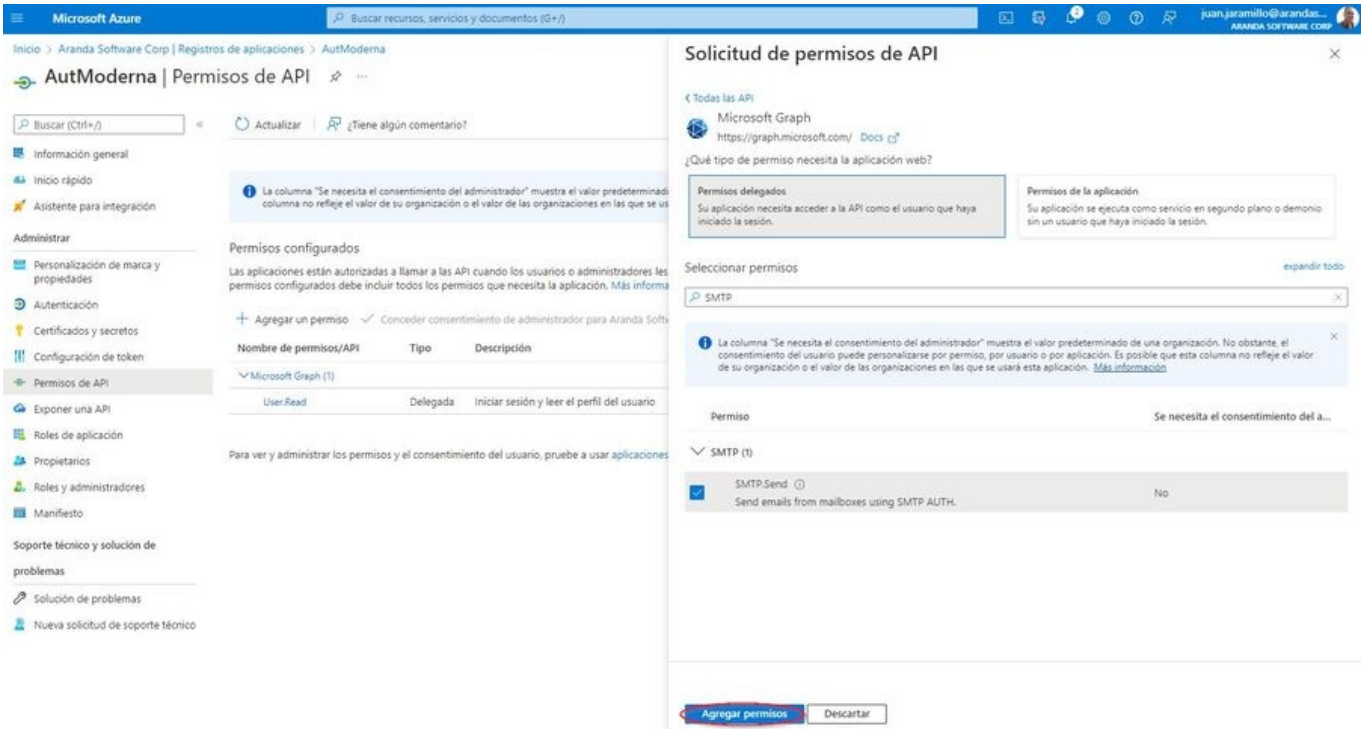


Configurar permissões de API

1. Para configurar permissões de API, acesse o Menu > do portal do Azure > Azure Active Directory > Logs de Aplicativos > selecione o aplicativo criado na lista que aparece no modo de exibição.
2. No Administrar Pesquise e selecione Permissões de API >Em seguida, clique em Adicionar uma permissão.



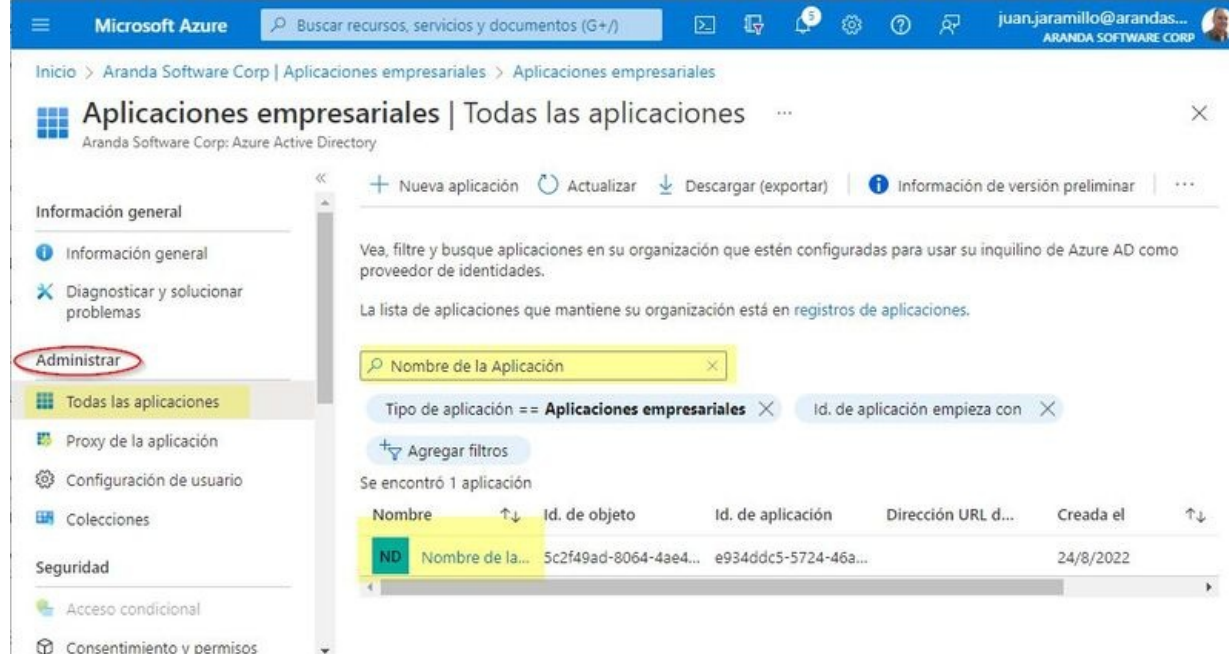
3. Na audiência Solicitar permissões de APIselecionar Microsoft Graph > posterior Permissões delegadas, Seleccione as permissões de acordo com seus requisitos: SMTP. Enviar (Envio de e-mails), IMAP e POP (Lendo e-mails). Clique Adicionar permissão.



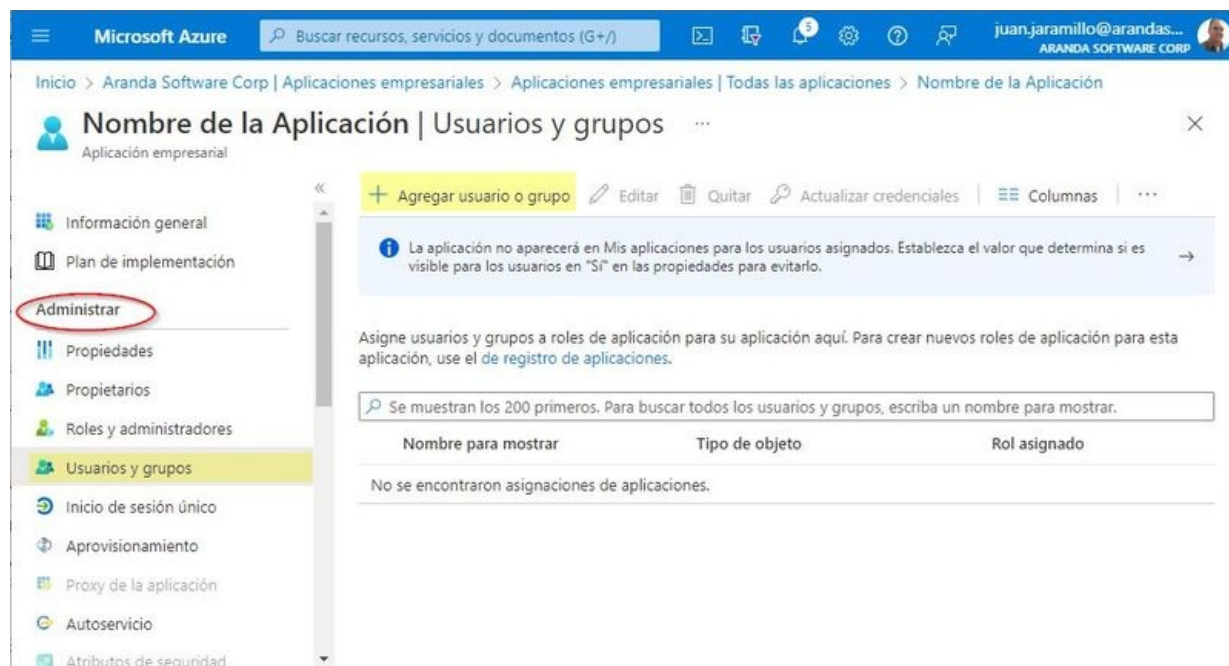
Configurações de usuário e grupo

Nesta configuração, as contas de e-mail que poderão acessar o aplicativo são associadas.

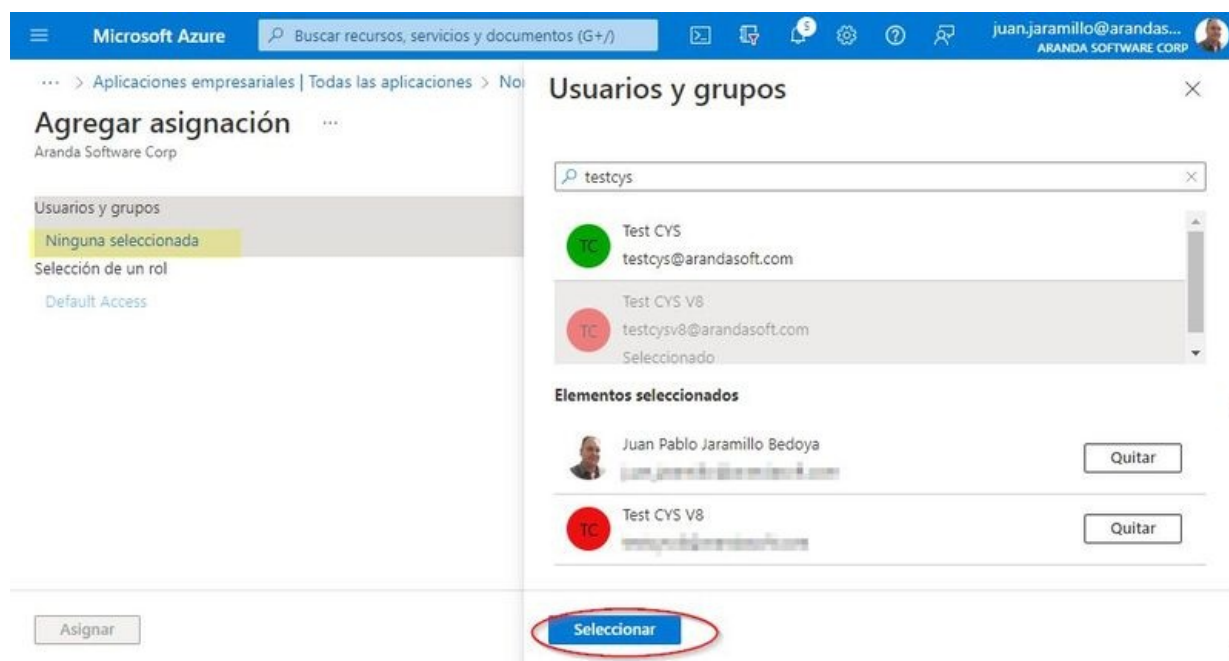
1. Você entra no portal do Azure> Menu> Azure Active Directory> Aplicativos de Negócios> seleciona o aplicativo criado na lista que aparece no modo de exibição.



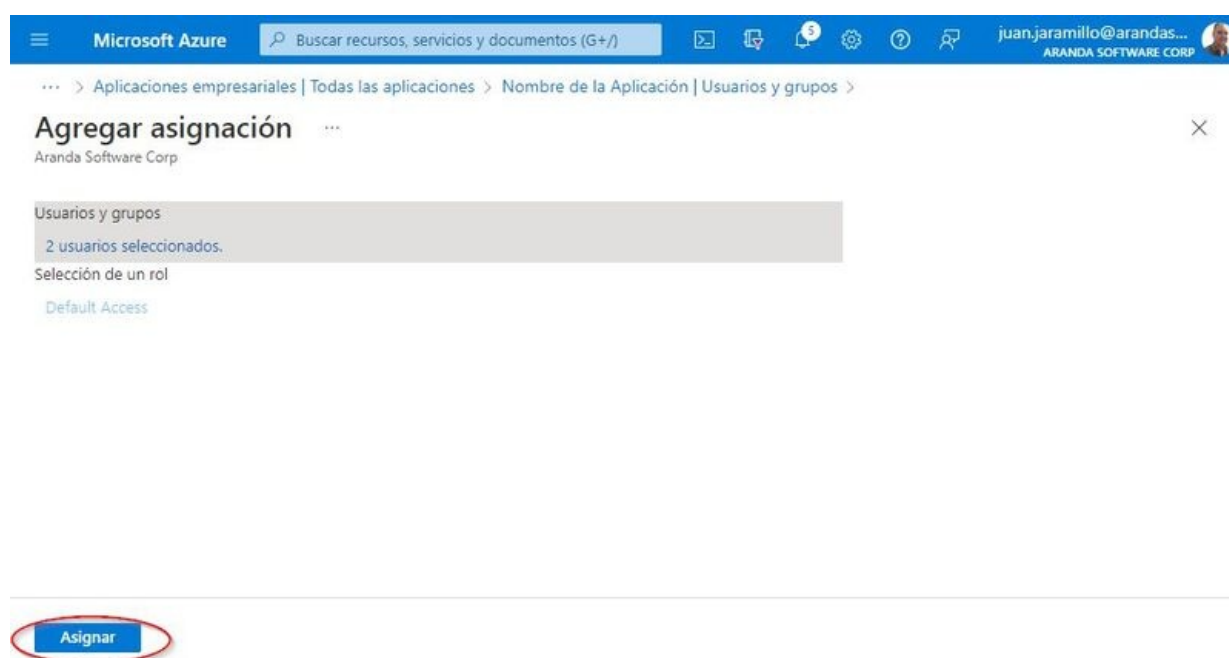
2. No Administrar Pesquise e selecione Usuários e grupos> e então Adicionar usuário ou grupo.



3. No modo de exibição Adicionar mapeamento, selecione Nenhum selecionado> Em seguida, procure a(s) conta(s) de e-mail que deseja adicionar, quando tiver todos os e-mails selecionados, clique em Selecionar.



4. Por fim, selecione Atribuir.

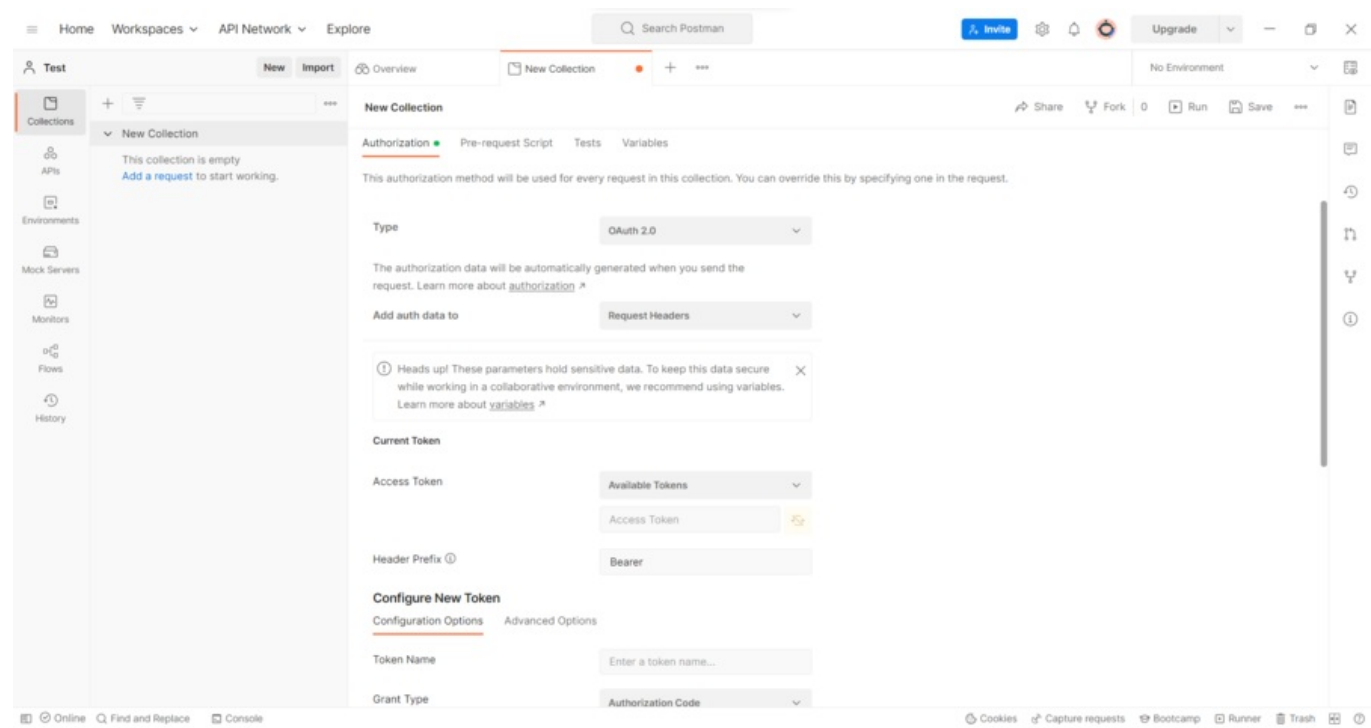


Criação manual de token

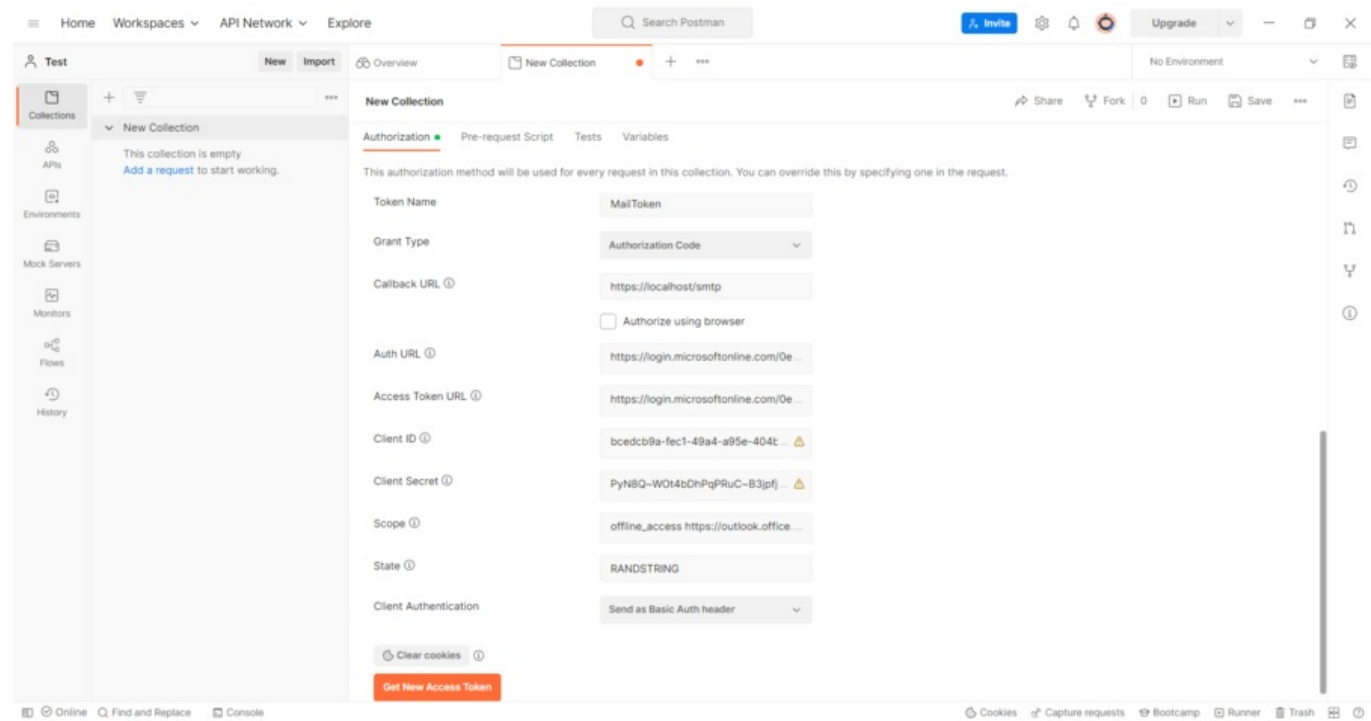
No processo de configuração do servidor de e-mail para autenticação OAuth, o token de autorização é obtido automaticamente nos diferentes aplicativos Aranda. No entanto, a geração manual de tokens também estará disponível para problemas de autenticação.

Configuração manual de token

1. Para gerar o token manual, você deve entrar no aplicativo Postman.
2. No menu principal, depois de gerar uma coleção, selecione o Autorização e no campo Tipo de autorização, selecione no menu suspenso o ícone OAuth 2.0

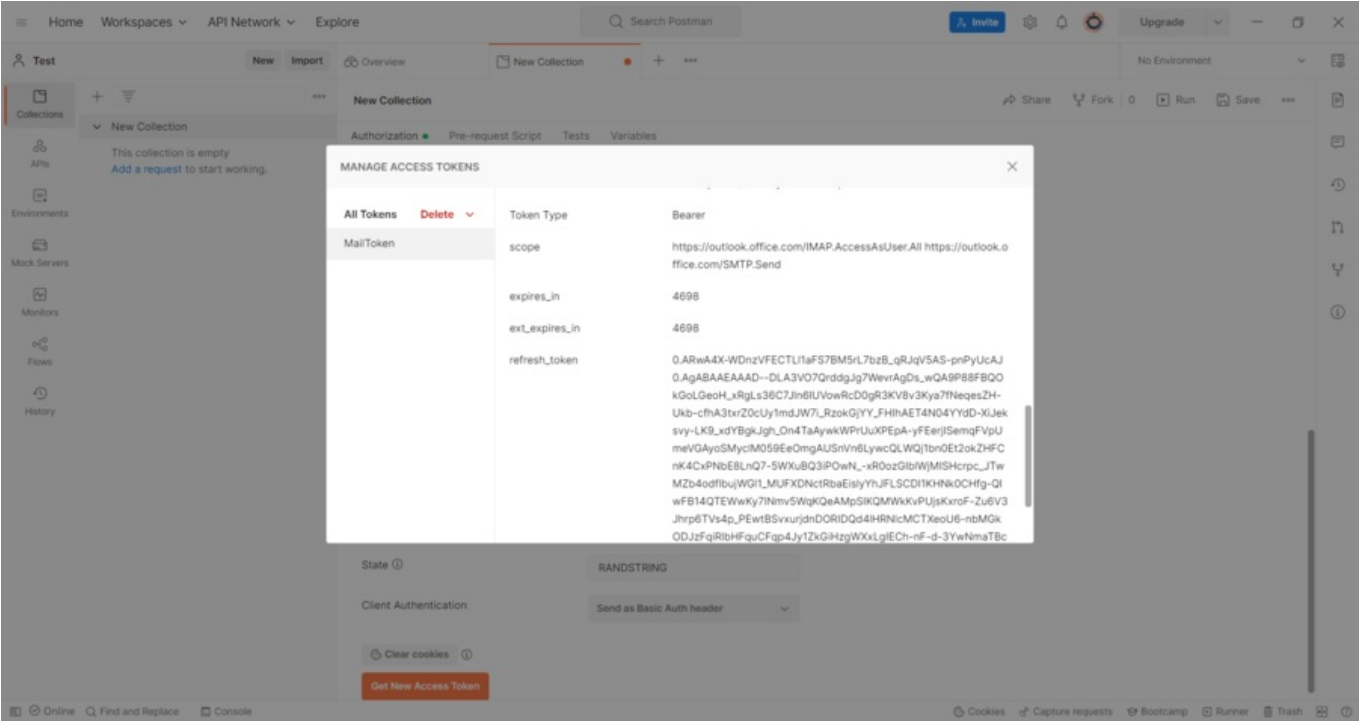


3. No Configurar novo token, clique no ícone Novo Token; O formulário está habilitado para cadastrar os seguintes campos:



Campo	Descrição
Tipo de concessão	Nesta opção, você deve selecionar o Código de autorização
URL de retorno de chamada	Insira a URL que o aplicativo está chamando: - Para o criador de casos de gerenciamento de serviços Aranda: http://localhost - Para o servidor de saída dos outros produtos Aranda: https://localhost/sntp
URL de autenticação	Insira o URL de autorização
URL do token de acesso	Digite o url o url do token
ID do cliente	Insira o ID do cliente
Segredo do cliente	Insira o valor secreto do cliente Insira as informações necessárias:
Âmbito	- Para o criador de casos de gerenciamento de serviços Aranda: offline_access https://outlook.office.com/SMTP.Send https://outlook.office.com/IMAP.AccessAsUser.All https://outlook.office.com/POP.AccessAsUser.All - Para o servidor de saída dos outros produtos Aranda: offline_access https://outlook.office.com/SMTP.Send
Autenticação de cliente	No menu suspenso, use o valor padrão (Enviar como cabeçalho de autenticação básica)

4. Selecione o ícone Obter novo token de acesso, para gerar o token (salve o refresh_token para configuração).



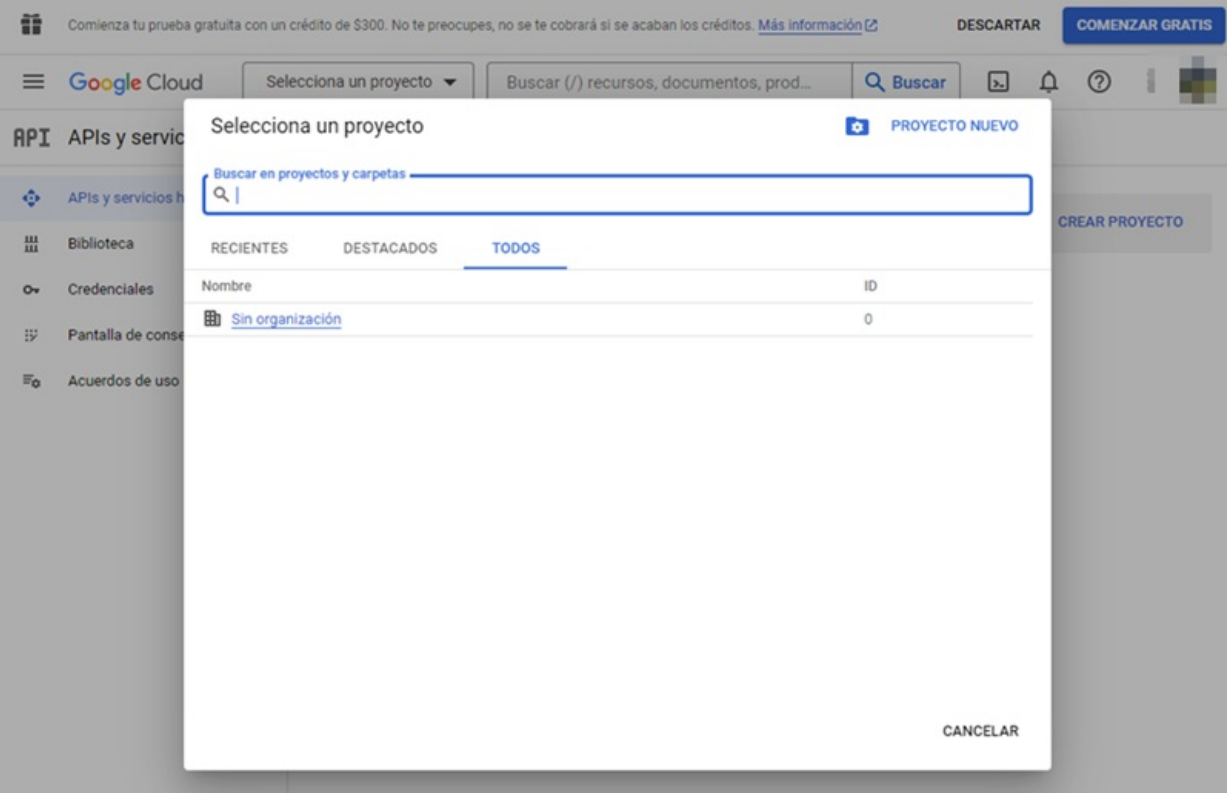
↳ Nota:Após realizar a configuração, o mailer enviará os respectivos e-mails de notificação.

Autenticação OAuth 2.0/Google

Criando um projeto no Google

↳ Nota: Se você já tem um projeto configurado no Google, pode pular esta etapa.

1. Acesso ao [Google Cloud Console](#) com a Conta do Google designada para esse processo, selecione o menu suspenso Selecione um projeto no menu de navegação superior. Em seguida, clique no ícone NOVO PROJETO.



2. Na janela Novo projeto Insira os quatro campos solicitados após as recomendações e clique no botão CRIAR.

Google Cloud

Proyecto nuevo

Nombre del proyecto *

Nombre del Proyecto

ID del proyecto *

nombre-del-proyecto-123

El ID del proyecto puede contener letras minúsculas, números o guiones. Debe empezar con una letra en minúscula y terminar con una letra o un número.

Organización *

Nombre de la Organización

Selecciona una organización para vincularla a un proyecto. No podrás cambiar esta selección más adelante.

Ubicación *

Nombre de la Organización

EXPLORAR

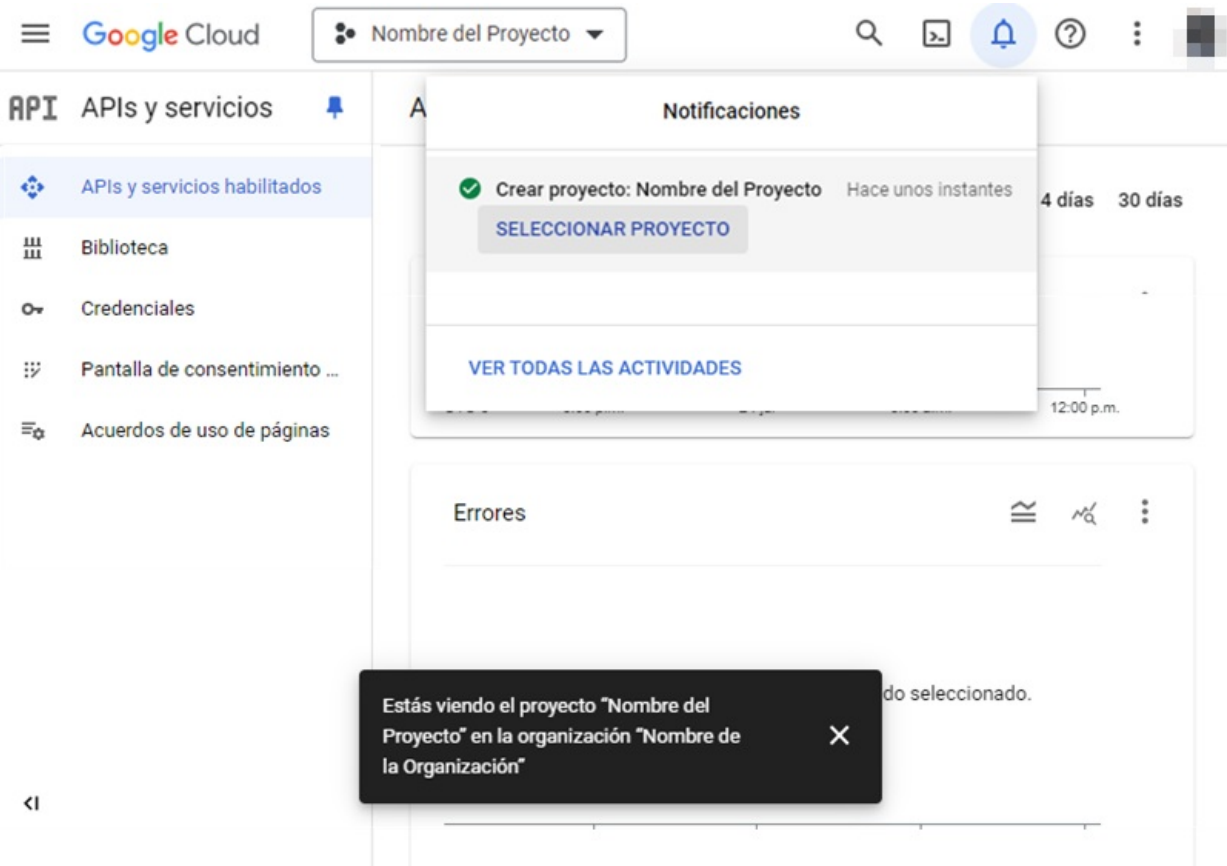
Organización o carpeta superior

CREAR

CANCELAR

Nota: Se estiver no campo Organização apenas a opção está listada Nenhuma organização é que o usuário com quem o projeto está sendo criado não tem as permissões necessárias.

3. A janela está ativada Notificações. Clique no botão SELECCIONE PROYECTO Para o projeto criado:



4. No menu suspenso Seleccione um projeto Você poderá exibir o nome do projeto criado.

Crie e configure seu aplicativo no Google

Quando o projeto for criado e selecionado, prossiga com a criação de um aplicativo OAuth da seguinte maneira:

Como criar um aplicativo no Google

1. Na seção Console do Google Cloud APIs e serviços Seleccione a opção Tela de consentimento OAuth e o tipo de usuário

- Selecionar Interno se você estiver usando um locatário de administrador do GSuite e estiver criando o aplicativo exclusivamente para sua organização.
- Selecionar Externo se você estiver tentando criar uma conta separada do Gmail.

Google Cloud

Nombre del Proyecto

🔍

📄

🔔

❓

⋮

API

APIs y servicios

🔗 APIs y servicios habilitados

📖 Biblioteca

🔑 Credenciales

🔑 Pantalla de consentimiento d...

⚙️ Acuerdos de uso de páginas

Pantalla de consentimiento de OAuth

Elige cómo deseas configurar y registrar tu app, incluidos los usuarios objetivo. Puedes asociar una sola app con tu proyecto.

User Type

☒ Interno

Solo está disponible para los usuarios de tu organización. No necesitarás enviar tu app para verificarla. [Obtén más información sobre el tipo de usuario](#)

☐ Externos

Está disponible para cualquier usuario de prueba con una Cuenta de Google. Tu app se iniciará en modo de prueba y solo estará disponible para los usuarios que agregues a la lista de usuarios de prueba. Una vez que la app esté lista para enviarse a producción, puede que debas verificarla. [Obtén más información sobre el tipo de usuario](#)

CREAR

2. Clique no botão CRIAR. 3. Na janela Tela de consentimiento OAuth Insira os campos Nome do aplicativo, E-mail de suporte ao usuário No Informações de aplicação e Endereços de e-mail No Informações de contato do desenvolvedor de acordo com as recomendações de cada campo (os demais campos são opcionais). Em seguida, clique no ícone SALVAR E CONTINUAR.

API

APIs y servicios

🔗 APIs y servicios habilitados

📖 Biblioteca

🔑 Credenciales

🔑 Pantalla de consentimiento d...

⚙️ Acuerdos de uso de páginas

Editar el registro de la app

1 Pantalla de consentimiento de OAuth

2 Permisos

3 Resumen

Información de la aplicación

Esta información aparece en la pantalla de consentimiento y permite que los usuarios finales sepan quién eres y cómo comunicarse contigo

Nombre de la aplicación *

Nombre de la Aplicación

El nombre de la aplicación que solicita el consentimiento

Correo electrónico de asistencia del usuario *

usuario@dominio.com

Para que los usuarios se comuniquen contigo si tienen preguntas sobre su consentimiento. [Más información](#)

Logotipo de la app

Este es tu logotipo. Ayuda a que las personas reconozcan tu app y aparece en la pantalla de consentimiento de OAuth.

Después de subir un logotipo, deberás enviar tu app para verificarla, a menos que esté configurada solo para uso interno o tenga el estado de publicación "Prueba". [Más información](#)

Dominios autorizados

Cuando un dominio se usa en la pantalla de consentimiento o en la configuración del cliente de OAuth, debe contar con un registro previo aquí. Si debes verificar la app, ve [Google Search Console](#) para comprobar si tus dominios están autorizados. [Más información](#)

+ AGREGAR UN DOMINIO

Información de contacto del desarrollador

Direcciones de correo electrónico *

usuario@dominio.com

Google enviará notificaciones sobre cualquier cambio en tu proyecto a estas direcciones de correo electrónico.

GUARDAR Y CONTINUAR

CANCELAR

4. Na janela Permissões Clique no botão ADICIONAR OU REMOVER PERMISSÕES.

API

APIs y servicios

APIs y servicios habilitados

Biblioteca

Credenciales

Pantalla de consentimiento d...

Acuerdos de uso de páginas

Editar el registro de la app

Pantalla de consentimiento de OAuth

Permisos

Resumen

Los permisos representan lo que solicitas que los usuarios autoricen para la app y permiten que tu proyecto tenga acceso a tipos específicos de datos privados del usuario de sus Cuentas de Google. [Más información](#)

AGREGAR O QUITAR PERMISOS

5. Na janela Atualizar permissões selecionadas No Adicionar permissões manualmente Insira o valor `https://mail.google.com/` e clique no ícone ADICIONAR À TABELA. Em seguida, em ATUALIZAÇÃO.

Actualiza los permisos seleccionados

Solo se muestran los permisos de las APIs habilitadas. Si deseas agregar un permiso faltante a esta pantalla, encuentra y habilita la API en la [Biblioteca de APIs de Google](#) o usa el recuadro para pegar permisos que aparece a continuación. Actualiza la página para ver las APIs nuevas que habilites en la biblioteca.

Filtro

Ingresa el nombre o el valor de la propiedad

☐	API ↑	Alcance	Descripción para el usuario
☐		.../auth/userinfo.email	See your primary Google Account email address
☐		.../auth/userinfo.profile	See your personal info, including any personal info you've made publicly available
☐	BigQuery API	.../auth/cloud-platform.read-only	Ver tus datos en todos los servicios de Google Cloud y ver la dirección de correo electrónico de tu Cuenta de Google
☐	BigQuery API	.../auth/devstorage.full_control	Manage your data and permissions in Cloud Storage and see the email address for your Google Account
☐	BigQuery API	.../auth/devstorage.read_only	Ver tus datos en Google Cloud Storage.
☐	BigQuery API	.../auth/devstorage.read_write	Administrar tus datos de Cloud Storage y ver la dirección de correo electrónico de tu Cuenta de Google

Filas por página: 10 1 – 10 de 24 < >

https://mail.google.com/

AGREGAR A LA TABLA

ACTUALIZAR

6. Na janela Permissões Verifique se a permissão foi adicionada no Suas permissões restritas e clique no ícone SALVAR E CONTINUAR para avançar para a janela Resumo onde você pode visualizar os dados do novo aplicativo. 7. Selecione a opção Credenciais, clique no ícone CRIAR CREDENCIAIS e selecione o ícone ID do cliente OAuth.

API

APIs y servicios

Credenciales

+ CREAM CREDENCIALES

BORRAR

APIs y servicios habilitados

Biblioteca

Credenciales

Pantalla de consentimiento

Acuerdos de uso de páginas

Clave de API

Identifica tu proyecto con una clave de API simple para verificar la cuota y el acceso

ID de cliente de OAuth

Solicita el consentimiento del usuario para que tu app pueda acceder a sus datos

Cuenta de servicio

Habilita la autenticación de servidor a servidor en el nivel de la app mediante cuentas robot

Ayúdame a elegir

Responde algunas preguntas para decidir qué tipo de credencial usar

☐

Nombre

Fecha de creación

Tipo

ID de cliente

Acciones

No hay clientes de OAuth para mostrar

Cuentas de servicio

[Administrar cuentas de servicio](#)

☐

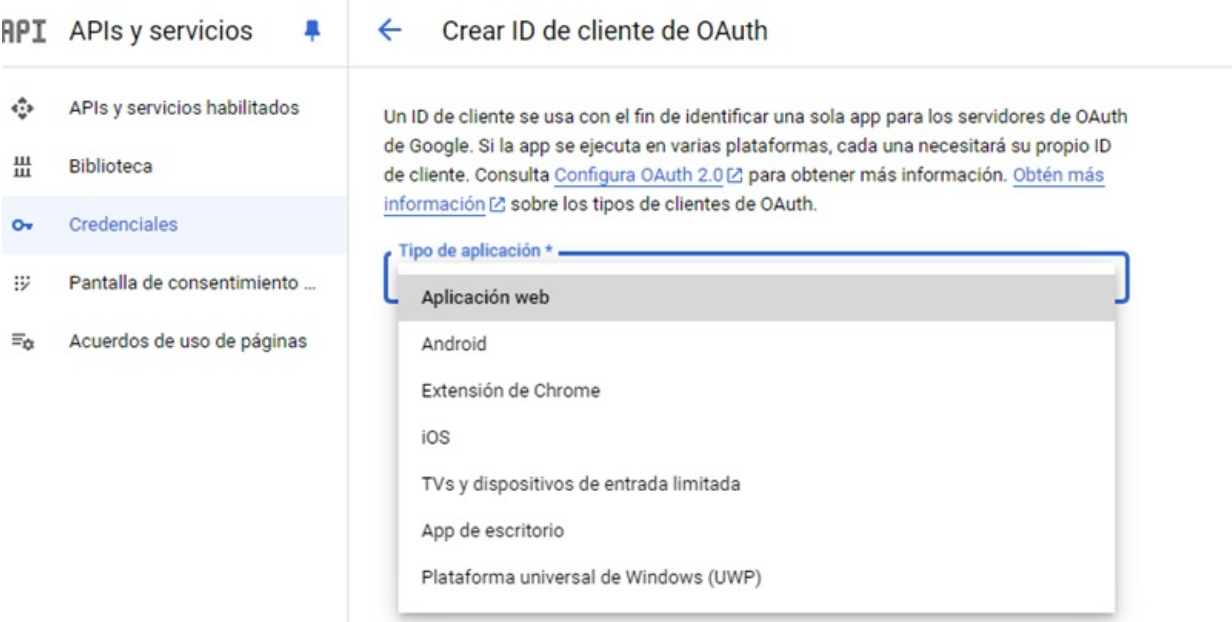
Correo electrónico

Nombre

Acciones

No hay cuentas de servicio para mostrar

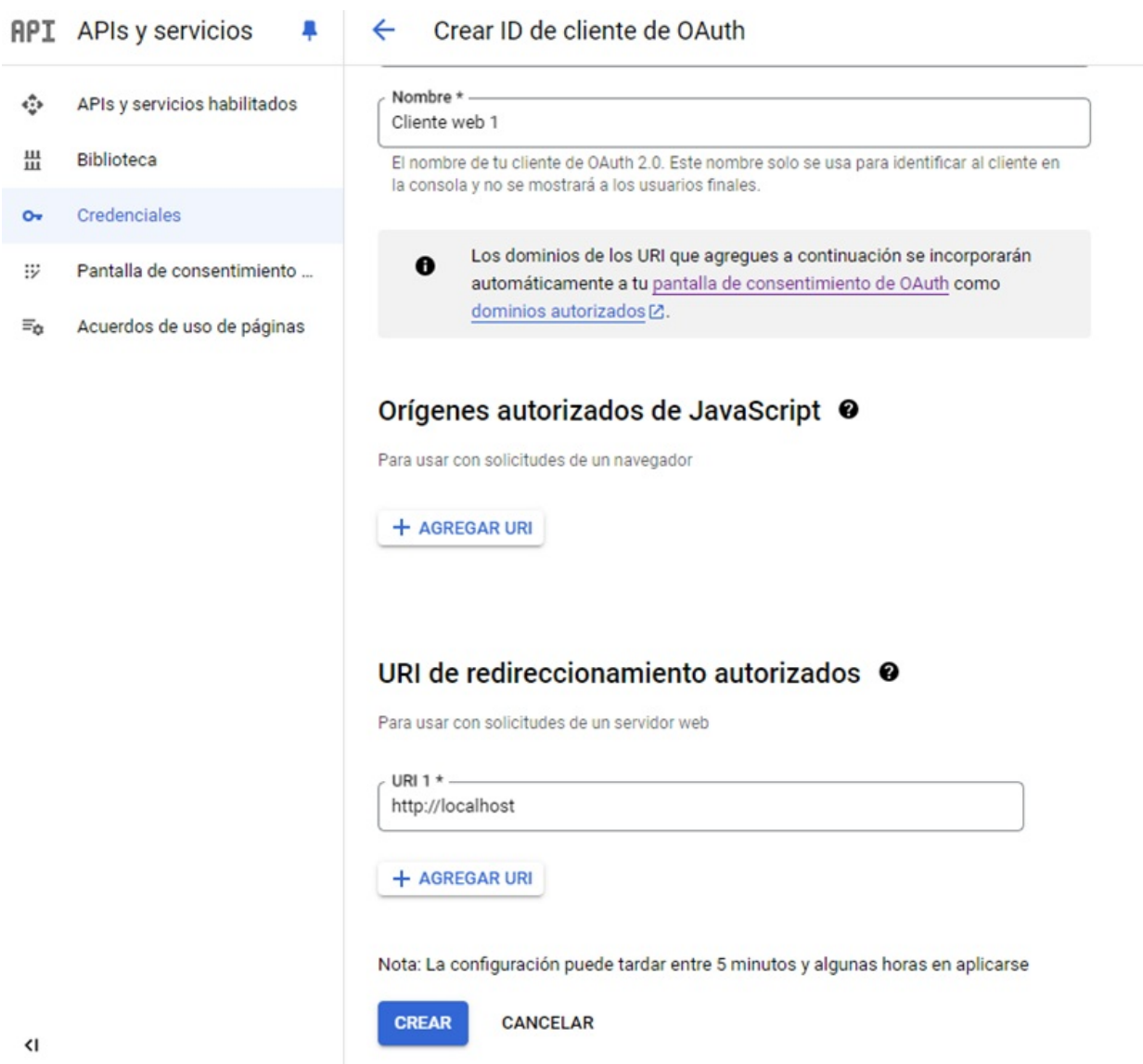
8. Na janela Criar ID do cliente OAuth No campo Tipo de aplicação, selecione o ícone Aplicação Web.



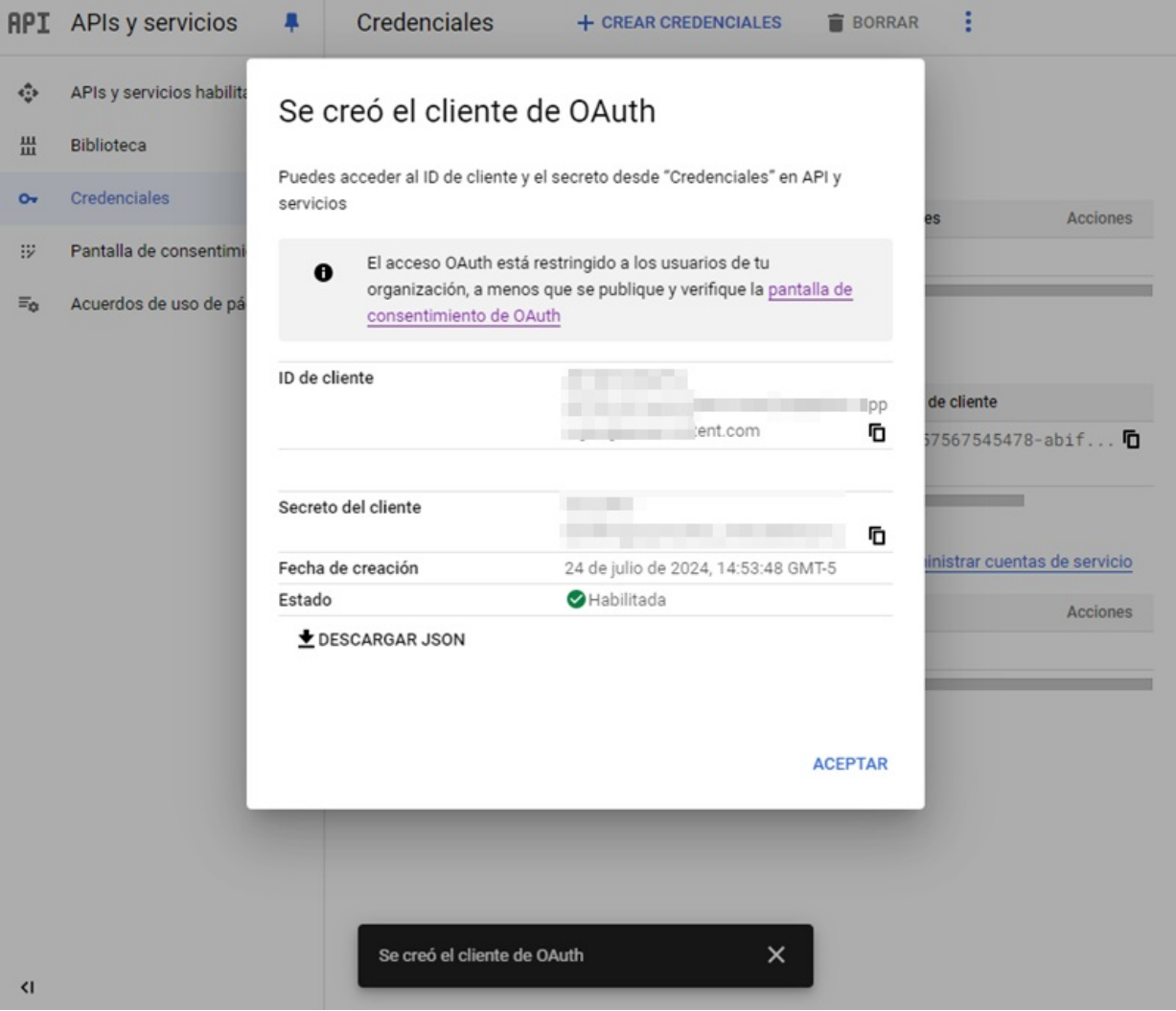
9. Na janela Criar ID do cliente OAuth No URLs de redirecionamento autorizados, insira o URL apropriado para o produto Gerenciamento de Serviços Aranda (ASMS) como segue:

- Servidor de saída: https://[domínio]/ASMSAdministrator/Principal/Páginas/OauthToken.aspx
- Servidor de entrada (Case Creator): (http://localhost)

Por fim, clique no botão CRIAR.



10. Na janela O cliente OAuth foi criado salvar os seguintes dados que são necessários para a configuração em aplicativos Aranda e na geração do [Token de atualização](#).

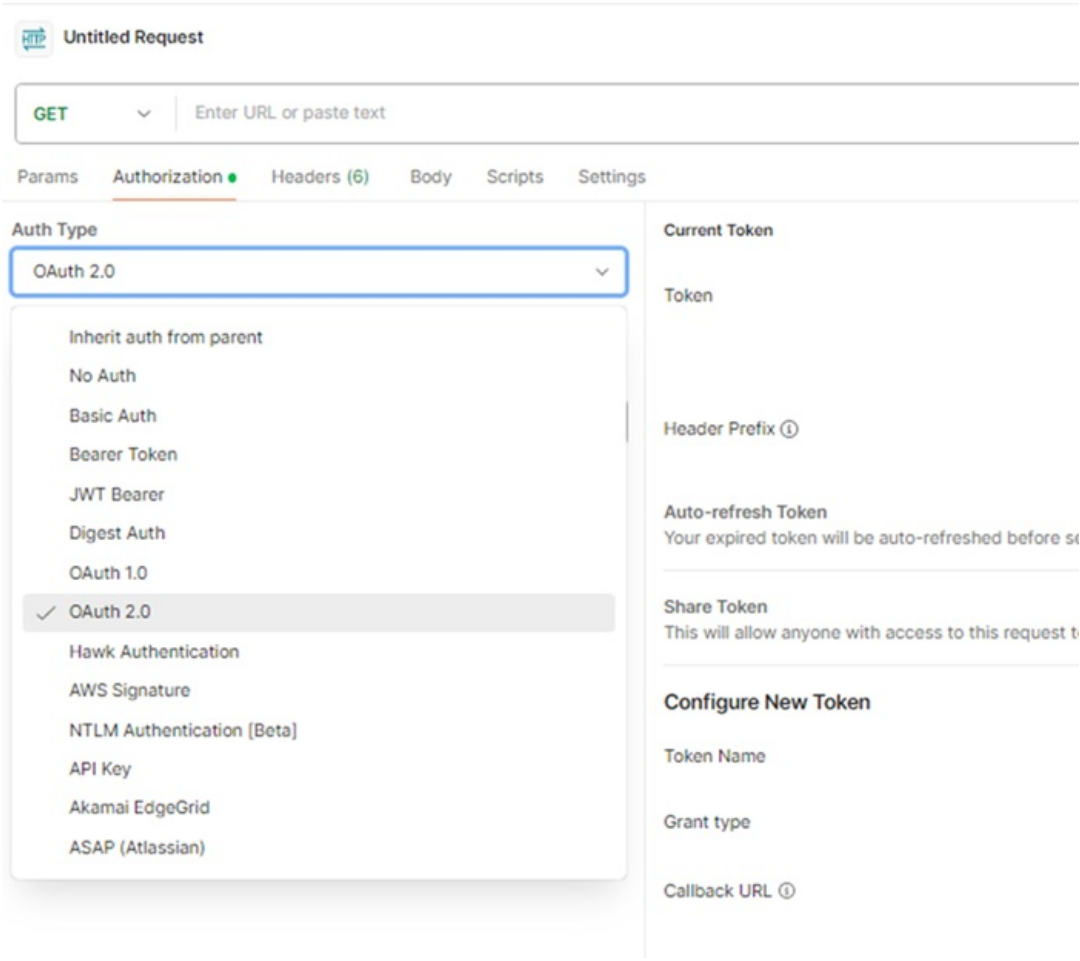


- ID do cliente -> ID do cliente.
- Valor do segredo do cliente - > segredo do cliente.
- -> URL do token `https://oauth2.googleapis.com/token`.
- URL de autorização -> `https://accounts.google.com/o/oauth2/v2/auth`

Aplicativo de token de atualização do Google

Para solicitação de refresh_ token, você deve usar o aplicativo da área de trabalho do Postman e executar as seguintes ações:

1. Crie uma nova coleção no Postman e selecione OAuth 2.0 no tipo de autorização.



2. Na exibição, insira os campos da seguinte maneira:

Untitled Request

GETEnter URL or paste text

ParamsAuthorizationHeaders (6)BodyScriptsSettings

Auth Type

OAuth 2.0

The authorization data will be automatically generated when you send the request. Learn more about [OAuth 2.0](#) authorization.

Add authorization data toRequest Headers

Current Token

TokenAvailable Tokens

Token

Header Prefix ⓘBearer

Auto-refresh Token
Your expired token will be auto-refreshed before sending a request.

Share Token
This will allow anyone with access to this request to view and use it.

Configure New Token

Token NamePruebas Google

Grant typeAuthorization Code

Callback URL ⓘhttp://localhost

☐ Authorize using browser

Auth URL ⓘhttps://accounts.google.com/o/oauth2/v2/t...

Access Token URL ⓘhttps://oauth2.googleapis.com/token

Client ID ⓘ

Client Secret ⓘ

Scope ⓘhttps://mail.google.com/

State ⓘState

Client Authentication ⓘSend as Basic Auth header

> Advanced

Clear cookies ⓘ

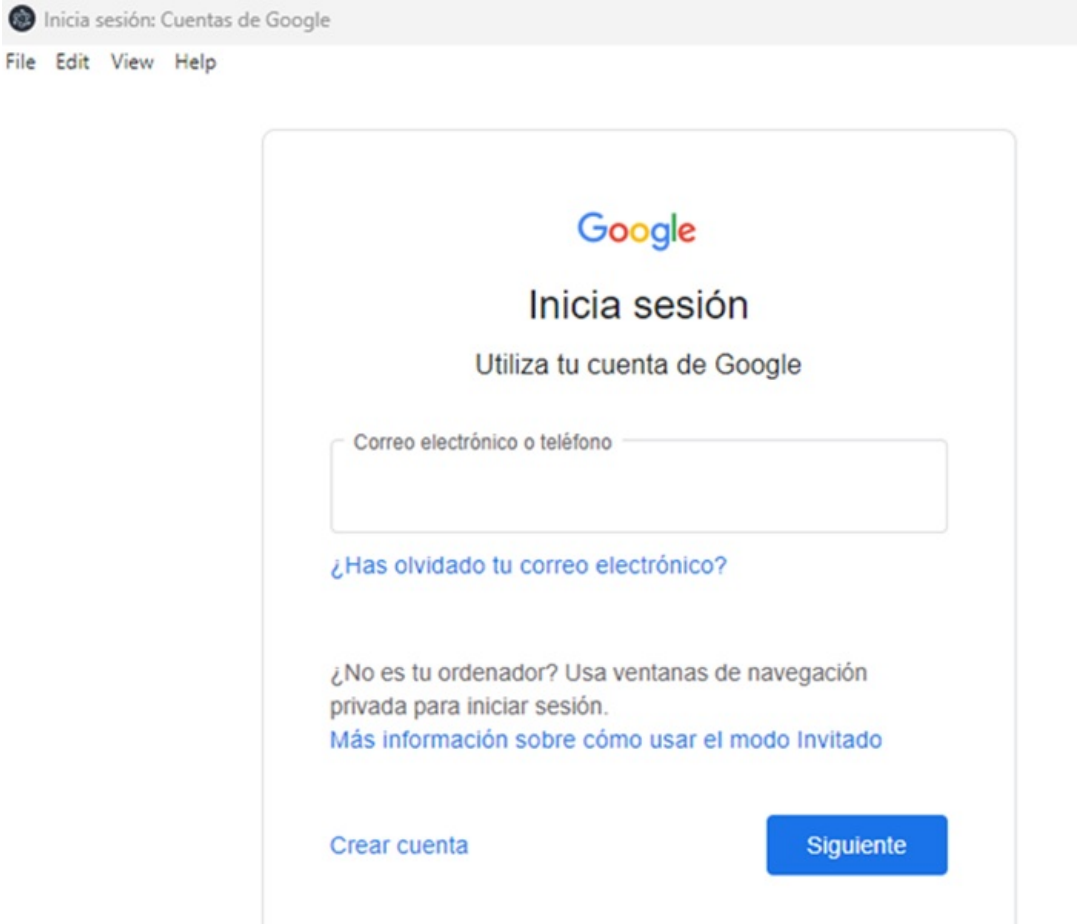
Get New Access Token

Campo	Descrição
Tipo	OAuth 2.0
Adicionar dados de autenticação a	Cabeçalhos de solicitação
Token de acesso	Token Disponível
Prefixo de cabeçalho	Portador
Nome do token	Nome que você deseja para o token
Ótimo tipo	Código de autorização
URL de retorno de chamada	http://localhost
URL de autenticação	https://accounts.google.com/o/oauth2/v2/auth?access_type=offline
URL do token de acesso	https://oauth2.googleapis.com/token
ID do cliente	Insira o valor de ID do aplicativo (cliente) .
Segredo do cliente	Entrar Valor secreto para o cliente .
Âmbito	https://mail.google.com/
Estado	Pode ser deixado em branco.
Autenticação de cliente	Enviar como cabeçalho de autenticação básica

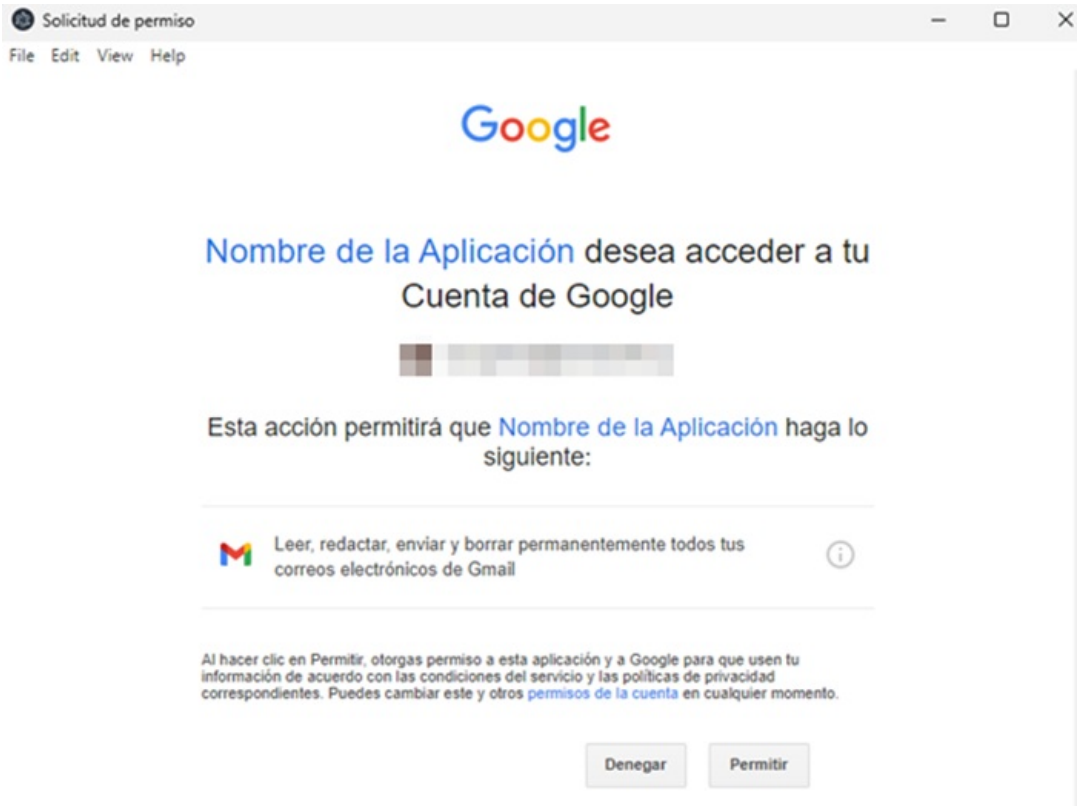
3. Ao inserir todas as informações, selecione Obter novo token de acesso.

📌 Nota: Para garantir a geração correta do Refresh_Token, verifique as URLs inseridas e certifique-se de que elas não contenham quebras de linha ou espaços em branco, tanto no início quanto no final.

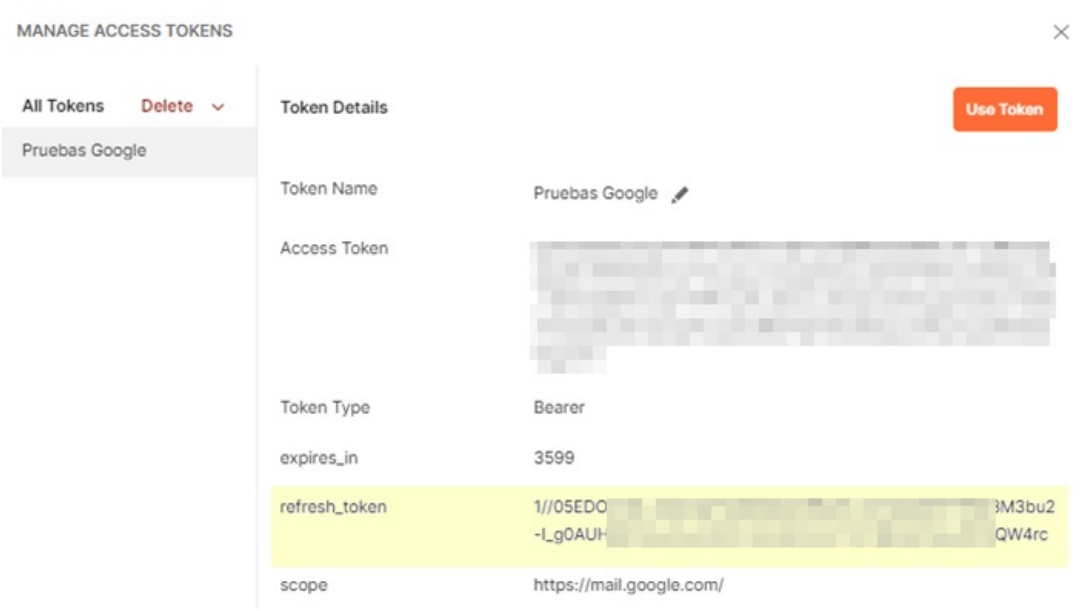
4. A janela de login da Conta do Google está ativada; Insira o e-mail e a senha para os quais o Token de Atualização deve ser gerado.



5. A sessão deve ser realizada com contas associadas à organização; Se a entrada for bem-sucedida, a sessão solicitará que eles aceitem as permissões necessárias.



5. Ao aceitar permissões, copie e salve o refresh_token, pois ele será usado nas configurações do criador de e-mail e caso nos aplicativos Aranda.



- 📌 Nota: Um token de atualização pode parar de funcionar por motivos como:
- O usuário revoga as permissões do aplicativo.
 - O token de atualização não é usado por seis meses.
 - O usuário alterou a senha e o token de atualização contém permissões do Gmail.
 - A conta de usuário excedeu a quantidade máxima de tokens de atualização (ativos) concedidos.
- Para obter mais informações, consulte a documentação do Google: [Expiração do token de atualização](#)

Gerenciamento de servidor de e-mail

Exibir servidor de e-mail

1. Na visualização de informações do servidor de e-mail, você pode exibir a lista de servidores agrupados por dados básicos do servidor de e-mail e o tipo de autenticação.

Servidor de correo

Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

Buscar todos los conceptos

NUEVO

ELIMINAR

☐	Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
☐	OU outlook	outlookoffice365.com	Basic	Diana Cortes	diana.cortes@arandasoft.c...
☐	SN servidor Notificaciones	smtppoffice365.com	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...
☐	SC Servidor Correo	https://dev-components-net...	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...

<1>

Mostrando 1 al 3 de 3 registros

2. Na visualização de informações do servidor de e-mail, você terá ações de gerenciamento de informações e organização habilitadas.[Visualização de informações no ambiente do Commons](#)

Links Relacionados:

- [Criar servidor de e-mail](#)
- [Editar servidor de e-mail](#)
- [Excluir servidor de e-mail](#)

Criar servidor de e-mail

1. Na visualização de informações do servidor de e-mail, selecione o Novo

Servidor de correo

Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

Buscar todos los conceptos

NUEVO

ELIMINAR

☐	Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
☐	OU outlook	outlookoffice365.com	Basic	Diana Cortes	diana.cortes@arandasoft.c...
☐	SN servidor Notificaciones	smtppoffice365.com	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...
☐	SC Servidor Correo	https://dev-components-net...	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...

<1>

Mostrando 1 al 3 de 3 registros

Fatos básicos

2. Na janela habilitada, você poderá preencher os dados básicos do servidor de e-mail e o tipo de autenticação

3. Nos dados básicos do servidor, você poderá inserir campos como nome, servidor, porta, nome e e-mail do remetente.

Cada um dos campos de serviços de diretório deve levar em conta o [Especificações para campos comuns](#)

Servidor de correo

Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

*Nombre del correo

*Servidor

*Puerto

0

Nombre del remitente

Correo del remitente

Establecer por defecto

NO

Habilitar SSL

NO

Tipo de autenticación

Selección el tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar

Básica

Oauth

Regulere autenticación

NO

4. No Tipo de autenticação, você pode selecionar as opções disponíveis por tipo de provedor:

- Autenticação básica
- Autenticação Oauth

Autenticação básica

5. Para Autenticação Básica, habilite o Requer autenticação e digite o login do servidor de e-mail e a senha necessária.

Servidor de correo

Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

*Nombre del correo

*Servidor

*Puerto

0

Nombre del remitente

Correo del remitente

Establecer por defecto

NO

Habilitar SSL

NO

Tipo de autenticación

Selección el tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar

Básica

Oauth

Regulere autenticación

SI

Los campos con * son obligatorios

*Usuario

*Contraseña

Autenticação Oauth (Autorização Aberta)

6. Para autenticação OAuth, defina um provedor de autenticação (Microsoft, Google, Configuração Manual).

Nota: Sim Microsoft é o provedor de autenticação, pré-configure as informações relevantes para o provedor de email Oauth no portal do Azure, gerando os parâmetros necessários para os campos de autenticação do servidor de email:

- [ID do cliente, URL de autorização e URL do token](#)
- [Segredo do cliente](#)
- [Token de acesso e token de atualização](#).

Nota: Sim Pesquise no Google Se você for o provedor de autenticação, poderá pré-configurar as informações relevantes para o provedor de e-mail Oauth no portal do Google, gerando os parâmetros necessários para os campos de autenticação do servidor de e-mail:

- [ID do cliente, URL de autorização, URL do token e segredo do cliente](#)
- [Token de acesso e token de atualização](#).

Tipo de autenticación

Selección el tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar

Básica

Oauth

Proveedor

Microsoft

Los campos con * son obligatorios

*ID Cliente

*Secreto del cliente (contraseña)

*URL de autorización

*URL de token

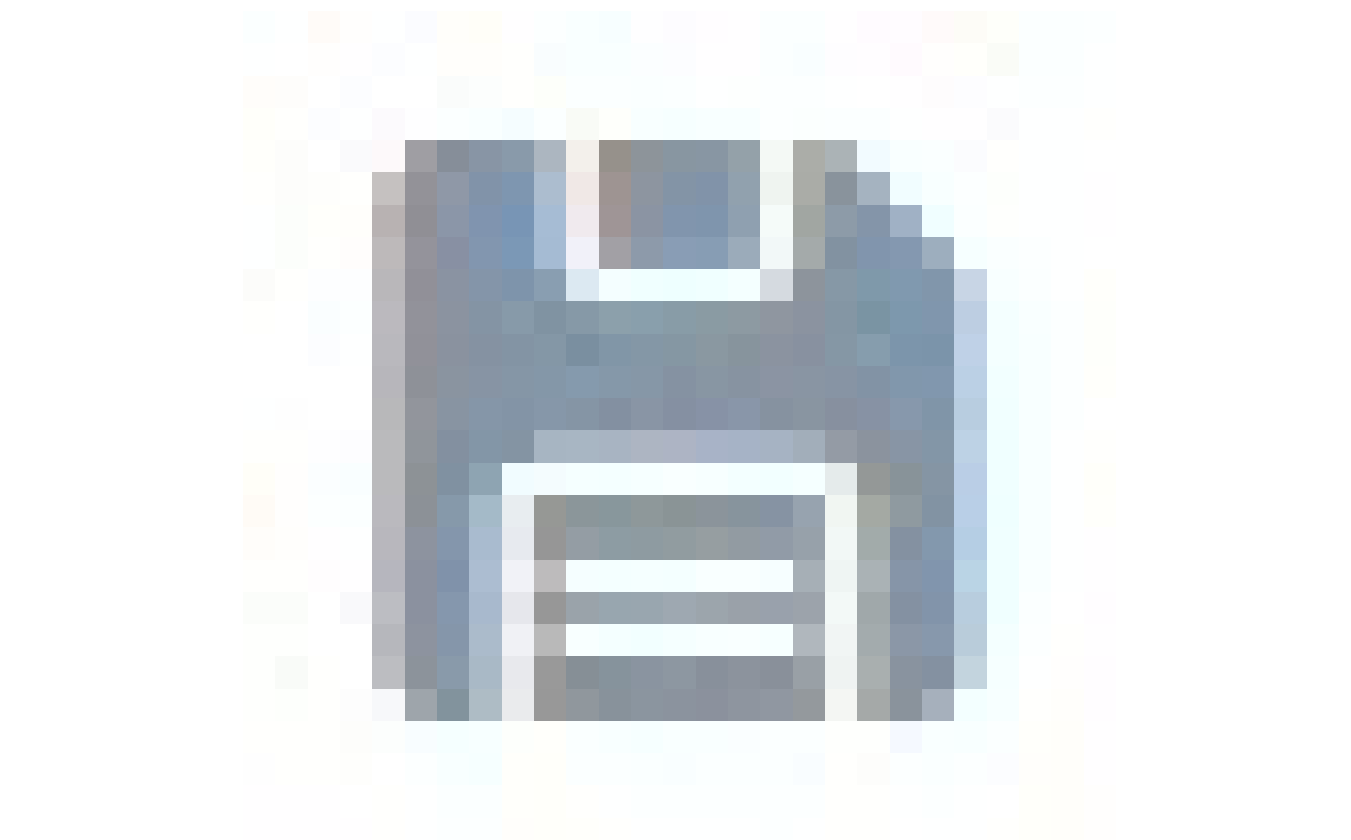
*Token de acceso

*Token de actualización

7. Se a conexão for com um provedor que não seja a Microsoft ou o Google, você poderá estabelecer o Configuração manual 8. Para cada fornecedor você pode definir os campos obrigatórios, como ID do cliente, segredo do cliente, URL de autorização, entre outros.

Cada um dos campos do servidor de e-mail para o tipo de autenticação Oauth deve ser levado em consideração [Especificações para campos comuns](#).

9. Quando terminar de configurar o servidor de e-mail, clique no botão Salvar

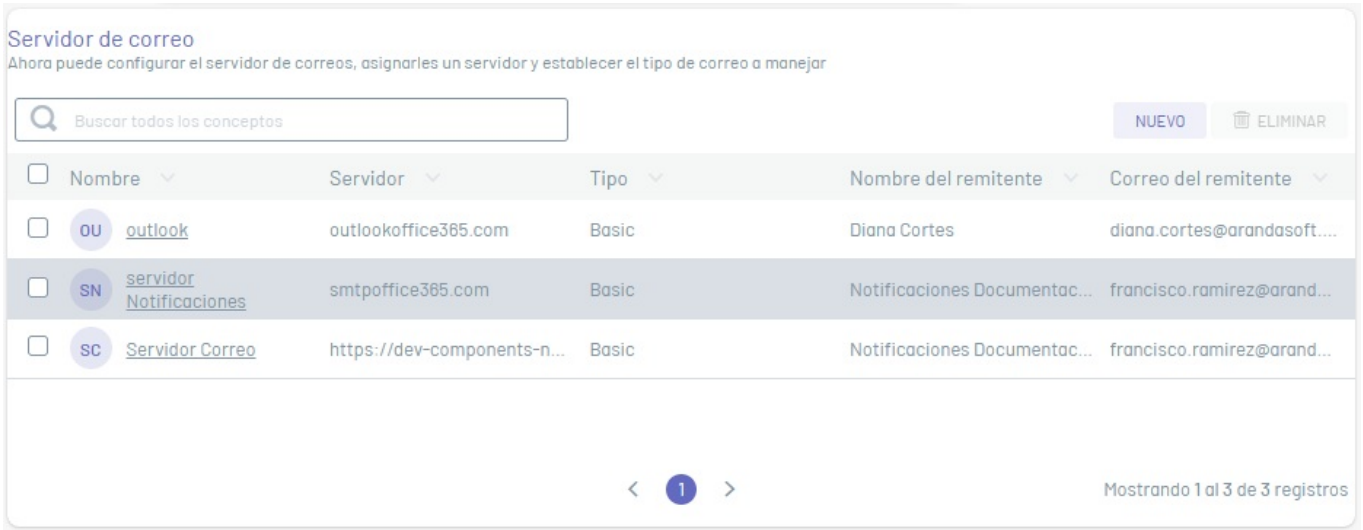


para confirmar as alterações feitas.

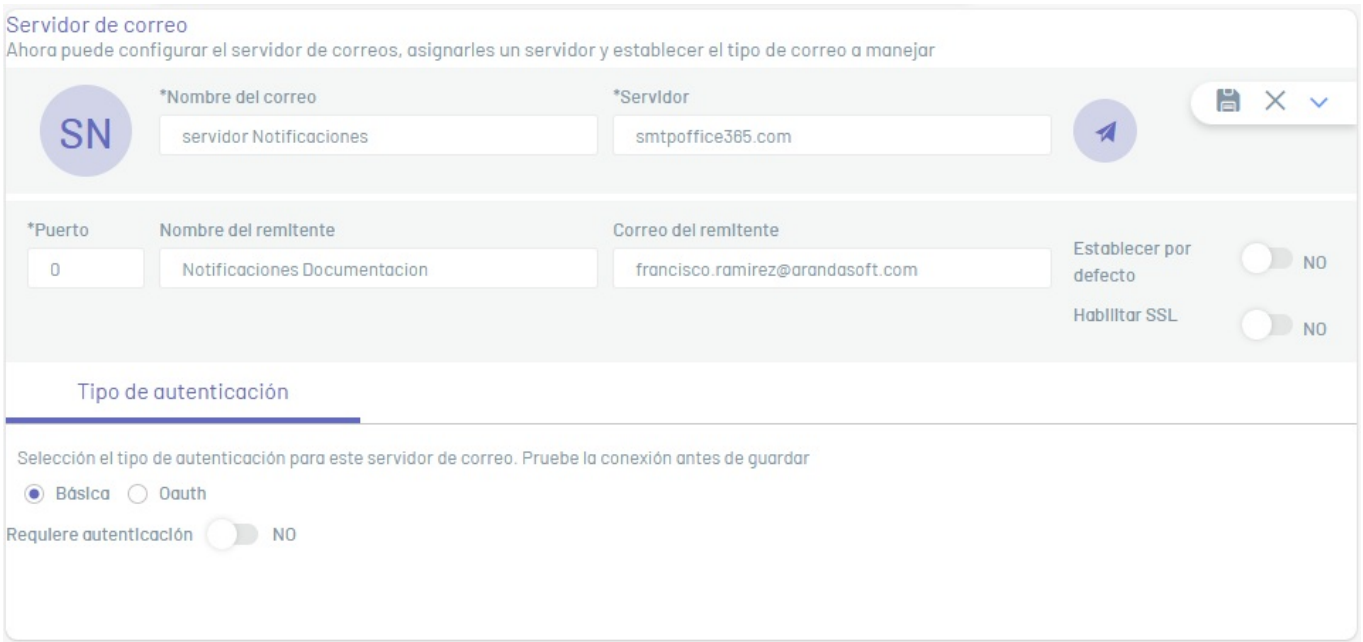
Nota: Se você tiver criado mais de uma configuração de servidor de e-mail, apenas uma delas poderá ser marcada como uma configuração Por padrão.

Editar servidor de e-mail

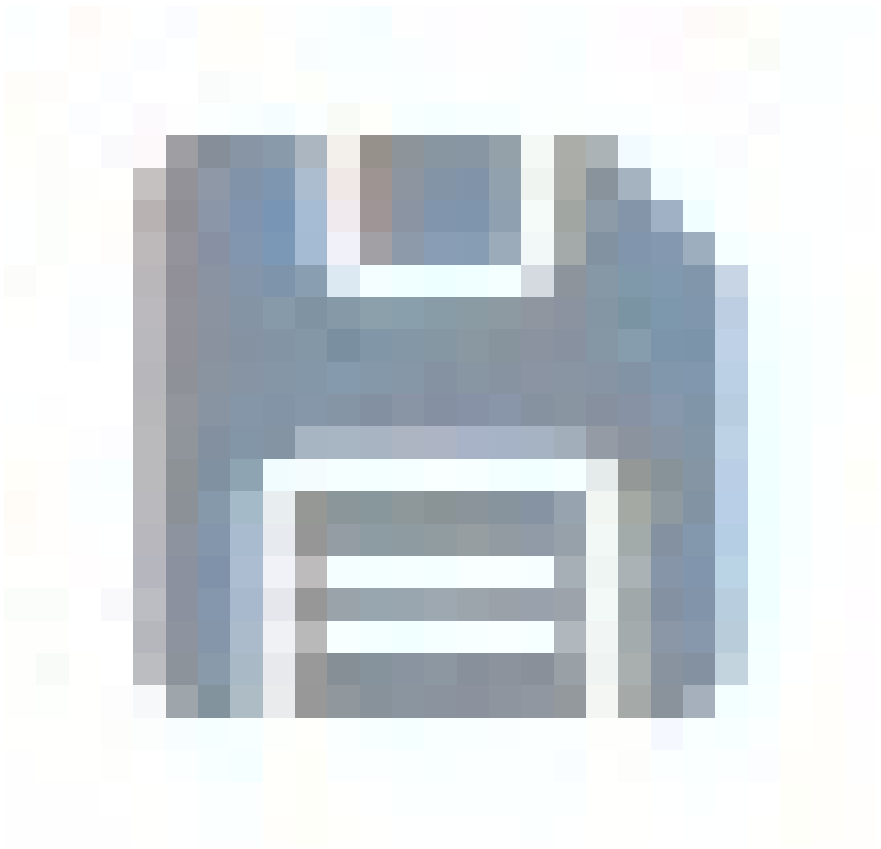
1. Para editar um servidor de e-mail, no modo de exibição Informações do Servidor, selecione um registro na lista de e-mails existente.



2. A janela Servidor de e-mail está ativada, onde você pode modificar os dados básicos do servidor de e-mail ou tipo de autenticação.



3. Quando terminar de editar o servidor de e-mail, clique no botão Salvar



para confirmar as alterações feitas.

Excluir servidor de e-mail

1. Na visualização Informações do Servidor de Email, selecione um registro na lista de serviços de email que você deseja excluir e clique no botão



Servidor de correo

Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

Q

Buscar todos los conceptos

NUEVO

ELIMINAR

☐	Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
☐	ou outlook	outlookoffice365.com	Basic	Diana Cortes	diana.cortes@arandasoft.c...
☒	SN servidor Notificaciones	smtpoffice365.com	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...
☐	SC Servidor Correo	https://dev-components-net...	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...

<

1

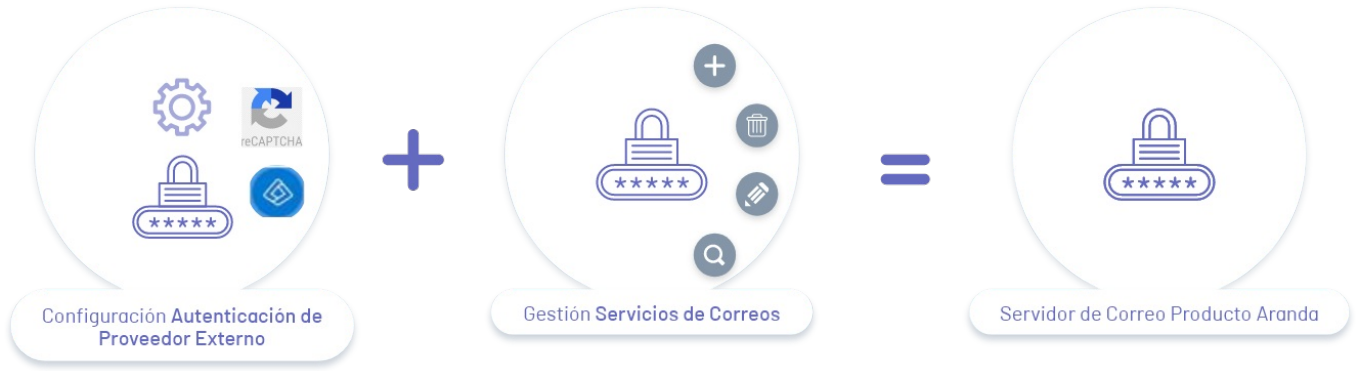
>

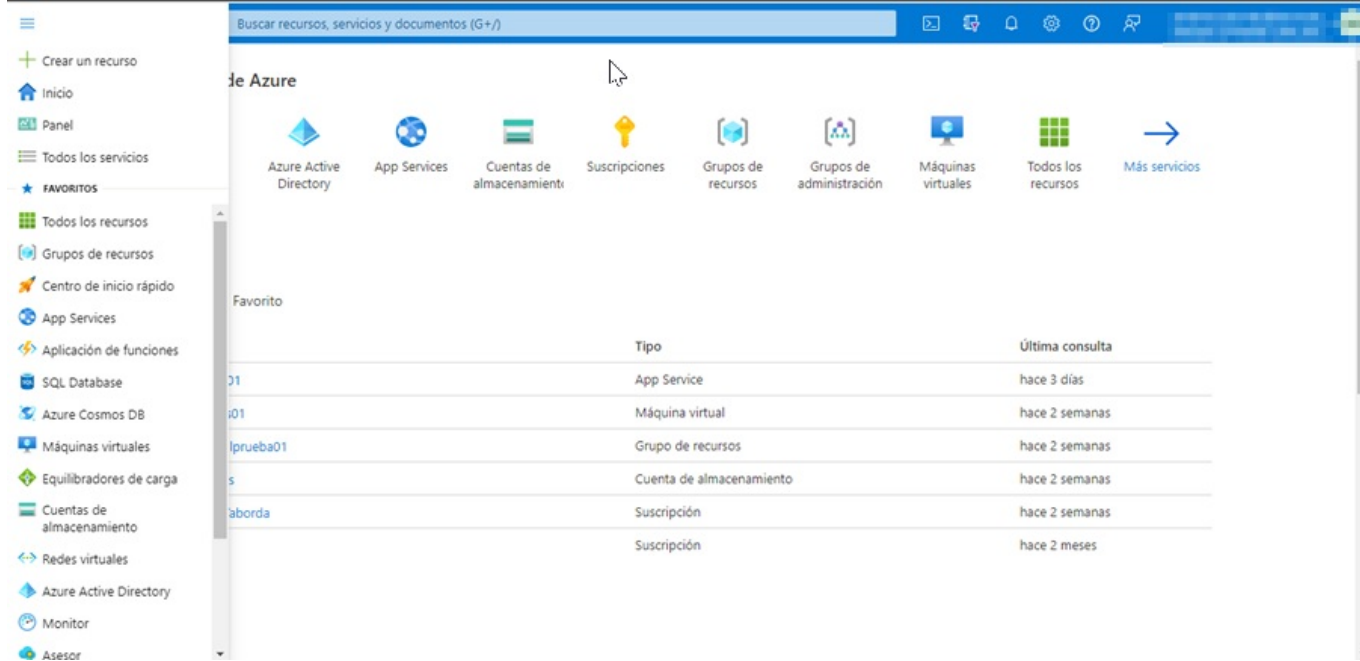
Mostrando 1 al 3 de 3 registros

2. Você poderá exibir uma mensagem de confirmação para validar a ação de exclusão.

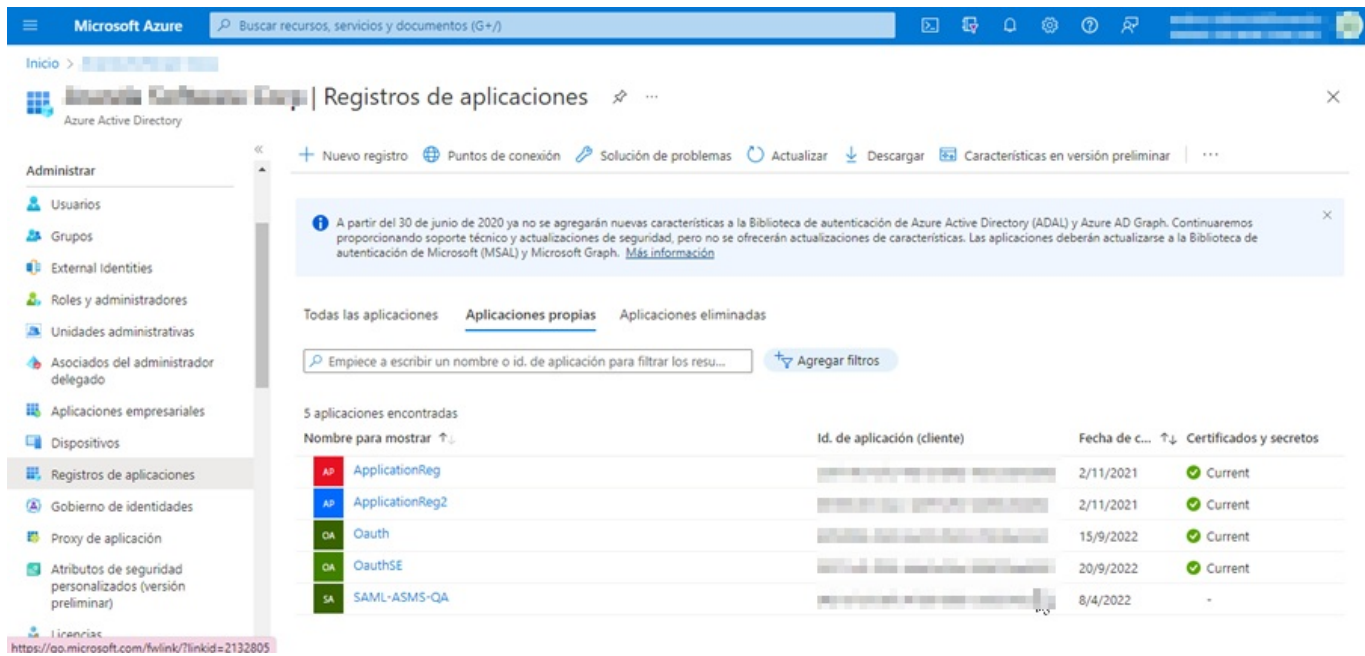
Módulo de serviço de diretório

Serviços de diretório de pré-configuração

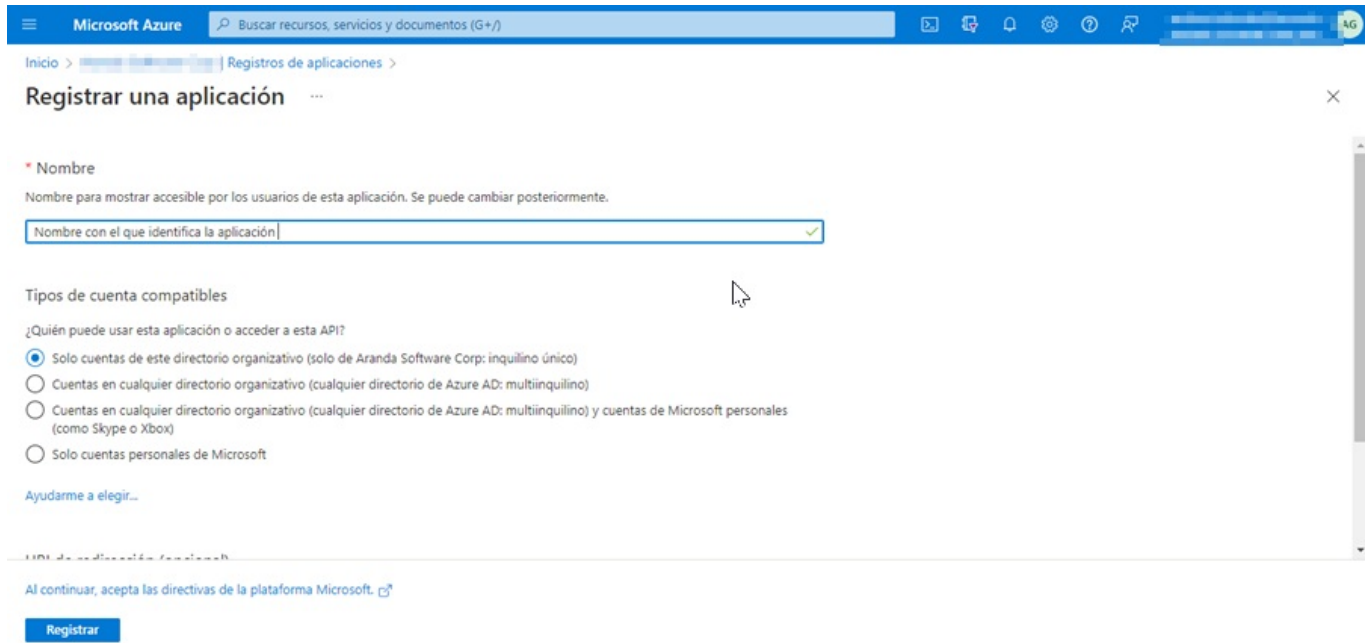




2. . No Administrar Pesquise e selecione Logs do aplicativoclique Novo Cadastro.



3. O campo de nome é preenchido e a opção desejada é selecionada em (Tipos de conta suportados), clique em Registro.

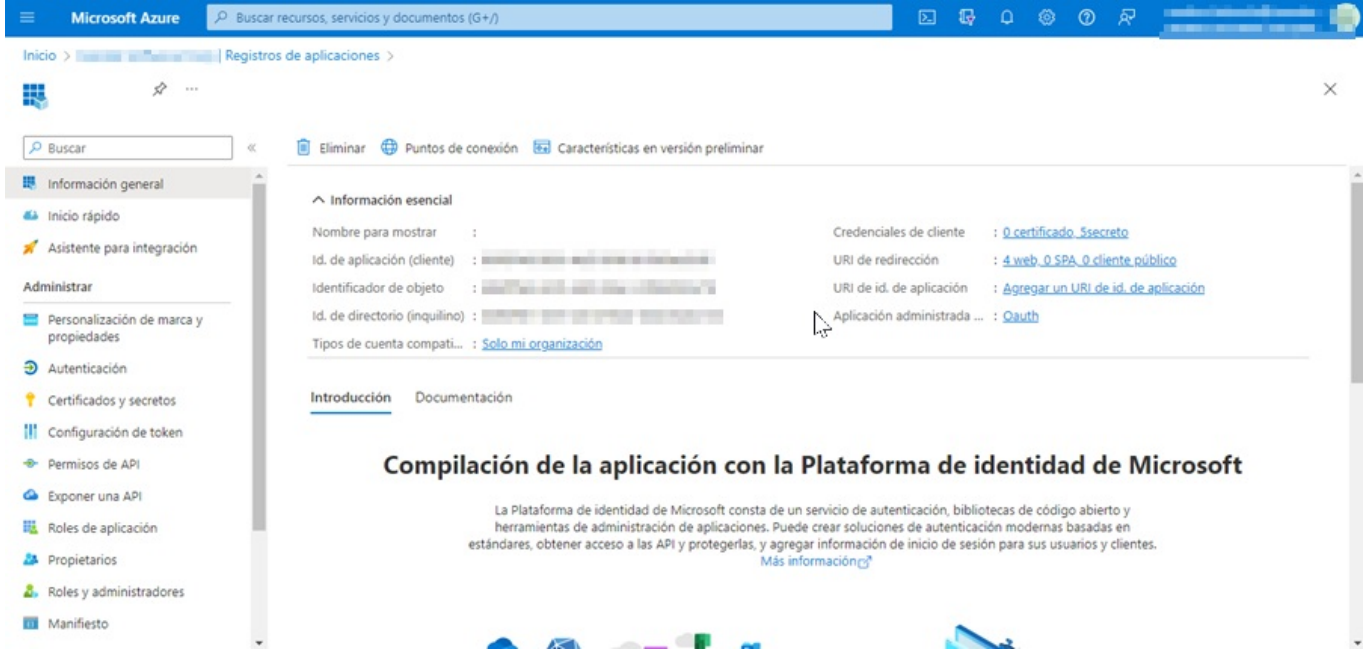


4.Quando o aplicativo estiver registrado, salve os seguintes dados necessários para a configuração na sincronização LDAP com o Microsoft Entra ID.

- ID do diretório (locatário)= URL

↳ Nota: A URL deve ser configurada da seguinte maneira: (https://login.microsoftonline.com/ + ID do locatário/diretório)

- ID do aplicativo (cliente)= ID do cliente

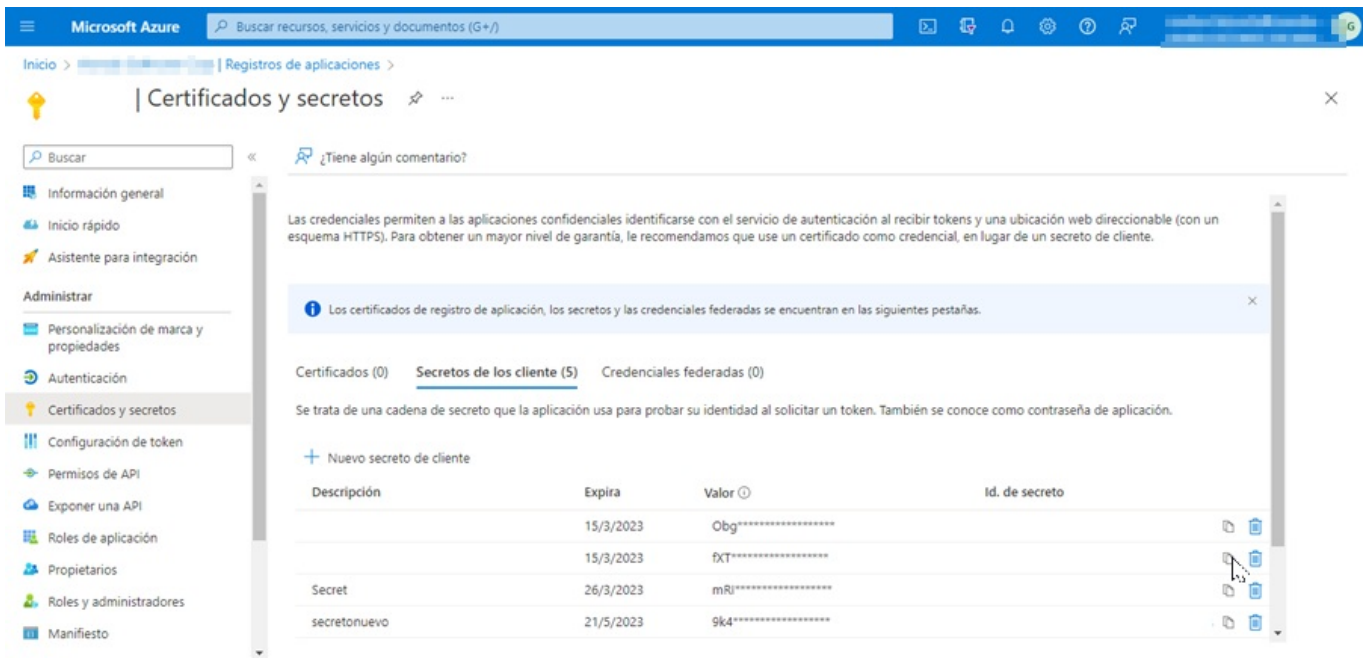


Configurar o aplicativo do Azure

Depois de criar o aplicativo e salvar os dados, você pode configurá-lo da seguinte maneira:

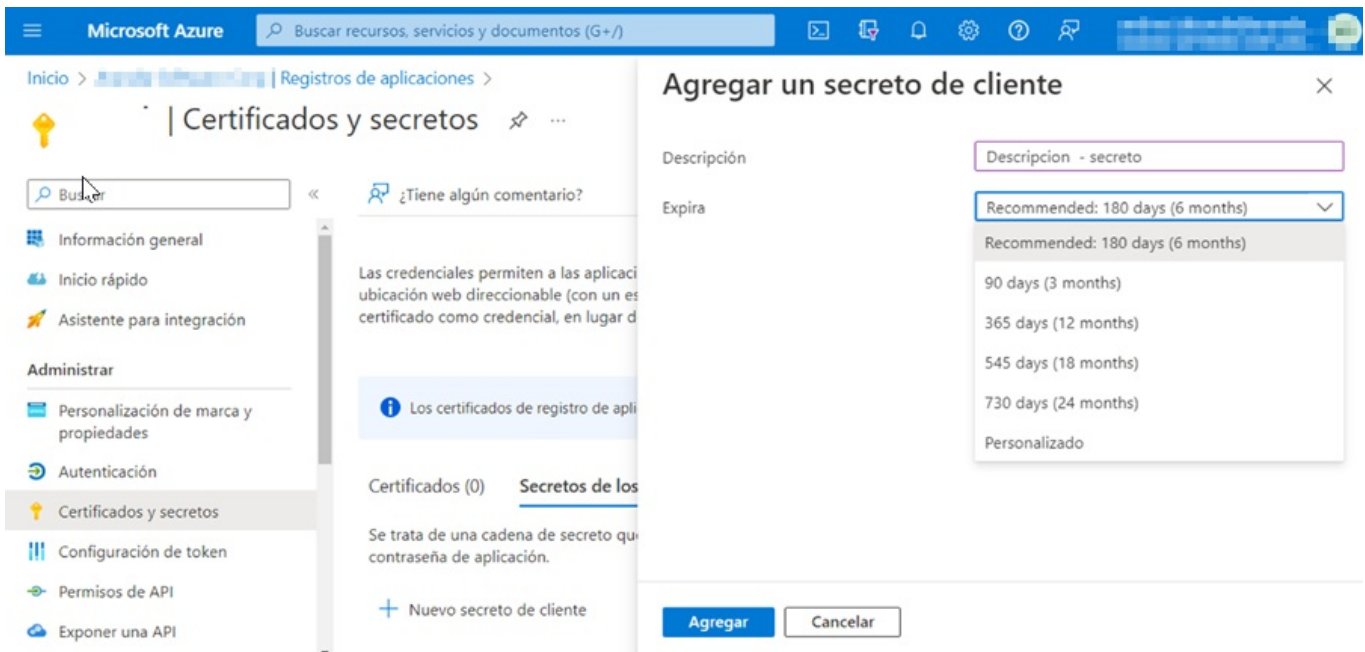
Criação do Segredo

- 1. Para criar o segredo, faça login no portal do Azure > Menu Microsoft> Insira a ID > Registros de Aplicativo > selecione o aplicativo criado na lista disponível.
- 2. No Administrar Selecione a opção Certificados e segredos > e, na visualização de informações, clique no ícone Novo segredo do cliente.



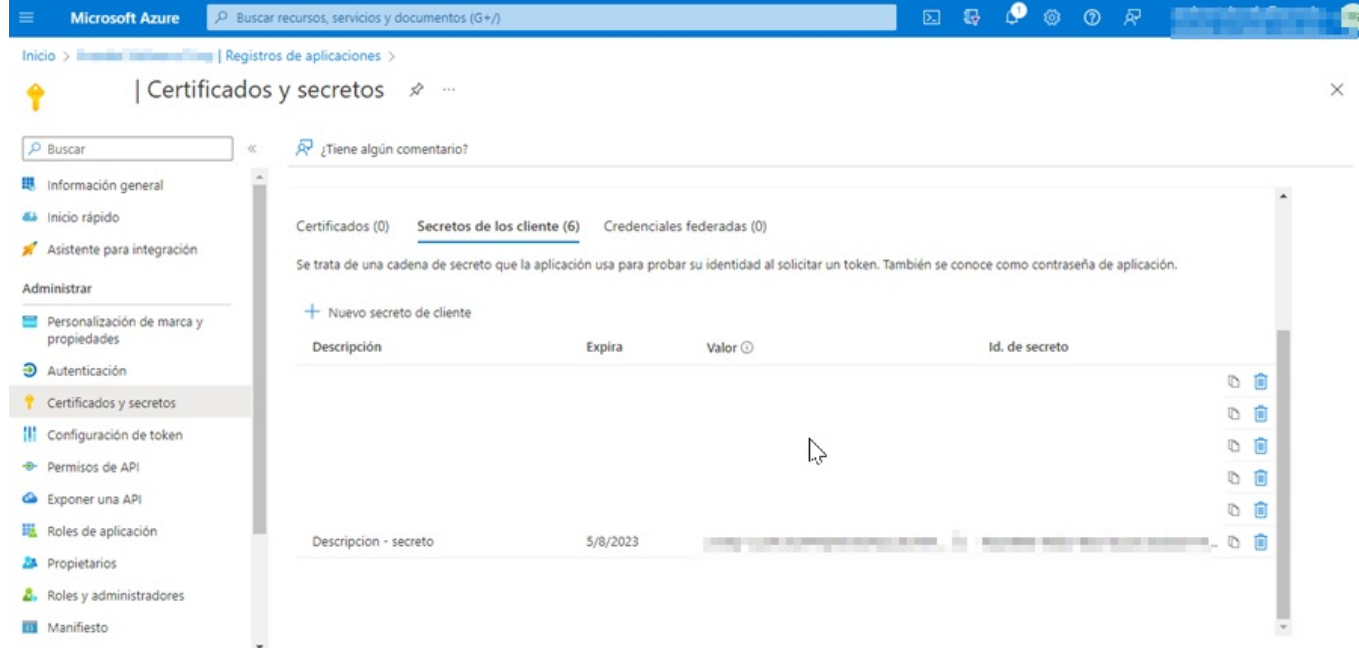
- 3. Na janela Adicionar um segredo do cliente Preencha o campo Descrição, defina a duração do segredo no campo Expira e clique no ícone Adicionar.

▮ Nota: Recomenda-se não esquecer o tempo de duração configurado. Em caso de expiração, se não for atualizado, a autenticação falhará



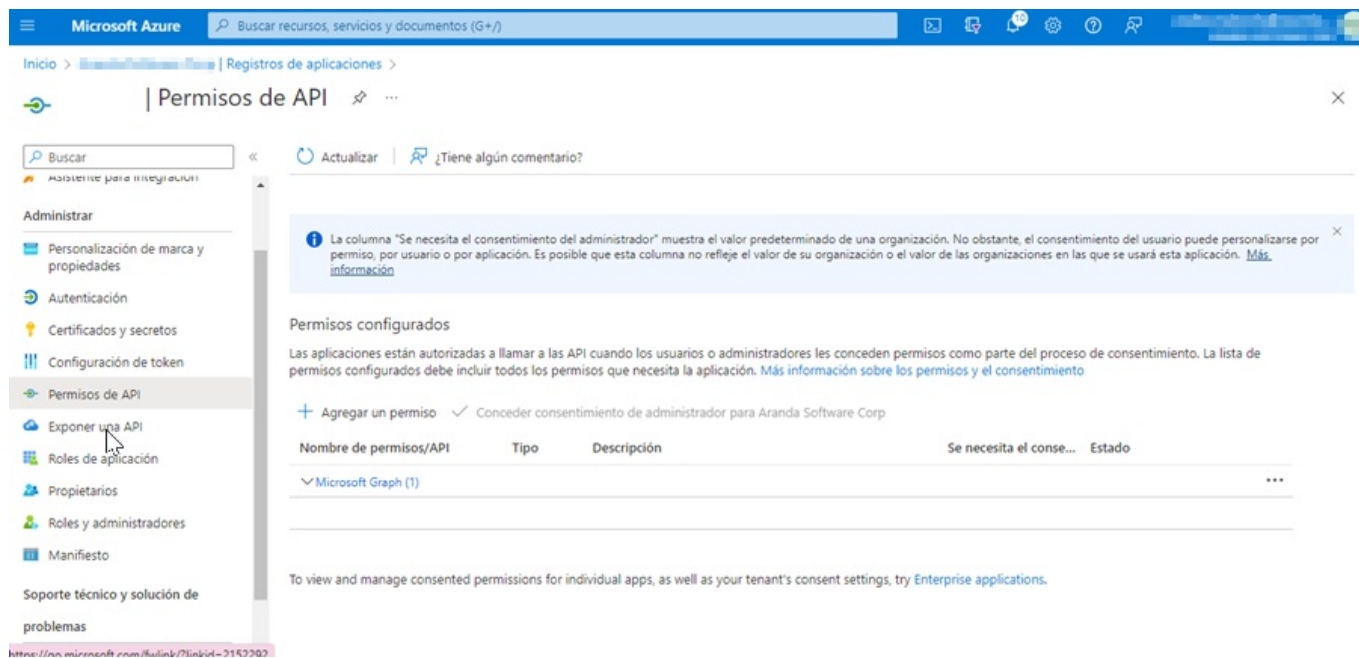
- 4. O valor do sigilo só é visível quando é criado; devem ser salvos para uso posterior ou referenciados durante as configurações necessárias nos produtos Aranda.

- Valor secreto para o cliente = Cliente Secreto.

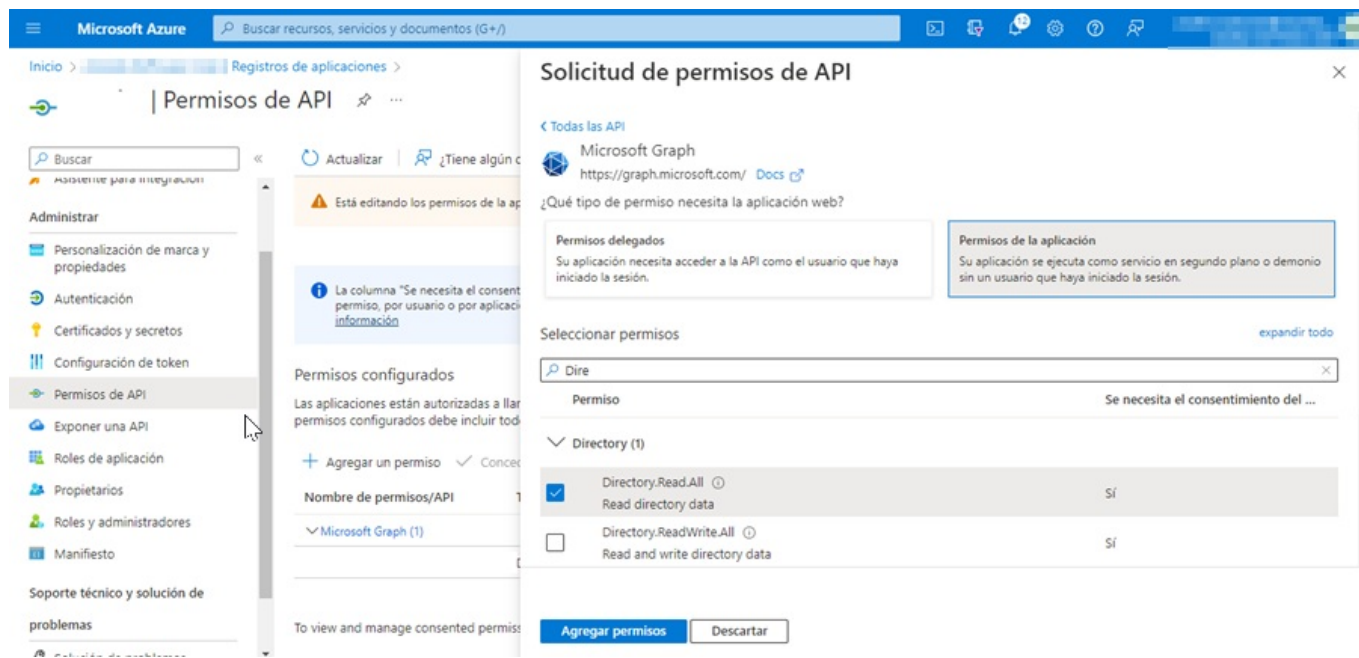


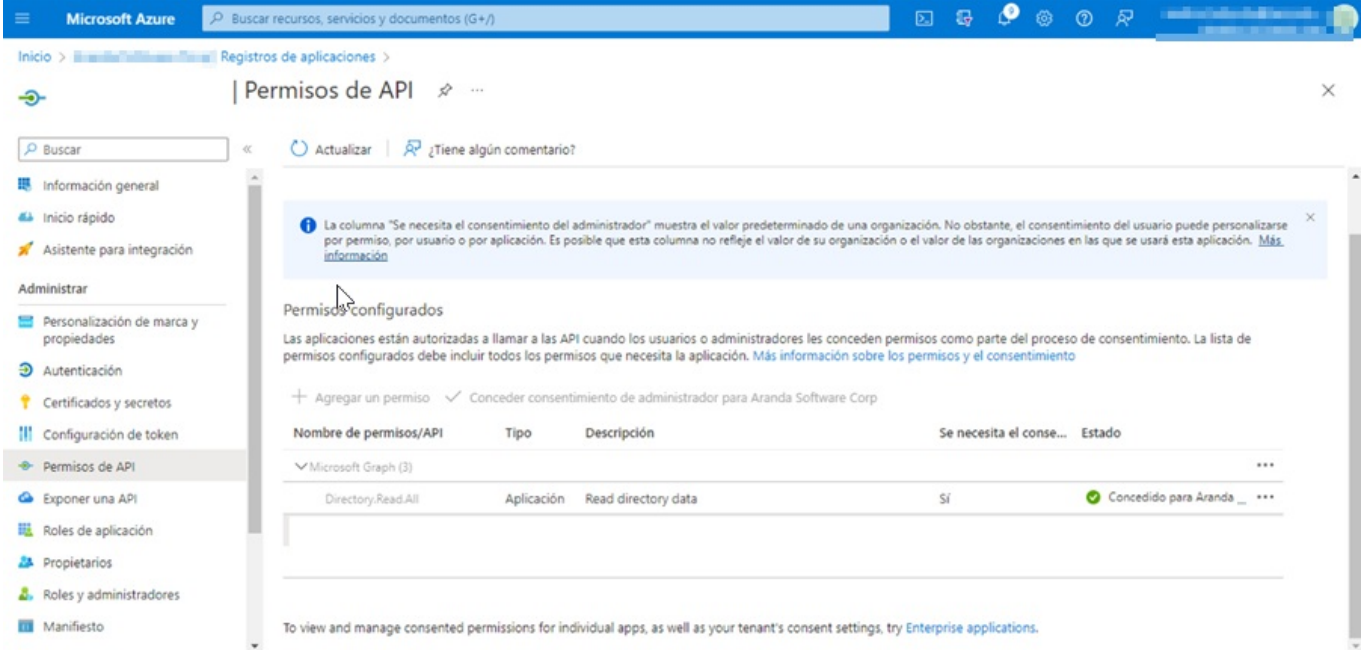
Configurar permissões de API

- 1. Para configurar permissões de API, insira o portal do Azure > Menu Inserir ID > Registros de Aplicativo > Microsoft > selecione o aplicativo criado na lista disponível.
- 2. No Administrar No menu principal, selecione o icone Permissões de API > e, na visualização de informações, na seção Permissões Configuradas, clique em Adicionar uma permissão.



- 3. Na janela Solicitar permissões de API, selecione o icone Microsoft Graph > e então Permissões de aplicativo, habilite as permissões de acordo com seus requisitos: Diretório.Read.All (Ler dados do diretório). Clique Adicionar permissão.





Depois que esse processo for concluído, você poderá concluir a sincronização com o Azure AD.

Sincronização de ID LDAP/Microsoft Entra

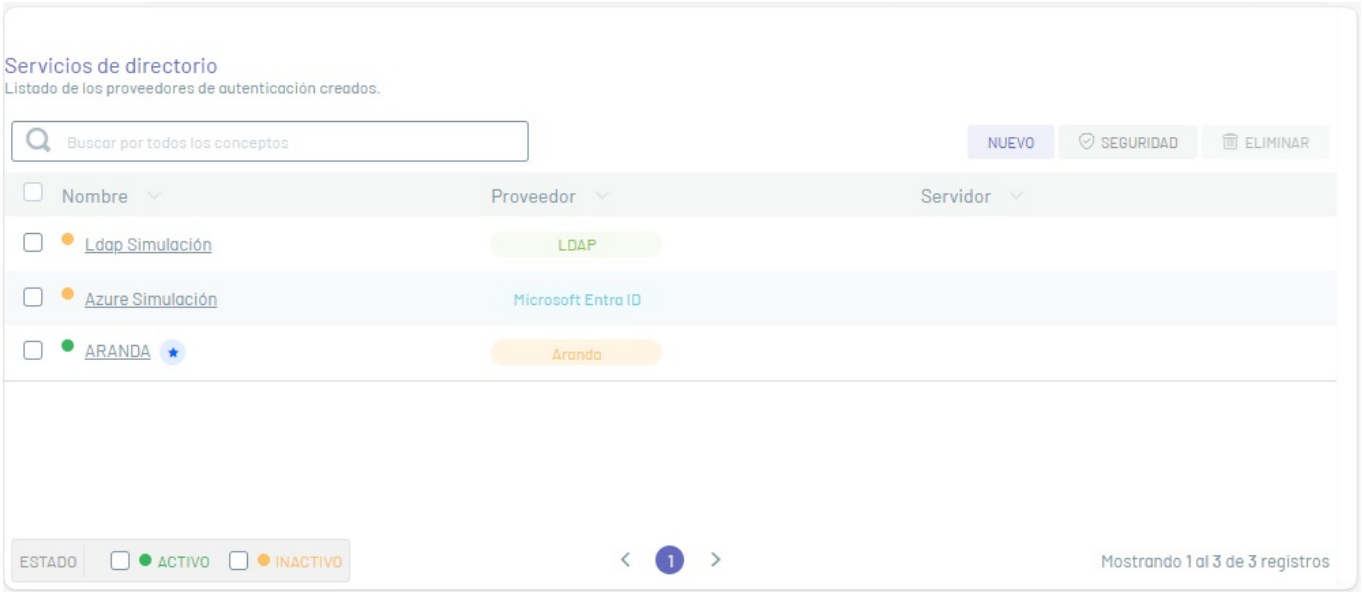
Para configurar o Ldap com o Microsoft Entra ID em aplicativos Aranda, verifique o seguinte link:

- [Consulte Sincronização e configuração do ASMS do Aranda Service Management](#)

Gestão de serviços de diretório

Exibir serviço de diretório

1. Na exibição de informações do Serviço de Diretório, você pode exibir a lista de provedores de autenticação, agrupados por dados como:



Campo	Tipo de campo	Descrição
Nome	Texto	O nome pelo qual o serviço de diretório é identificado.
Fornecedor	Texto	Tipo de serviço de diretório.
Servidor	Texto	Nome e/ou IP onde o domínio está localizado.

- ▮ Nota: A coluna Fornecedor indica o tipo de provedor de serviços de diretório; que pode ser Aranda, LDAP e ID de inserção da Microsoft
- ▮ Nota: Através do provedor interno ArandaÉ possível [Configurar especificações para políticas de senha](#) para o acesso de Aranda.

2. Na exibição de informações dos serviços de diretório, você terá as ações de gerenciamento e organização de informações habilitadas.[Visualização de informações no ambiente do Commons](#)

- Links Relacionados:
- [Criar serviço de diretório](#)
 - [Editar serviço de diretório](#)
 - [Excluir serviço de diretório](#)

Criar serviços de diretório

1. Na visualização de informações do servidor de diretório, selecione o ícone Novo.

Servicios de directorio

Listado de los proveedores de autenticación creados.

Q

Buscar por todos los conceptos

NUEVO

SEGURIDAD

ELIMINAR

☐	Nombre	Proveedor	Servidor
☐	pruebaADM	External	192.168.3.2
☐	Ldap	LDAP	
☐	Azure	Microsoft Entra ID	
☐	ARANDA	Aranda	

ESTADO

☐ ACTIVO

☐ INACTIVO

<

1

>

Mostrando 1 al 4 de 4 registros

Fatos básicos

2. Na janela habilitada, você poderá preencher as informações básicas necessárias para estabelecer a conexão com seu servidor de diretório, como nome, servidor, porta, tipo de autenticação, provedores, entre outros.

Cada um dos campos de serviços de diretório deve levar em conta o [Especificações para campos comuns](#)

NC

Nombre completo

INACTIVO

*Nombre completo

*Servidor LDAP

*Puerto

*Tipo de autenticación

Seleccione

*Formato de usuario

Seleccione

Estado

Inactivo

Seleccione el tipo de autenticación

Seleccione el proveedor por el que va crear el tipo de autenticación

LDAP

Cree uno o varios directorios empresariales.

Microsoft Entra ID

Importar usuario de office 365.

Utilizar proveedor por defecto

Usar distinción de nombre DN

Habilitar SSL

IMPORTAR

Tipo de autenticação

4. No Tipo de autenticação, você pode definir o tipo de provedor para autenticação:

- [LDAP](#): É um protocolo de aplicativo padrão para consultas, que pode armazenar, gerenciar, proteger e autenticar informações do usuário.
- [Microsoft EntraID](#): O serviço de gerenciamento de identidade baseado em nuvem da Microsoft, do qual os usuários do Office 365 podem ser importados

Provedor LDAP

5. Na visualização Detalhes do fornecedor, clique no botão IMPORTAÇÃO; janela está ativada Importação onde você poderá inserir os dados necessários para a sincronização. Nas Informações básicas do diretório de negócios LDAP, insira os dados de nome de usuário e senha.

Nota:

- Para diretórios ativos configurados com OpenLDAP, preencha o campo Nome distinto.
- Você pode verificar alguns [Filtros](#) exemplo para LDAP

Nas guias Mapeamentos, você pode especificar os atributos de nomenclatura correspondentes para cada campo, e os filtros devem estar em conformidade com a sintaxe LDAP para sincronizar as informações.

No Mapeamento de usuário os campos obrigatórios a serem cadastrados são: Filtro de usuário a ser levado em consideração na importação, identificador único e nome de usuário.

Importar

Seleccione el tipo de proveedor de autenticación para importar.

FR

Francisco Jose Ramirez

LDAP

Servidor LDAP

https://dev-components-netframework.azurewebsites.net/directoryservice

Usar distinción de nombre DN

Utilizar proveedor por defecto

Habilitar SSL

Inactivo

Puerto

1

*Tipo de autenticación

Básica

*Formato de usuario

Sólo nombre de usuario (usuario)

*Usuario

Escribe un nombre

*Contraseña

Nombre distintivo

DC=interseq=DCLocal

Mapeo de usuarios

Mapeo de grupos

*Ingrese el filtro de usuario para tener en cuenta en la Importación

*Identificador único

*Nombre de usuario

Correo electrónico

Nombre completo

Jefe Inmediato

Identificación

País

Departamento

Ciudad

Teléfono

Teléfono oficina

Teléfono oficina 2

Fax

Móvil

Compañía

Ubicación oficina

Dirección

Sede

Piso en el edificio

Cargo dentro de la compañía

Área de compañía

No Mapeamento de grupo (grupos de usuários) se você inserir qualquer valor no campo “Insira o filtro de grupo a ser levado em consideração na importação”, os campos “Identificador único” e “nome do grupo” tornam-se obrigatórios.

Importar

Seleccione el tipo de proveedor de autenticación para importar.

LS

Ldap Simulación

LDAP

Servidor LDAP

https://dev-components-netframework.azurewebsites.net/directoryservice

Usar distinción de nombre DN

Utilizar proveedor por defecto

Habilitar SSL

Inactivo

Puerto

0

*Tipo de autenticación

Anónima

*Formato de usuario

Sólo nombre de usuario (usuario)

*Usuario

Escribe un nombre

*Contraseña

Nombre distintivo

DC=interseq=DCLocal

Mapeo de usuarios

Mapeo de grupos

Ingrese el filtro de grupos para tener en cuenta en la Importación

Identificador único

Nombre del grupo

6. Ao cadastrar os campos, clique no botão Conexão de teste

. Se a conexão foi bem-sucedida, você poderá visualizar a mensagem: As informações estão completas, agora você pode concluir a importação e a continuação do processo é autorizada.

7. Quando terminar de gravar as informações, clique no botão Sincronizar



e na janela habilitada, ative a sincronização.



Última ejecución

dd/MM/yyyy h:mm a

Activo

Programar sincronización

Seleccione la fecha y la hora en la que quiere hacer la programación

☒ Ejecutar ahora

☐ Programar

CANCELAR

CONFIRMAR SINCRONIZACIÓN

8. A sincronização pode ser manual (imediatamente) ou pode ser agendada automaticamente uma ou a cada poucas horas para atualizar novos usuários. Depois de selecionar o tipo de sincronização e executar as configurações, clique no botão CONFIRMAR A SINCRONIZAÇÃO.



Última ejecución

dd/MM/yyyy h:mm a

Activo

Programar sincronización

Seleccione la fecha y la hora en la que quiere hacer la programación

☐ Ejecutar ahora

☒ Programar

Periodicidad

☐ Una Vez

☒ Por Hora

Iniciar en:

01/11/2024

08: 03 PM



Repetir cada:

1

Hora(s)

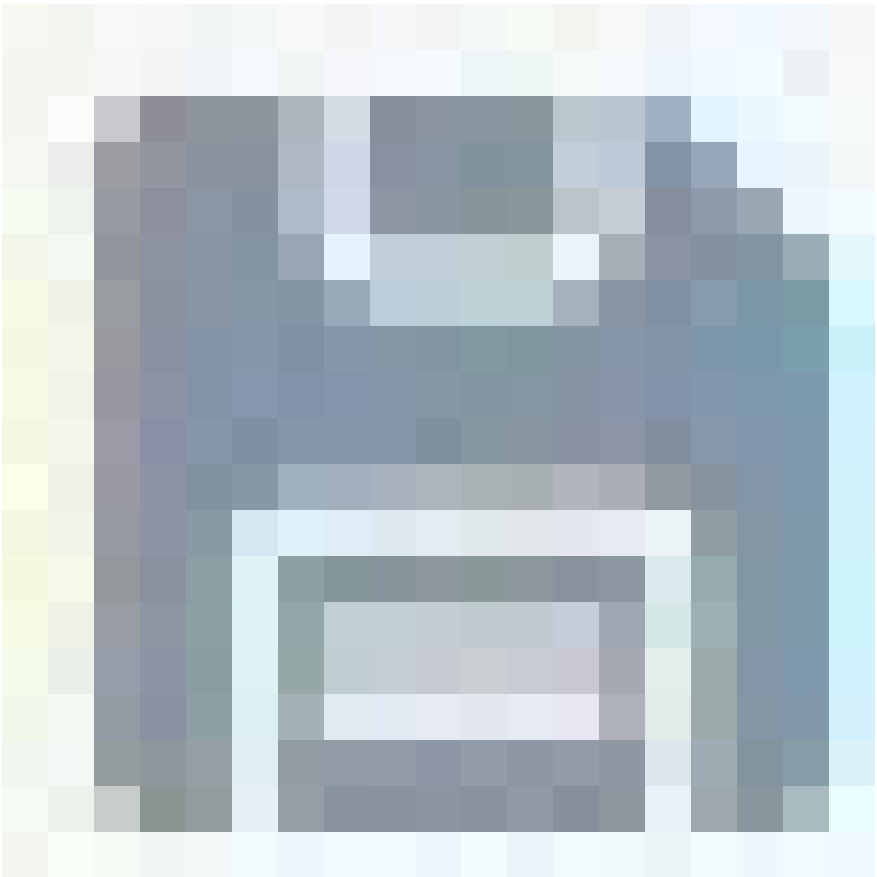
CANCELAR

CONFIRMAR SINCRONIZACIÓN

9. Quando terminar de configurar o diretório LDAP, na janela Importar, clique no botão de confirmação



e na janela Configuração básica do LDAP, clique em Salvar



LS

Ldap Simulación

ACTIVO

*Nombre completo

Ldap Simulación

*Servidor LDAP

192.168.3.2

*Puerto

0

*Tipo de autenticación

Negociada

*Formato de usuario

Sólo nombre de usuario (usuario)

Estado

Activo

Selecione el tipo de autenticación

Selecione el proveedor por el que va crear el tipo de autenticación

☒ LDAP

Cree uno o varios directorios empresariales.

☐ Microsoft Entra ID

Importar usuario de office 365.

☒ Utilizar proveedor por defecto

☐ Usar distinción de nombre DN

☐ Habilitar SSL

IMPORTAR

10. Quando a sincronização for concluída, o administrador poderá atribuir as respectivas funções aos usuários sincronizados.

Provedor Microsoft EntraID

1. Na visualização de detalhes do provedor, insira o nome completo do diretório que deseja sincronizar e clique no botão IMPORTAÇÃO; janela está ativada Importação onde você poderá inserir os dados necessários para a sincronização. Nas informações básicas do diretório, insira a URL da autoridade, a ID do cliente e o segredo do cliente fornecidos pelo Microsoft EntraID.

No Mapeamento de usuário os campos obrigatórios a serem cadastrados são:Filtro de usuário para importação, identificador único e Nome de usuário.

Importar

Seleccione el tipo de proveedor de autenticación para importar.

M

MS

Microsoft Entra ID

✓

✕

▼

*URL de autoridad

*Identificador del cliente

*Secreto del cliente

Mapeo de usuarios

Mapeo de grupos

*Ingrese el filtro de usuario para tener en cuenta en la Importación

*Identificador único

*Nombre de usuario

Correo electrónico

Nombre completo

Jefe Inmediato

Identificación

País

Departamento

Ciudad

Teléfono

Teléfono oficina

Teléfono oficina 2

Fax

Móvil

Compañía

Ubicación oficina

Dirección

Sede

Piso en el edificio

Cargo dentro de la compañía

Área de compañía

No Mapeamento de grupo (grupos de usuários) se você inserir qualquer valor no campo “Insira o filtro de grupo a ser levado em consideração na importação”, os campos “Identificador único” e “nome do grupo” tornam-se obrigatórios.

Importar

Seleccione el tipo de proveedor de autenticación para importar.

P

Proveedor

Microsoft Entra ID

✓

✕

▼

*URL de autoridad

*Identificador del cliente

*Secreto del cliente

Mapeo de usuarios

Mapeo de grupos

Ingrese el filtro de grupos para tener en cuenta en la importación

Identificador único

Nombre del grupo

Para obter informações sobre filtros e atributos de usuário para mapeamento de campo, você pode consultar a documentação da Microsoft nos seguintes links: [Filtro de usuário e grupo](#)
[Campos de usuário](#)
[Agrupar campos](#)

📌 Nota: : Você pode consultar alguns [Filtros](#) e [Mapeamento de campo](#) Exemplo de Microsoft EntraID

6. Ao cadastrar os campos, clique no botão Conexão de teste



. Se a conexão foi bem-sucedida, você poderá visualizar a mensagem: As informações estão completas, agora você pode concluir a importação e a continuação do processo é autorizada. 7. Quando terminar de gravar as informações, clique no botão Sincronizar



e na janela habilitada, ative a sincronização.



Última ejecución

dd/MM/yyyy h:mm a

Activo

Programar sincronización

Seleccione la fecha y la hora en la que quiere hacer la programación

☒ Ejecutar ahora

☐ Programar

CANCELAR

CONFIRMAR SINCRONIZACIÓN

8. A sincronização pode ser manual (imediatamente) ou pode ser agendada automaticamente uma ou a cada poucas horas. Depois de seleccionar o tipo de sincronização e executar as configurações, clique no botão SINCRONIZAÇÃO DE CO-ASSINATURA.



Última ejecución

dd/MM/yyyy h:mm a

Activo

Programar sincronización

Seleccione la fecha y la hora en la que quiere hacer la programación

☐ Ejecutar ahora

☒ Programar

Periodicidad

☐ Una Vez

☒ Por Hora

Iniciar en:

01/11/2024

08: 03 PM



Repetir cada:

1

Hora(s)

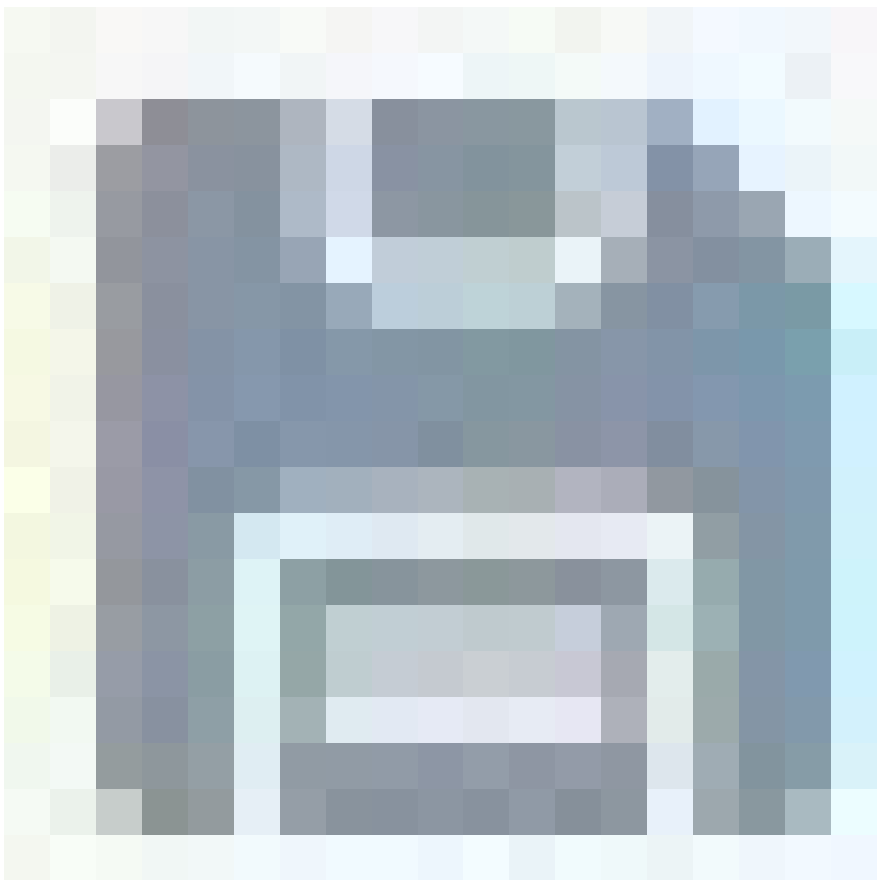
CANCELAR

CONFIRMAR SINCRONIZACIÓN

9. Quando terminar de configurar o diretório Microsofrt Enter ID na janela Importar, clique no botão de confirmação



e na janela Configuração básica do fornecedor, clique em Salvar



⚠ Importante: O provedor de ID do Microsoft Entra permite apenas a sincronização de usuários e grupos de usuários, ele não se aplica a ser usado como um provedor de autenticação, portanto, ele sempre permanece em um estado Inativo. Para acessar o site do produto Aranda usando os usuários desse tipo de diretório, a autenticidade externa (SAML) deve ser configurada.

Editar serviços de diretório

1. Para editar um diretório ou provedor de autenticação, no modo de exibição de informações dos Serviços de Diretório, selecione um registro na lista de provedores existentes.

Servicios de directorio

Listado de los proveedores de autenticación creados.

Buscar por todos los conceptos

NUEVO

SEGURIDAD

ELIMINAR

☐ Nombre	Proveedor	Servidor
☐ pruebaADM	External	192.168.3.2
☐ Ldap	LDAP	
☐ Azure	Microsoft Entra ID	
☐ ARANDA	Aranda	

ESTADO

☐ ACTIVO

☐ INACTIVO

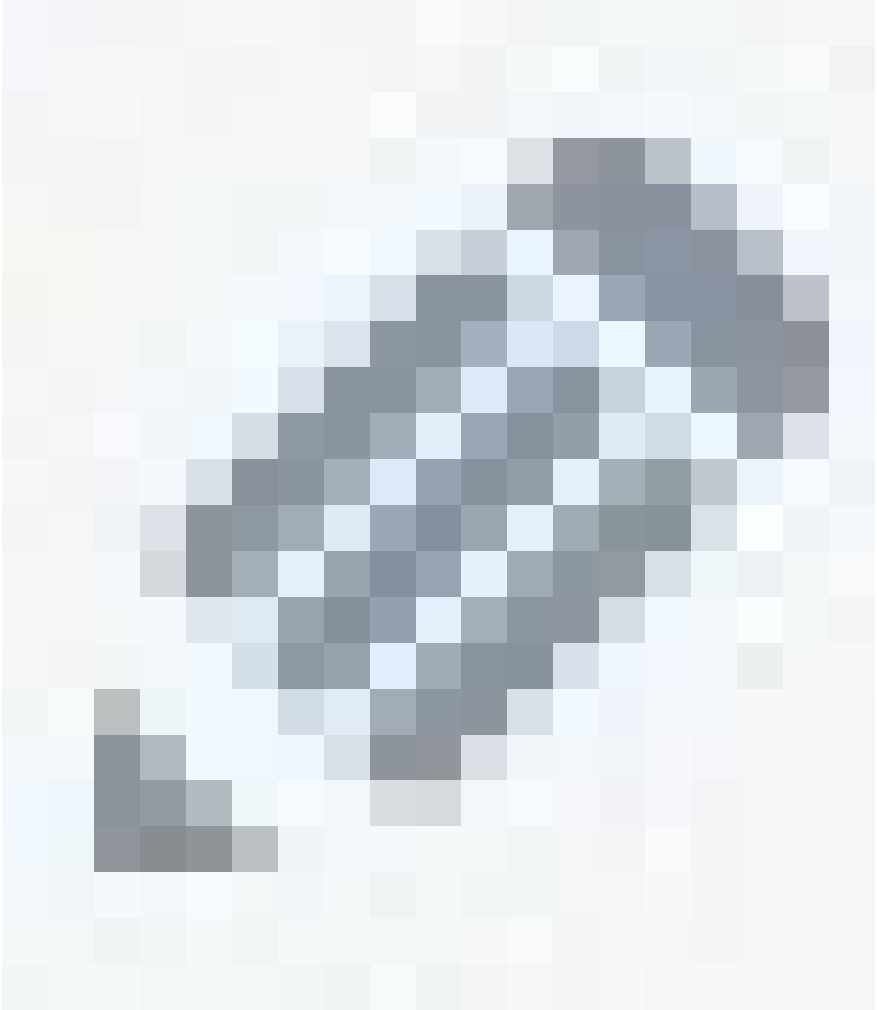
<

1

>

Mostrando 1 al 4 de 4 registros

2. Na visualização de detalhes, clique no ícone de edição



para modificar as informações necessárias.

AS

Azure Simulación

INACTIVO

Nombre completo: Azure Simulación

ELIMINAR

Tipo de autenticación

Microsoft Entra ID

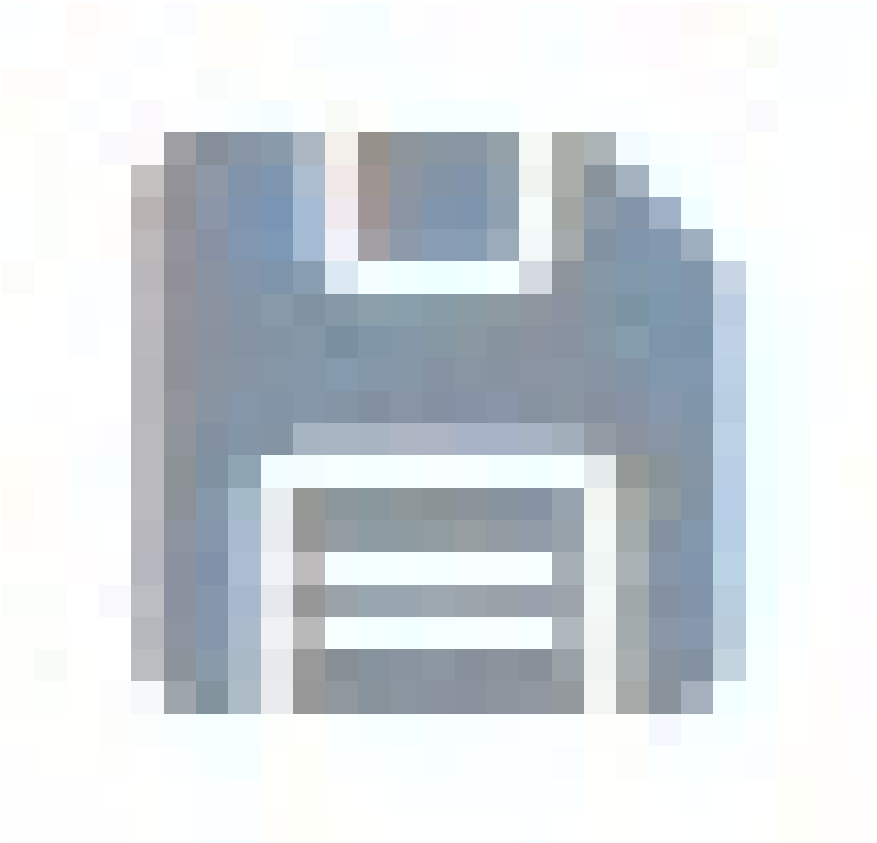
Sincronización

Edite la sincronización de la importación.

Última ejecución

dd/MM/yyyy h:mm

3. Na janela Edição de diretório, você pode atualizar as informações básicas e as informações importadas do fornecedor. 4. Quando terminar de editar o usuário, clique no botão Salvar



para confirmar as alterações feitas.

Excluir serviços de diretório

A exclusão de registros de serviços de diretório pode ser feita de duas maneiras:

1. Na visualização Informações dos Serviços de Diretório, selecione um registro na lista de serviços de diretório ou provedores de autenticação que você deseja excluir e clique no ícone



Servicios de directorio

Listado de los proveedores de autenticación creados.

Q

Buscar por todos los conceptos

NUEVO

SEGURIDAD

ELIMINAR

☐	Nombre	Proveedor	Servidor
☐	pruebaADM	External	192.168.3.2
☐	Ldap	LDAP	
☒	Azure	Microsoft Entra ID	
☐	ARANDA	Aranda	

ESTADO

☐ ACTIVO

☐ INACTIVO

<

1

>

Mostrando 1 al 4 de 4 registros

2. Na visualização de detalhes de um serviço de diretório ou provedor selecionado que você deseja excluir, clique no ícone ELIMINAR

AS

Azure Simulación

INACTIVO

Nombre completo: Azure Simulación

ELIMINAR

Tipo de autenticación

Microsoft Entra ID

Sincronización

Edite la sincronización de la importación.

Última ejecución

dd/MM/yyyy h:mm

3. Em ambos os casos, você pode exibir uma mensagem de confirmação para validar a ação de exclusão.

Configuração de segurança do reCAPTCHA

⚠ Importante: A configuração do reCAPTCHA é um componente Opcional que você pode implementar no gerenciamento do provedor de serviços de diretório, se precisar dessa condição de autenticação.

1. Para configurar o reCAPTCHA, na visualização de informações do servidor de diretório, selecione o



Servicios de directorio

Listado de los proveedores de autenticación creados.

Q

Buscar por todos los conceptos

NUEVO

SEGURIDAD

ELIMINAR

☐	Nombre	Proveedor	Servidor
☐	pruebaADM	External	192.168.3.2
☐	Ldap Simulación	LDAP	
☐	Azure Simulación	Microsoft Entra ID	
☐	ARANDA	Aranda	

ESTADO

☐ ACTIVO

☐ INACTIVO

<

1

>

Mostrando 1 al 4 de 4 registros

2. A janela reCAPTCHA está habilitada, onde você pode configurar este componente. Clique no botão Editar



R

reCAPTCHA

INACTIVO

reCAPTCHA ayuda a proteger tus sitios de actividades fraudulentas, spam y abuso.

Para obtener más información sobre las funciones de reCAPTCHA y comparación de funciones entre versiones de reCAPTCHA. [Haga clic aquí](#)

Configuración

Seleccione la versión

Ninguna

2. Seleccione a versão necessária, de acordo com o tipo de [Chave configurada no Google](#) e preencha as informações solicitadas:

R

reCAPTCHA

INACTIVO

reCAPTCHA ayuda a proteger tus sitios de actividades fraudulentas, spam y abuso.

Para obtener más información sobre las funciones de reCAPTCHA y comparación de funciones entre versiones de reCAPTCHA. [Haga clic aquí](#)

Configuración

Seleccione la versión

V2

reCAPTCHA V2

Complete la información para la configuración.

Los campos marcados * son obligatorios.

*Clave de sitio

123456789012345678901234567890123...

Requerido

*Clave secreta

Requerido

Campo	Tipo de campo	Descrição
Versão	Seletor	Versão configurada no Google.
Chave do site	Texto	Chave pública obtida a partir da configuração feita no Google.
Chave secreta	Texto	Chave secreta obtida a partir da configuração feita no Google.
Pontuação	Texto	Se você escolher a versão V3, defina o Pontuação para classificação do usuário

⌵ Nota: Ao alterar a versão do reCAPTCHA, será necessário preencher novamente os campos solicitados ou cancelar a operação.

Configuração para reCAPTCHA V2 e V3

Pré-condições

Crie chaves reCAPTCHA para sites

- Inscreva-se para [Pesquise no Google](#).
- [Prepare seu ambiente para o reCAPTCHA Enterprise](#).
- Verifique se você tem a função de Gerenciamento de Identidade e Acesso: reCAPTCHA Enterprise Administrator (roles/recaptchaenterprise.admin)
- [Defina o tipo de chave que melhor se adapta ao seu caso de uso](#).

Configurar tokens para google recaptcha

Informações necessárias para a configuração

⌵ Nota: Uma conta do Google e um ambiente criados anteriormente são necessários para o reCAPTCHA Enterprise: Para criar o console do Google Cloud e o projeto do Google Cloud: [Acesse o Google Cloud](#)

Ativar a API corporativa reCAPTCHA

1. No console do Google Cloud, acesse a página da API do Google Cloud. reCAPTCHA Empresa
2. Verifique se o nome do projeto aparece no seletor de projetos na parte superior da página. Se você não vir o nome do projeto, clique no seletor de projeto e selecione o projeto desejado.
3. Clique em Ativar.

⌵ Nota: O redirecionamento é realizado na página, onde será permitida a criação de credenciais.

Criando chaves reCAPTCHA

1. No console do Google Cloud, acesse a página do reCAPTCHA Enterprise.
2. Verifique se o nome do projeto aparece no seletor de recursos na parte superior da página.

⌵ Nota: Se você não vir o nome do projeto, clique no seletor de recursos e selecione o projeto necessário.

3. Clique em Criar chave.

Google Cloud

Traslate

Buscar (/) recursos, documentos, productos y r

Seguridad

Security Command Center

Descripción general de rie...

Amenazas

Vulnerabilidades

Cumplimiento

Recursos

Resultados

Fuentes

Administración de la post...

Detecciones y controles

Google SecOps

reCAPTCHA

Web Security Scanner

reCAPTCHA

⚠

La protección de tu sitio es limitada. Agrega hoy una cuenta de facturación y g

MÁS INFORMACIÓN

HABILITAR FACTURACIÓN

🔮

Fraud report generated by Gemini

Informes diarios de la IA sobre el cambiante panorama de los fraudes

2 oct 2024

Banking and Finance Websites Targeted by Bots

Banking and finance websites are being targeted by bots, with 2% of events attempted by bots. These attacks can lead to...

Government Websites Under Attack

Government websites are being targeted by bots, with 18% of events attempted by bots. These attacks can lead to sensitive...

Mostrar informe completo

Claves de reCAPTCHA

+ CREAR CLAVE

4. En el campo Nombre visible, ingrese el nombre visible para la clave.

Nombre visible *

Usa un nombre descriptivo que ayude a identificar la clave dentro de la lista de claves.0 / 50

5. En el menú Elegir tipo de plataforma, seleccione Sitio web.

Elegir tipo de plataforma *

Una vez creada la clave, no se puede modificar el tipo de plataforma.

Sitio web

App para Android

App para iOS

Nota: O Lista de domínios.

6. Digite o nome de domínio do site:

Lista de dominios

AGREGAR UN DOMINIO

Se debe agregar al menos un dominio a la clave de la plataforma del sitio web

FIREWALL DE APLICACIÓN WEB (WAF), VERIFICACIÓN DE DOMINIOS, PÁGINAS DE AMP Y DESAFÍO

- En la sección Lista de dominios, haga clic en Agregar un dominio, ingrese el nombre del dominio.
 - En el campo Dominio, ingrese el nombre del dominio.
 - Opcional: Para agregar un dominio adicional, haga clic en Agregar un dominio e ingrese el nombre de otro dominio en el campo Dominio. Se podrán agregar hasta 250 dominios.
- La clave de reCAPTCHA, para sitios web, es única para los dominios y subdominios definidos. Se podrá definir más de un dominio si se entrega el sitio web desde varios dominios. Si define un dominio (por ejemplo, examplepetstore.com), no es requerido definir los subdominios (por ejemplo, subdomain.examplepetstore.com). Según el tipo de clave de reCAPTCHA que requiere crear para el sitio web, podrá realizar cualquiera de las acciones correspondientes:

Nota: Criar uma chave com base nas pontuações é a opção padrão no console do Google Cloud.”

- reCAPTCHA com base em pontuações:
- Para proteger a chave reCAPTCHA para domínio e subdomínios, valide se a opção Desativar verificação de domínio está desativada. Se você precisar da chave baseada em pontuação para trabalhar com Accelerated Mobile Pages (AMP), alterne a opção **Desativar a verificação de domínio é um risco de segurança porque não há restrições no site, para que qualquer pessoa possa acessar e usar a chave reCAPTCHA.

<center></center>

- Si requiere que la clave basada en puntuaciones funcione con Accelerated Mobile Pages (AMP), active el botón Permitir que esta clave funcione con páginas de AMP.
- En entornos que no son de producción, si requiere especificar una puntuación que muestre la clave al crear evaluaciones para ella, haz lo siguiente:
 - Haga clic en el botón de activación Esta es una clave de prueba..
 - En el cuadro Score, especifique una puntuación entre 0 y 1.0.

Tipo de clave

Firewall de aplicación web (WAF) ?

Para las implementaciones en la capa perimetral.

This is a testing key

This key will return the same score for every assessment. A test key can't be changed to a regular key.

Puntuación *

0

De 0 (alto riesgo) a 1.0 (bajo riesgo).

- Haga clic en Crear clave.

CREAR CLAVE

CANCELAR

Nota: A nova chave aparecerá no Chaves reCAPTCHA.

📌 Nota: O uso de teclas de caixa de seleção não é recomendado, pois elas aumentam o atrito do usuário e não melhoram a precisão.

- reCAPTCHA com caixas de seleção:
- Expanda a seção Firewall de aplicativo Web (WAF), verificação de domínio, páginas AMP e desafio.

```
<center></center> - Para proteger a chave reCAPTCHA para domínio e subdomínios, confirme se a opção Desativar verificação de domínio está desativada. Desativar a verificação de domínio é um risco de segurança porque não há restrições no site, para que qualquer pessoa possa acessar e usar a chave reCAPTCHA.
```

```
<center></center> - Ative o botão de ativação Use o desafio da caixa de seleção.
```

```
<center></center> - Selecione a opção Desafie a segurança adequado. - Para um ambiente de não produção, se você precisar especificar uma pontuação que exiba a chave ao gerar avaliações para ele, lembre-se do seguinte:
```

- Clique no botão de ativação **Esta é uma chave de teste**.

- Na pintura **Pontuação**, especifica uma pontuação entre 0 e 1,0.

- Selecione a opção **Tipo de Desafio** adequado.

- Em algumas ocasiões, o desafio aparece como **Automático**.

- **Sem CAPTCHA** não mostra um desafio.

- Um **Desafio não resolvido** mostra as imagens, mas o desafio não é aprovado.

```
<center></center>
```

- Clique Criar chave.

```
<center></center>
```

📌 Nota: A nova chave aparecerá no Chaves reCAPTCHA.

📌 Nota:

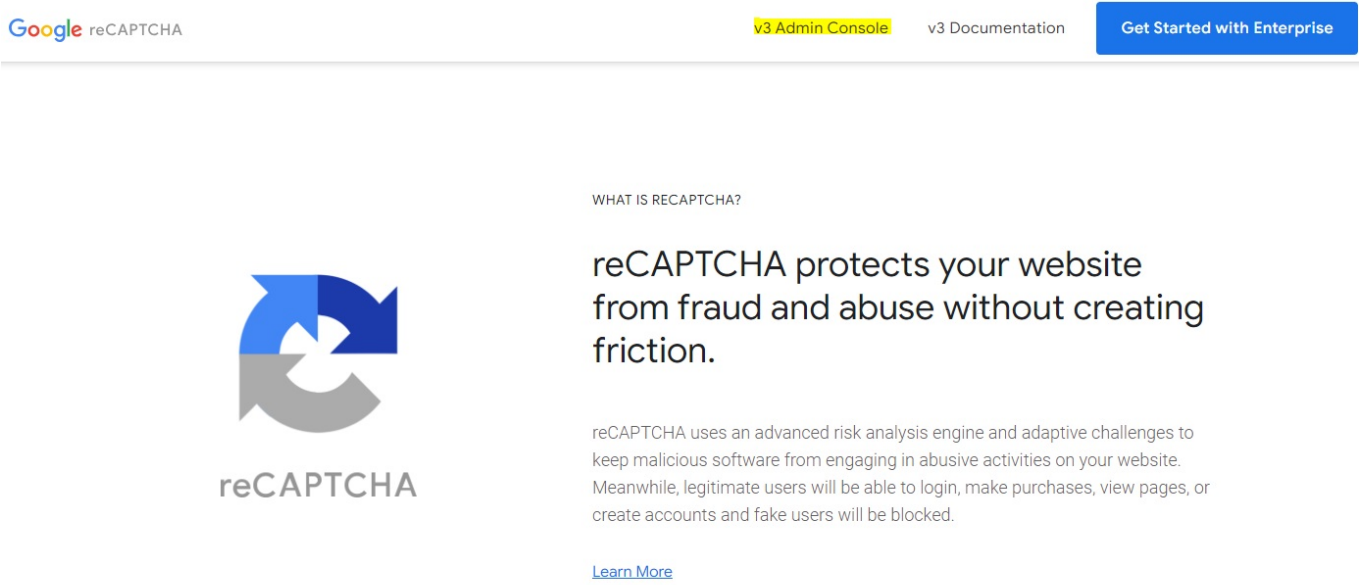
- A opção de segurança do desafio controla a probabilidade de solicitar a um usuário um desafio secundário para selecionar imagens com base em uma categoria identificada (por exemplo, selecionar as imagens com uma motocicleta ou escadas).
- Para garantir uma melhor proteção contra fraudes, selecione (mais seguro contra bots).
- Se você selecionar a opção Dificuldade do desafio mais simples, é menos provável que os usuários sejam solicitados para o desafio visual.

📌 Nota: Observação: depois de criar as chaves reCAPTCHA, você pode editá-las ou excluí-las. Você não poderá recuperar chaves excluídas.

Configurar o reCAPTCHA V2

reCAPTCHA versão 2

1. Uma vez cadastrado no google, digite o [administração](#) por reCAPTCHA



2. Adicione o valor do campo Etiqueta

Etiqueta

demo.com

3. Na tela que está ativada, selecione Desafio (v2) e dependendo da configuração desejada:

- Marque a opção Caixa de seleção “Não sou um robô”
- Marque a opção “Selo reCAPTCHA invisível”

Tipo de reCAPTCHA ⓘ

- ☐ Basado en una puntuación (v3) Verifica las solicitudes mediante una puntuación
- ☒ Desafío (v2) Verifica las solicitudes con un desafío
- ☒ Casilla de verificación "No soy un robot"
Valida las solicitudes con la casilla de verificación "No soy un robot"
- ☐ Insignia de reCAPTCHA invisible Valida las solicitudes en segundo plano

⌵ Nota: Você poderá visualizar uma notificação de configuração do site; Aguarde até que as opções sejam ativadas para continuar:



Todavía estamos estableciendo la configuración de reCAPTCHA en Google Cloud, pero puedes comenzar con los detalles de la clave que se indican a continuación.

La configuración completa debería demorar alrededor de 1 minuto. Una vez que se haya completado, podrás realizar evaluaciones ilimitadas y utilizar las funciones avanzadas, como MFA y Protección de cuentas.

4. Adicione o valor do campo Domínios.

Dominios ⓘ

+ midemodominio.com

5. Selecione o nome do projeto e clique em Enviar.

Google Cloud Platform

Al parecer, ya usaste Google Cloud. Para comenzar, crearemos un proyecto nuevo y habilitaremos las APIs necesarias.

Nombre del proyecto*

reCaptcha

9 / 30

^ GOOGLE CLOUD PLATFORM

CANCELAR

ENVIAR

⌵ Nota: A página exibirá automaticamente as chaves do site, para configuração posterior no componente DirectoryServices

6. Copie as informações exibidas nos campos:

- Chave do site.
- Chave secreta.

Inserta esta clave de sitio en el código HTML que utiliza tu sitio. [Ver la integración del lado del cliente](#)

🔑 COPIAR CLAVE DE SITIO

6LcbdGDQKFtJrWEvHsEz

Utiliza esta clave secreta para la comunicación entre tu sitio y reCAPTCHA. [Ver la integración del lado del servidor](#)

🔑 COPIAR CLAVE SECRETA

6LcbdAAFGCW r_DNAOr9BW1Ja3p

7. Após salvar ou configurar as teclas, clique no botão “IR PARA CONFIGURAÇÕES”

IR A CONFIGURACIÓN

⌵ Nota: Verifique na página se está habilitado se as informações apresentadas correspondem aos valores preenchidos anteriormente.

Etiqueta ⓘ

demo.com

Tipo de reCAPTCHA: Casilla de verificación v2

Claves de reCAPTCHA ▾

Dominios ⓘ

✕ midemodominio.com

+ Agregar un dominio, p. ej., ejemplo.com

Propietarios

✕ arandasoftautomate@gmail.com

+👤 Ingresar direcciones de correo electrónico

8. Valide e configure o Preferência de segurança conforme necessário e clique no botão Salvar

Preferencia de seguridad

La configuración más fácil para los usuarios

La configuración más segura

☒

Verificar el origen de las soluciones de reCAPTCHA

Si esta opción está inhabilitada, debes [revisar el nombre del host](#) en tu servidor al verificar una solución.

☐

Enviar alertas a los propietarios

Recibe alertas si Google detecta problemas con tu sitio, como un error de configuración o un aumento del tráfico sospechoso.

CANCELAR

GUARDAR

Configurar o reCAPTCHA V3

reCAPTCHA Versão 3

1. Uma vez cadastrado no google, digite o [administração](#) por reCAPTCHA

Google reCAPTCHA

[v3 Admin Console](#)[v3 Documentation](#)[Get Started with Enterprise](#)



reCAPTCHA

WHAT IS RECAPTCHA?

reCAPTCHA protects your website from fraud and abuse without creating friction.

reCAPTCHA uses an advanced risk analysis engine and adaptive challenges to keep malicious software from engaging in abusive activities on your website. Meanwhile, legitimate users will be able to login, make purchases, view pages, or create accounts and fake users will be blocked.

[Learn More](#)

2. Adicione o valor do campo Etiqueta

Etiqueta

demo.com

8 / 50

3. Na tela que está ativada, selecione Com base em uma pontuação (v3) e dependendo da configuração desejada:

Tipo de reCAPTCHA

- ☒ Basado en una puntuación (v3) Verifica las solicitudes mediante una puntuación
- ☐ Desafío (v2) Verifica las solicitudes con un desafío

📌 Nota: Ao visualizar a notificação de configuração do site, aguarde até que as opções continuem habilitadas:



Todavía estamos estableciendo la configuración de reCAPTCHA en Google Cloud, pero puedes comenzar con los detalles de la clave que se indican a continuación.

La configuración completa debería demorar alrededor de 1 minuto. Una vez que se haya completado, podrás realizar evaluaciones ilimitadas y utilizar las funciones avanzadas, como MFA y Protección de cuentas.

4. Adicione o valor do campo Domínios.

Domínios

+ midemodominio.com

5. Selecione o nome do projeto e clique em Enviar.

Google Cloud Platform

Al parecer, ya usaste Google Cloud. Para comenzar, crearemos un proyecto nuevo y habilitaremos las APIs necesarias.

Nombre del proyecto*

 reCaptcha

9 / 30

 GOOGLE CLOUD PLATFORM

CANCELAR

ENVIAR

📌 Nota: A página exibirá automaticamente as chaves do site, para configuração posterior no componente DirectoryServices

6. Copie as informações exibidas nos campos:

- Chave do site.
- Chave secreta.

Inserta esta clave de sitio en el código HTML que utiliza tu sitio. [Ver la integración del lado del cliente](#)

 COPIAR CLAVE DE SITIO

6Lcbd GDQKFtJr WEv HsEz

Utiliza esta clave secreta para la comunicación entre tu sitio y reCAPTCHA. [Ver la integración del lado del servidor](#)

 COPIAR CLAVE SECRETA

6Lcbd AAFgCW r_DNAOr9B W1Ja3p

7. Após salvar ou configurar as teclas, clique no botão “IR PARA CONFIGURAÇÕES”

IR A CONFIGURACIÓN

Nota: Verifique na página se está habilitado se as informações apresentadas correspondem aos valores preenchidos anteriormente.

Etiqueta

demo.com

Tipo de reCAPTCHA:

v3

VER EN LA CONSOLA DE CLOUD

Claves de reCAPTCHA

Dominios

midemo.com

Agregar un dominio, p. ej., ejemplo.com

Propietarios

arandasoftautomate@gmail.com

Ingresar direcciones de correo electrónico

8. Valide e configure o Preferência de segurança conforme necessário e clique no botão Salvar

Verificar el origen de las soluciones de reCAPTCHA

Si esta opción está inhabilitada, debes [revisar el nombre del host](#) en tu servidor al verificar una solución.

Permitir que esta clave funcione con las páginas AMP

Debes marcar esta casilla de verificación para usar [amp-recaptcha-input](#) en las páginas de [AMP](#).

Enviar alertas a los propietarios

Recibe alertas si Google detecta problemas con tu sitio, como un error de configuración o un aumento del tráfico sospechoso.

CANCELAR

GUARDAR

Módulo de autenticação externa

Gerenciamento de fornecedores terceirizados

Ver fornecedores terceirizados

1. Na visualização de informações de fornecedores externos é possível visualizar a lista de fornecedores cadastrados, agrupados por dados como:

Autenticación externa

Listado de proveedores de autenticación creados.

Q

Buscar por nombre

NUEVO

ELIMINAR

☐ Nombre	Consola para la autenticación	Url de la consola
☐ ● Microsoft prueba	ASDK-Administrator.ExternalProviders	https://google.com.co

ESTADO

☐

● ACTIVO

☐

● INACTIVO

<1>

Mostrando 1 al 1 de 1 registros

Campo	Tipo de campo	Descrição
Nome	Texto	Nome com o qual o fornecedor é identificado.
Console para autenticação	Texto	Indica o tipo de console que você deseja integrar.
Console URL	Texto	Essa é a URL pública do console, esse valor deve ser fornecido ao provedor de autenticação como um identificador (ID da entidade).

2. Na visualização de informações de fornecedores externos, você terá ações de gerenciamento e organização de informações habilitadas.[Visualização de informações no ambiente do Commons](#)

Links Relacionados:

- [Criar provedor de terceiros](#)
- [Editar provedor terceirizado](#)
- [Remover provedor de terceiros](#)

Criar fornecedor terceirizado

1. Para criar um novo fornecedor terceirizado, na exibição de informações do fornecedor, clique no botão Novo.

Autenticación externa

Listado de proveedores de autenticación creados.

Q

Buscar por nombre

NUEVO

ELIMINAR

☐ Nombre	Consola para la autenticación	Url de la consola
☐ ● Microsoft deshabilitado	ASDK-Administrator.ExternalProviders	https://google.com.co
☐ ● Auth0	ASDK-Administrator.ExternalProviders	https://auth0.com
☐ ● Okta	ASDK-Administrator.ExternalProviders	https://oauth.com
☐ ● Google	ASDK-Administrator.ExternalProviders	https://google.com.co
☐ ● Microsoft	ASDK-Administrator.ExternalProviders	https://microsoft.com.co

ESTADO

☐

● ACTIVO

☐

● INACTIVO

<1>

Mostrando 1 al 5 de 5 registros

📌 Nota: No se tiene restricción de crear proveedores externos con información duplicada, se pueden crear cuantos sean necesarios.

Fatos básicos

2. Na janela que está habilitada, você poderá preencher os dados básicos do provedor externo, como nome do provedor, URL do console, URL de login, URL de logout, status, ícone e texto do provedor, entre outros.
Cada um dos campos de fornecedores terceirizados deve levar em conta o [Especificações para campos](#)

📌 Nota: Os campos Login URL e Saida de URL têm funcionalidade de preenchimento automático e baseiam-se nas informações fornecidas no campo Console URL.

NP

Nombre de proveedor

INACTIVO

Nombre de proveedor

Elija consola para configurar la autenticación

URL de la consola

URL inicio de sesión

URL cerrar sesión

Estado ☐ Inactivo

Icono y texto del proveedor

Texto corto

Nombre que aparece al lado del icono

Seleccionar icono

Icono (Tamaño: 20x20 pixeles png, jpg)

Información del proveedor

Complete la información para la creación del proveedor de autenticación

Identificador de identidad

Ingrese url donde se configura la identidad

URL inicio de sesión

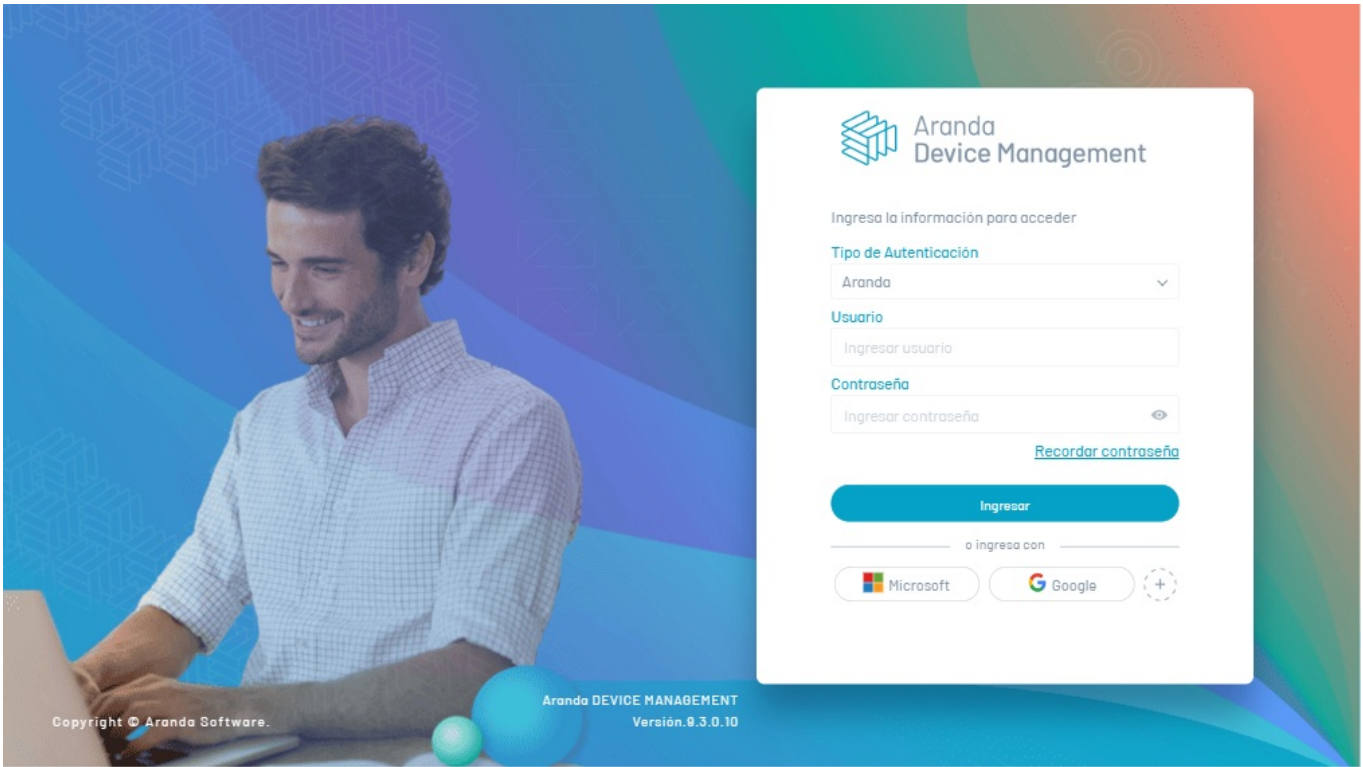
Ingrese la url con la que va a iniciar sesión

URL cerrar sesión

Ingrese la url con la que va a cerrar sesión

4. Quando terminar de configurar a autenticação do provedor, clique no ícone Salvar.

- 📌 Anotações:
- Se a configuração for bem-sucedida, na exibição de fornecedor externo, você poderá exibir os registros dos últimos fornecedores criados.
 - Na tela inicial e no acesso ao aplicativo necessário, você poderá exibir o ícone com o nome dado ao provedor externo.



- 📌 Anotações:
- O e-mail com o qual a autenticação é realizada do provedor externo é usado como identificação do usuário e deve ser registrado no respectivo aplicativo.
 - Para que o site autentique o usuário, o usuário deve ser importado ou criado antes de executar a configuração de autenticação externa.

Editar fornecedor terceirizado

1. Para modificar um fornecedor terceirizado, na exibição de informações do fornecedor terceirizado, selecione um registro na lista de fornecedores existentes.

Autenticación externa

Listado de proveedores de autenticación creados.

🔍 Buscar por nombre

NUEVO ELIMINAR

☐ Nombre	Consola para la autenticación	Url de la consola
☐ <u>Microsoft deshabilitado</u>	ASDK-Administrator.ExternalProviders	https://google.com.co
☐ <u>Auth0</u>	ASDK-Administrator.ExternalProviders	https://auth0.com
☐ <u>Okta</u>	ASDK-Administrator.ExternalProviders	https://oauth.com
☐ <u>Google</u>	ASDK-Administrator.ExternalProviders	https://google.com.co
☐ <u>Microsoft</u>	ASDK-Administrator.ExternalProviders	https://microsoft.com.co

ESTADO

☐ ACTIVO ☐ INACTIVO

< 1 >

Mostrando 1 al 5 de 5 registros

2. Na visualização de detalhes do fornecedor, clique no ícone Editar



e modifique as informações necessárias.

M

Microsoft

ACTIVO

Nombre de proveedor: Microsoft

Consola para la autenticación:
ASDK-Administrator.ExternalProviders

URL de la consola:
https://microsoft.com.co

URL de inicio de sesión:
https://google.com.co/api/externalauth/9b9e7a0f-778f-4992-8a3d-fa575a41df17/login

URL cierre de sesión:
https://google.com.co/api/externalauth/9b9e7a0f-778f-4992-8a3d-fa575a41df17/logout

Estado ☒ Activo

ELIMINAR

Información del proveedor

Identificador de identidad
https://google.com.co

URL inicio de sesión
https://google.com.co

URL cerrar sesión
https://google.com.co

3. Na janela Processamento de fornecedores terceirizados Você poderá atualizar as informações básicas do fornecedor.

M

Microsoft

ACTIVO

Nombre de proveedor

Microsoft

Elija consola para configurar la autenticación

Administrator

URL de la consola

https://microsoft.com.co

URL inicio de sesión

https://google.com.co/api/externalauth/9b

URL cerrar sesión

https://google.com.co/api/externalauth/9b

Estado ☒ Activo

Icono y texto del proveedor

Texto corto
Nombre que aparece al lado del icono

Microsoft

Seleccionar icono
Icono (Tamaño 20x20 pixels png, jpg)

Información del proveedor

Complete la información para la creación del proveedor de autenticación

Identificador de identidad
Ingrese url donde se configura la identidad

https://google.com.co

URL inicio de sesión
Ingrese la url con la que va a iniciar sesión

https://google.com.co

URL cerrar sesión
Ingrese la url con la que va a cerrar sesión

https://google.com.co

Nota: O valor do campo Ícone Seleccionar Ele não ficará visível no modo de exibição de edição, no entanto, se nenhuma alteração for feita nesse campo, a imagem que foi salva quando o provedor foi criado deverá ser mantida.

4. Quando terminar de editar o provedor de terceiros, clique no botão Salvar



para confirmar as alterações feitas.

Remover provedor terceirizado

A exclusão de registros de fornecedores terceirizados pode ser feita de duas maneiras:

1. Na visualização Informações de Fornecedores de Terceiros, selecione um registro da lista de fornecedores que você deseja excluir e clique no ícone



Autenticación externa

Listado de proveedores de autenticación creados.

Q

Buscar por nombre

NUEVO

ELIMINAR

☐ Nombre	Consola para la autenticación	Url de la consola
☐ Microsoft deshabilitado	ASDK-Administrator.ExternalProviders	https://google.com.co
☒ Auth0	ASDK-Administrator.ExternalProviders	https://auth0.com
☒ Okta	ASDK-Administrator.ExternalProviders	https://oauth.com
☐ Google	ASDK-Administrator.ExternalProviders	https://google.com.co
☐ Microsoft	ASDK-Administrator.ExternalProviders	https://microsoft.com.co

ESTADO

☐ ACTIVO

☐ INACTIVO

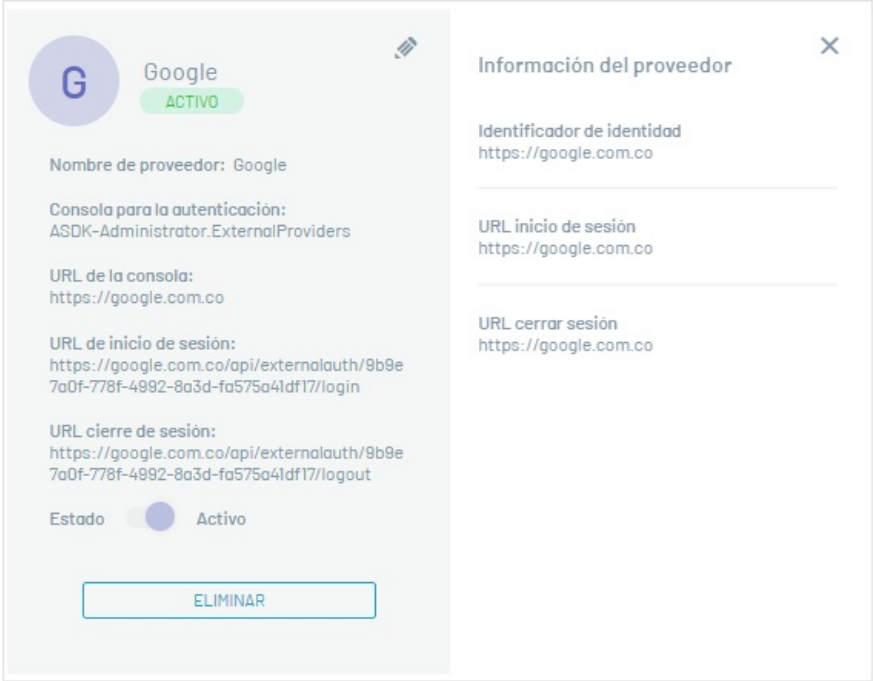
<

1

>

Mostrando 1 al 5 de 5 registros

2. Na visualização de detalhes de um fornecedor selecionado que você deseja excluir, clique no botão ELIMINAR



3. Em ambos os casos, você pode exibir uma mensagem de confirmação para validar a ação de exclusão.

Nota:

- Um provedor excluído não pode ser restaurado.
- O provedor não tem restrição quanto ao seu descarte.

Módulo de Token de Integração

Gerenciamento de token

Ver Tokens

1. Na visualização Informações do token, você pode exibir a lista de tokens criados, agrupados por dados como:

Configuración de API

Listado de tokens de conexiones de API creados.

Buscar por todos los conceptos

NUEVOELIMINAR

☐	Nombre de usuario	Descripción	Fecha de creación	Fecha de expiración Token
☐	APPLICATION ADMINISTRATOR	token datos	19/11/2024 9:47:23 am	04/11/2024 11:59:00 pm
☐	APPLICATION ADMINISTRATOR	Token descripcion	19/11/2024 9:46:57 am	23/11/2024 11:59:00 pm

ESTADO

☐ VIGENTE☐ VENCIDO

<1>

Mostrando 1 al 2 de 2 registros

Campo	Tipo de campo	Descrição
Nome de usuário	Texto	Nome do usuário associado ao token.
Descrição	Texto	Descrição do token.
Data de criação	Texto	Data de criação.
Data de expiração do token	Texto	Data em que o token expira.

2. Na exibição de informações do token, você terá o gerenciamento de informações e as ações da organização habilitadas.[Visualização de informações no ambiente do Commons](#) 3. Para exibir um token de integração, na visualização de informações do token, selecione um registro na lista de tokens existentes. Na visualização de detalhes do token você poderá visualizar as informações com as quais o token foi criado, essas informações não podem ser editadas.

JC

Juan Francisco Carrillo

VIGENTE

Detalle: para conexión

Fecha de creación: 13/11/2024

ELIMINAR

Fecha de expiración Token

Noviembre 28, 2024

Token

Recuerda, el Token sólo se puede copiar en la creación.

Links Relacionados:

- [Criar integração de token](#)
- [Remover integração de token](#)

Criar tokens

1. Para criar um novo token de integração, na visualização de informações do token, clique no ícone Novo.

Configuración de API

Listado de tokens de conexiones de API creados.

Buscar por todos los conceptos

NUEVO

ELIMINAR

Nombre de usuario	Descripción	Fecha de creación	Fecha de expiración Token
APPLICATION ADMINISTRATOR	token datos	19/11/2024 9:47:23 am	04/11/2024 11:59:00 pm
APPLICATION ADMINISTRATOR	Token descripcion	19/11/2024 9:46:57 am	23/11/2024 11:59:00 pm

ESTADO

VIGENTE

VENCIDO

<

1

>

Mostrando 1 al 2 de 2 registros

Fatos básicos

2. Na janela que está habilitada você poderá preencher os dados do token: Descrição, usuário e data de validade. Cada um dos campos de token deve levar em conta o [Especificações para campos comuns](#)

Creación de conexiones para API

Realiza la configuración de conexión para la API y agrega detalles para crear el Token

1

Añadir descripción para la conexión

2

Seleccione el usuario

3

4

Descripción

admin

APPLICATION ADMINISTRATOR

Cancelar

3. Ao concluir a configuração de cada campo, clique no botão



para confirmar as alterações geradas.

2. Você poderá exibir uma mensagem de confirmação para validar a ação de exclusão.