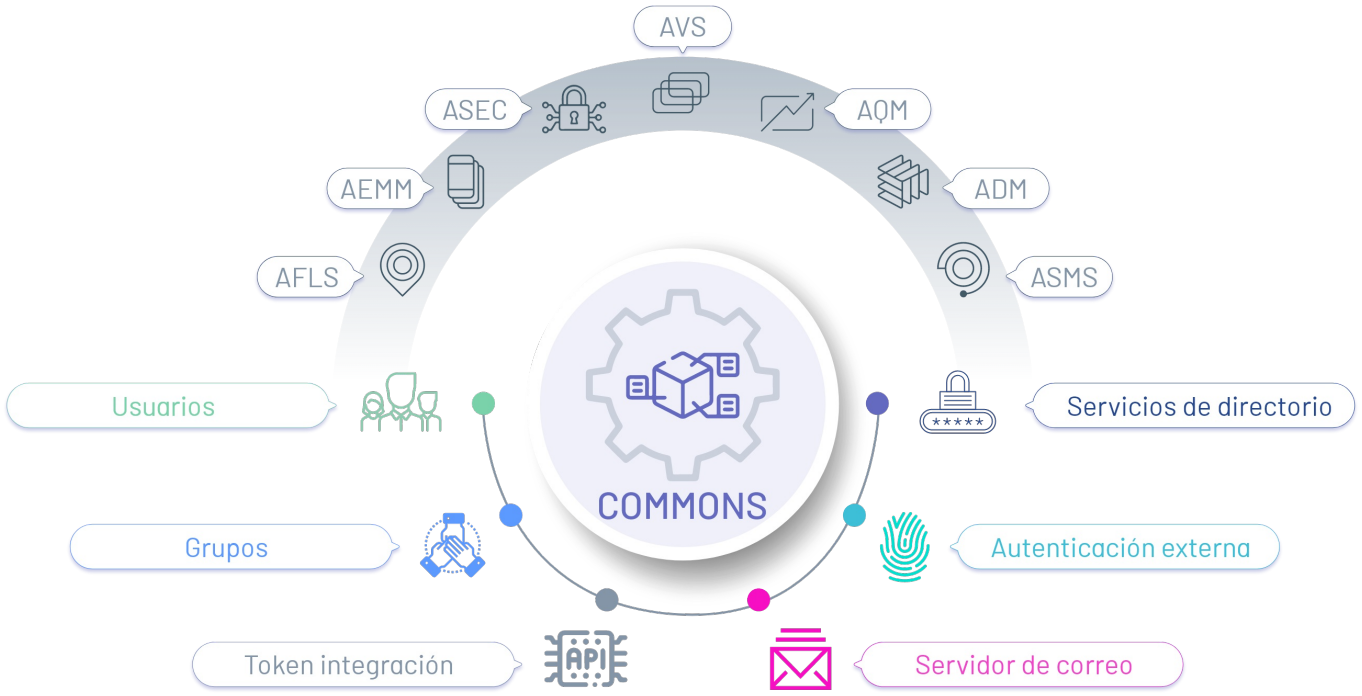
Configuración de Commons

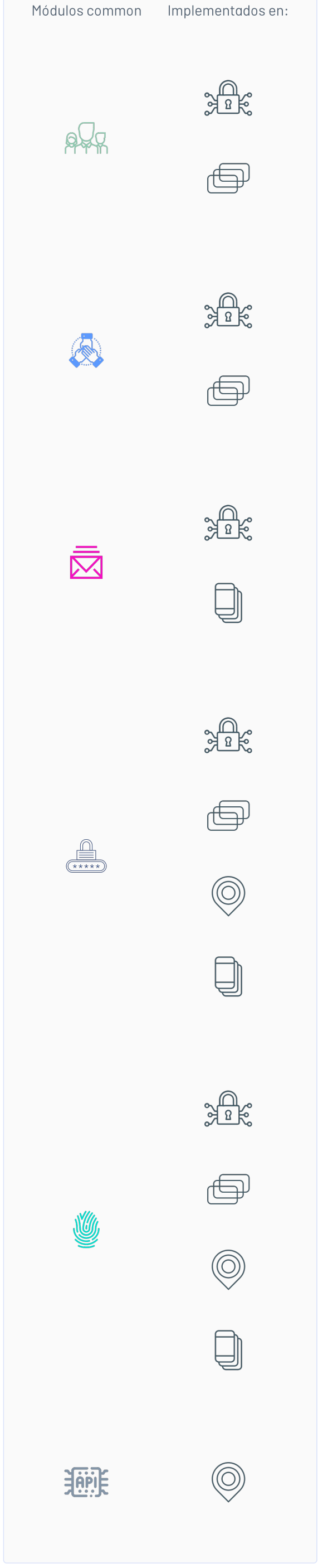
En los procesos de configuración de las diferentes aplicaciones de Aranda, existen conceptos y funcionalidades transversales que permiten agilizar y compartir datos afines para cada proyecto.

Aranda COMMONS es una librería que comparte componentes o módulos transversales para los procesos de configuración general de productos de Aranda como ASEC, AVS, AFLS, ADM, AQM.



2. Módulos

Los siguientes módulos comunes de configuración se integran nativamente con nuestras soluciones:



¿Para Quién es este Manual?

Esta manual está diseñado para los usuarios de productos de Aranda que comparten diferentes módulos de configuración transveral de Aranda COMMON.

¿Cuál es Nuestra Documentación?

- Manual de Integración ADM (Usted está AQUÍ)

Módulos de Configuración

Módulos Common

El administrador general desde la consola Web de podrá realizar las siguientes tareas de configuración transversal:

1. Usuarios

En este módulo podrá Configurar los usuarios encargados de los difrentes procesos de gestión de los productos de Aranda. Estas configuraciones sólo las podrá realizar un usuario con rol de administrador. Adicionalmente podrá asociar grupos y roles.

Para mayor información consulte la Gestión de Usuarios ↪.

2. Grupos de usuarios

En este módulo podrá configurar y administrar los grupos de usuarios para realizar la asignación de roles de una manera más eficiente.

Para mayor información consulte la Gestión de Grupos ↪.

3. Servidor de Correo

En este módulo podrá configurar un proveedor de correo para la operación de los productos de Aranda; desde este servidor se enviarán notificaciones a los usuarios. Se configura el correo para poder realizar la recuperación de contraseña de usuarios que hayan sido creados manualmente (No aplica para los que son importados).

Para mayor información consulte la Gestión de Servidor de Correos ↪.

4. Servicios de Directorio

En este módulo podrá establecer los servicios de directorio que pueden ser usados en una aplicación de Aranda, como el protocolo ligero de acceso a directorios LDAP, que permite configurar la conexión con otros directorios empresariales o el servicio de directorios Azure Active Directory

Para mayor información consulte la Gestión Servicios de Directorio ↪.

5. Proveedores de Autenticación

En este módulo podrá establecer los proveedores de autenticación externa, que siguen el estandar SAML (Security Assertion Markup Language) para realizar la autenticación del usuario en la aplicación. y posterior y notificación sobre el estado de la validación.

Para mayor información consulte la Gestión Proveedores de Autenticación ↪.

6. Tokens de Integración

En este módulo podrá realizar la configuración de conexión del API y agregar detalles para la creación del Token. Este token permite consumir las APIS del producto que lo requiere, desde aplicaciones externas, sin necesidad de credenciales de autenticación.

Para mayor información consulte la Gestión Tokens de Integración ↪.

Entorno Commons

La gestión y configuración de los procesos de configuración para diferentes aplicaciones Aranda se realizan desde un entorno web con opciones y acciones compartidas.

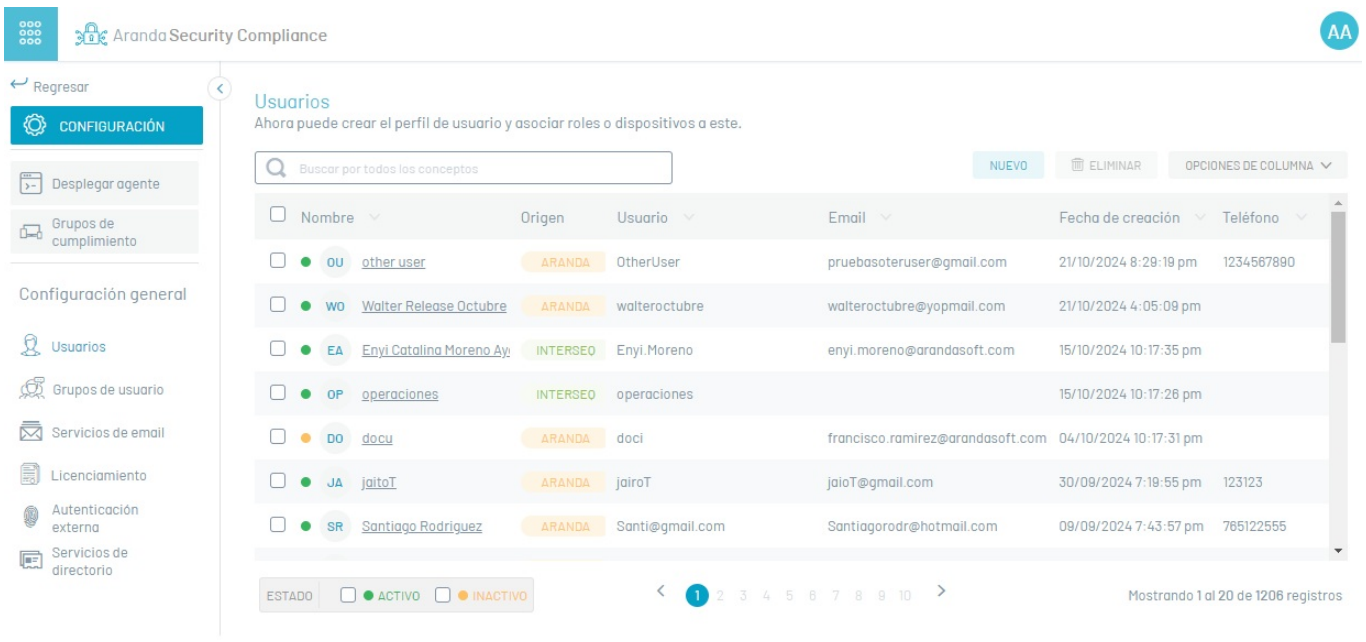
Visualizar Entorno

1. Después de iniciar sesión, ingrese a la consola web del producto con el rol establecido (administrador, especialista, usuarios).

2. En el menú principal del producto Aranda, en la sección de Configuración, seleccione el módulo respectivo (Usuarios, servidor de correo, autenticación externa, servicios

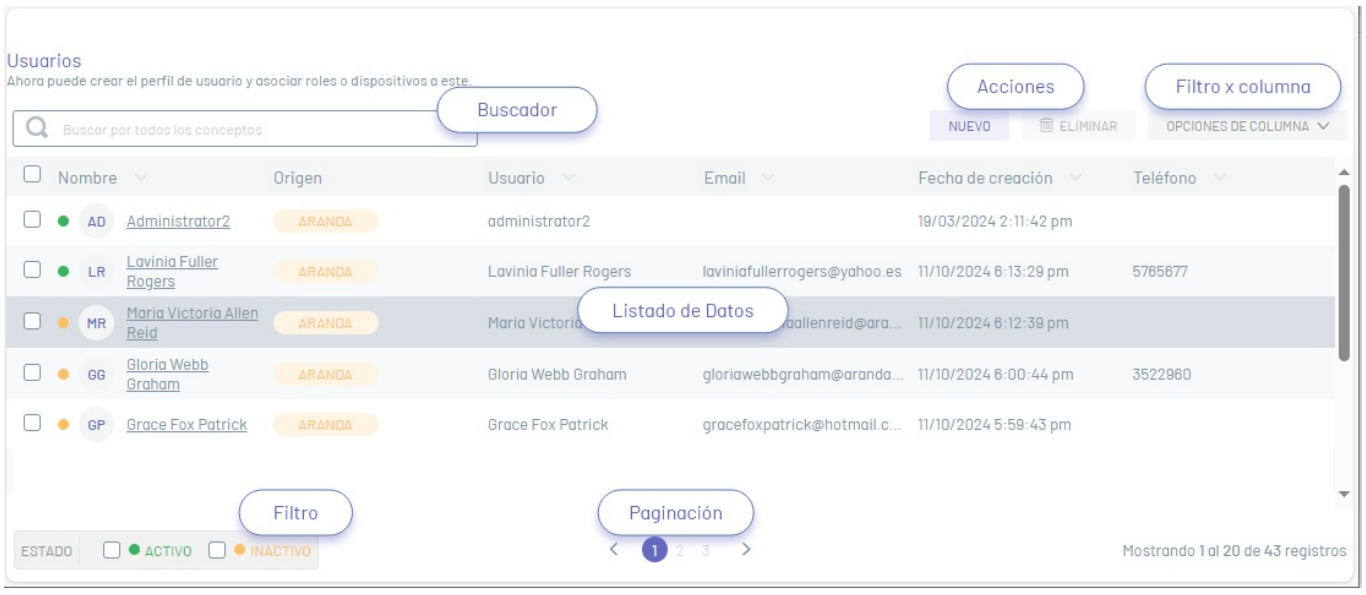
de directorio, tokens de integración) y al hacerlo se habilita la vista de información con los datos relacionados.

⚐ Ejemplo: En la siguiente imagen podrá visualizar la sección de configuración del producto Aranda Security, con los módulos common utilizados.



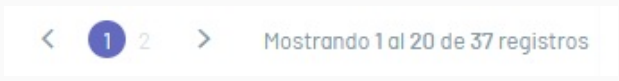
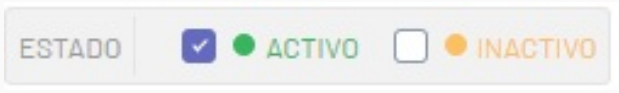
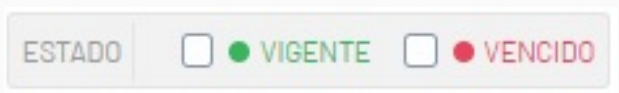
Entorno Commons/ Módulos

3. En la vista de información del módulo común seleccionado (Usuarios, Servidor de correo, Servicios de directorio, autenticación externa) podrá encontrar acciones transversales que complementan las tareas de gestión como:



A continuación se presentan las opciones disponibles y los módulos de commons donde son utilizadas:

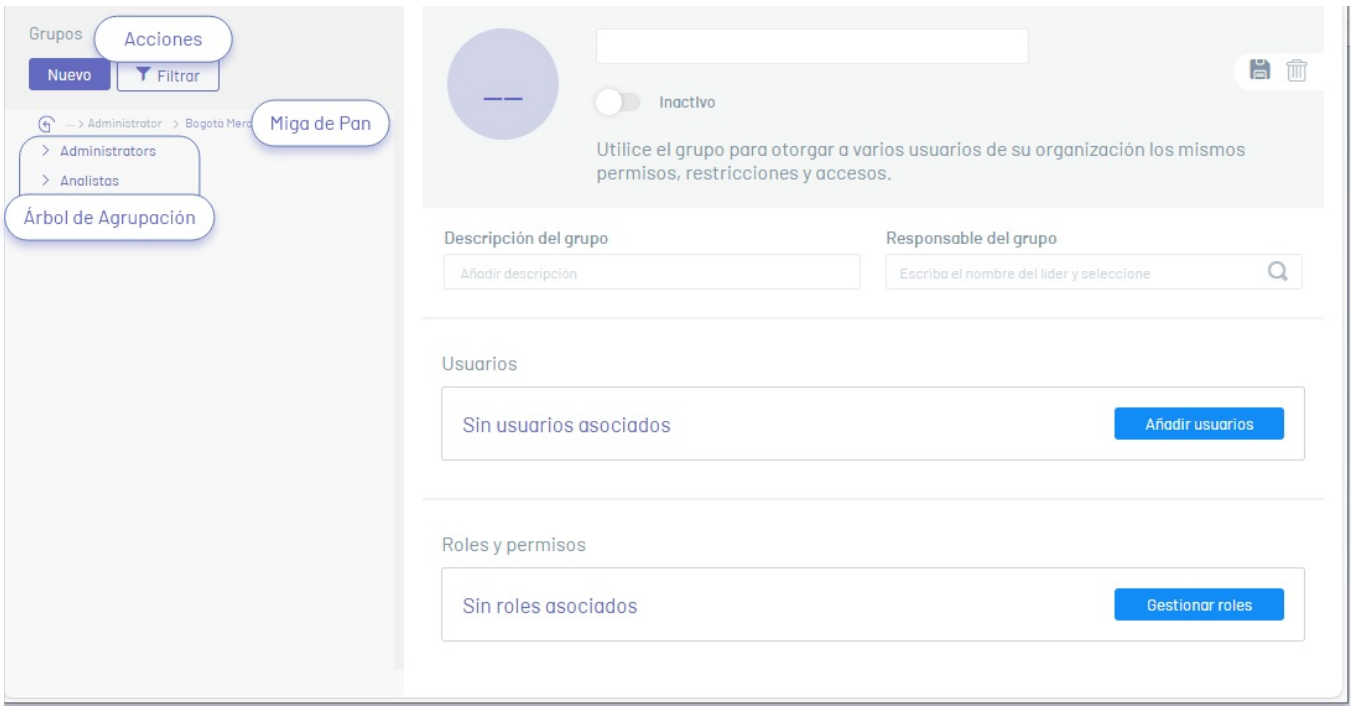
Opción	Descripción	Módulos common
Búsqueda	Permite buscar el listado de usuarios de acuerdo al criterio de búsqueda. Se puede buscar por el nombre de los campos definidos de cada concepto asociado.	
Listado de datos	Esta sección agrupa la información de los registros encontrados por módulo o concepto seleccionado. La información presentada se agrupa en columnas con los datos ingresados. Al seleccionar el registro del listado disponible, podrá consultar y editar los datos asociados, o eliminar el registro.	

Nuevo	Este botón define la acción para crear un registro para cada concepto de gestión de los productos de Aranda. Al activar esta acción se habilita una ventana para completar la información relacionada. 
Eliminar	Este botón define la acción para eliminar un registro ya creado en los procesos de gestión. 
Filtro por de columna	Permite mostrar o ocultar opciones de la lista.  Las opciones de columna del módulo de usuarios son: Nombre, origen, usuario, email, fecha de creación y teléfono.
Paginación	Permite navegar entre las páginas del listado de registros de usuario encontrados. 
Filtro por estado	Permite filtrar por el estado activo o inactivo de usuarios o proveedores de autenticación.  En el módulo Tokens de integración permite filtrar por el estado vigente o vencido de tokens de conexiones de API creados. 
Seguridad	Este botón  define la acción para realizar la configuración del reCAPTCHA para usarla al momento de autenticación de los usuario.

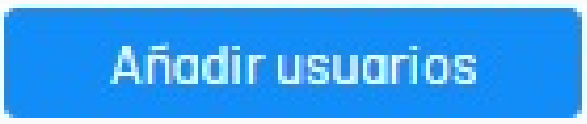
Entorno Commons/ Modulo Grupos

4. En la vista de información del módulo común seleccionado (Grupos) podrá encontrar acciones que complementan las tareas de gestión.

5. En la estructura tipo árbol para los grupos de usuario, podrá identificar los siguientes componentes:



Opción	Descripción	Módulos common
Nuevo	Este botón  define la acción para crear un registro grupos de usuario. Al activar esta acción se habilita una ventana para completar la información relacionada.	
Filtrar	Este botón  define la acción para realizar una búsqueda avanzada por todo el árbol de grupos. Al activar esta acción se habilita una ventana para completar la información relacionada	
Árbol de agrupación	Esta seción despliega los grupos y subgrupos definidos.	
Eliminar	Este botón  define la acción para eliminar un registro ya creado de grupos	
	Este ícono	

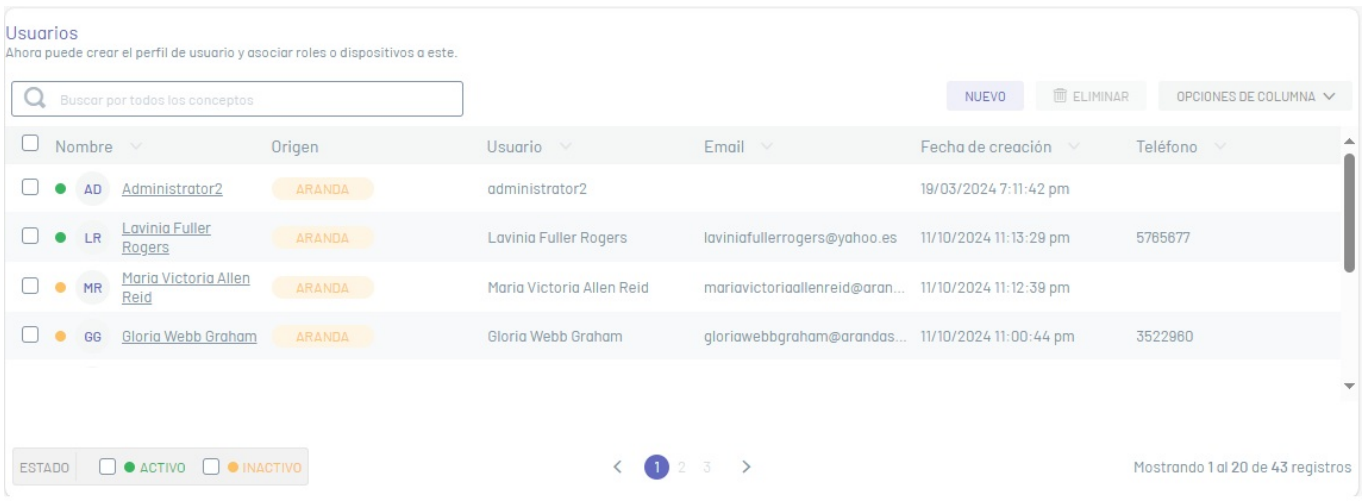
Miga de pan		muestra la ubicación actual en el árbol de los grupos.
Añadir Usuarios		Este botón define la acción para asociar usuarios a un grupo establecido.
Gestionar Roles		Este botón define la acción para asociar roles a un grupo establecido.

Módulo Usuarios

Gestión de usuarios

Visualizar Usuarios

1. En la vista de información de Usuarios podrá visualizar el listado de usuarios registrados o importados, agrupados por datos como:



Campo	Tipo Campo	Descripción
Nombre	Texto	Nombre con el cual se identifica el usuario.
Origen	Texto	Indica el origen por el cual fue creado el usuario
Usuario	Texto	Nombre usado por el usuario para acceder a la aplicación.
Email	Texto	Correo del usuario para recibir información.
Fecha de creación	Selector	Indica si el usuario se encuentra activo o inactivo.
Teléfono	Texto	Número de teléfono del usuario.

⚐ Nota: La columna Origen indica el nombre del servicio de directorio que realizó la importación del usuario; si el nombre del origen es Aranda son usuarios que no fueron importados sino que se crearon directamente desde esta interfaz.

2. En la vista de información de los usuarios, tendrá habilitadas acciones de gestión y organización de la información.Vista de Información en Entorno Commons

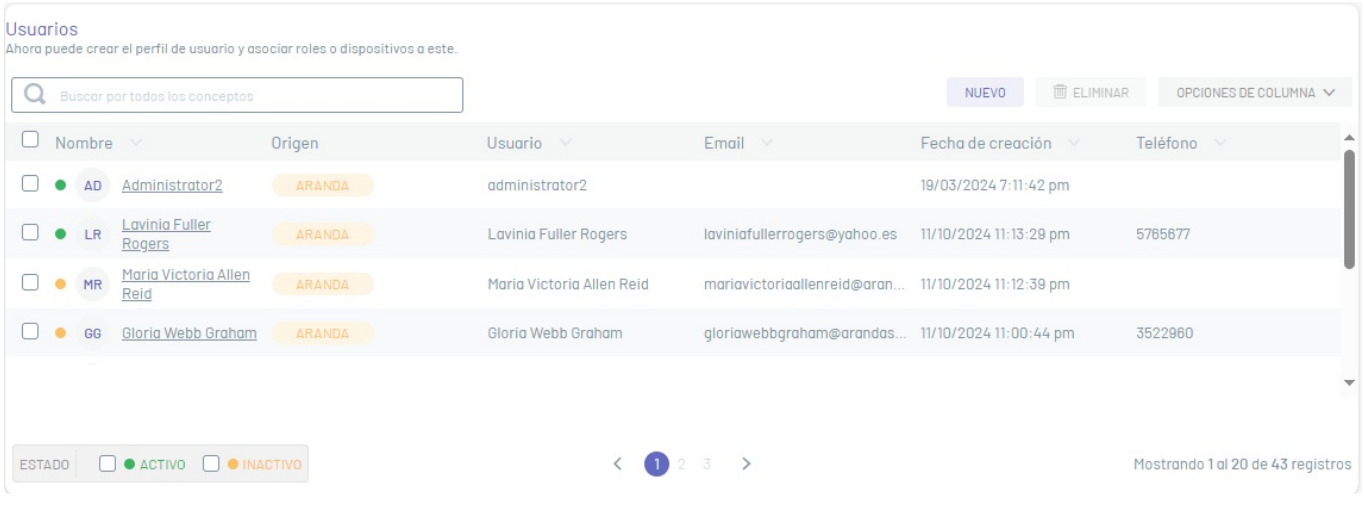
Enlaces Relacionados:

- Crear Usuarios
- Editar Usuarios

- Eliminar Usuarios

Crear usuarios

1. Para crear un nuevo usuario, en la vista de información de usuario, haga clic en el botón Nuevo.

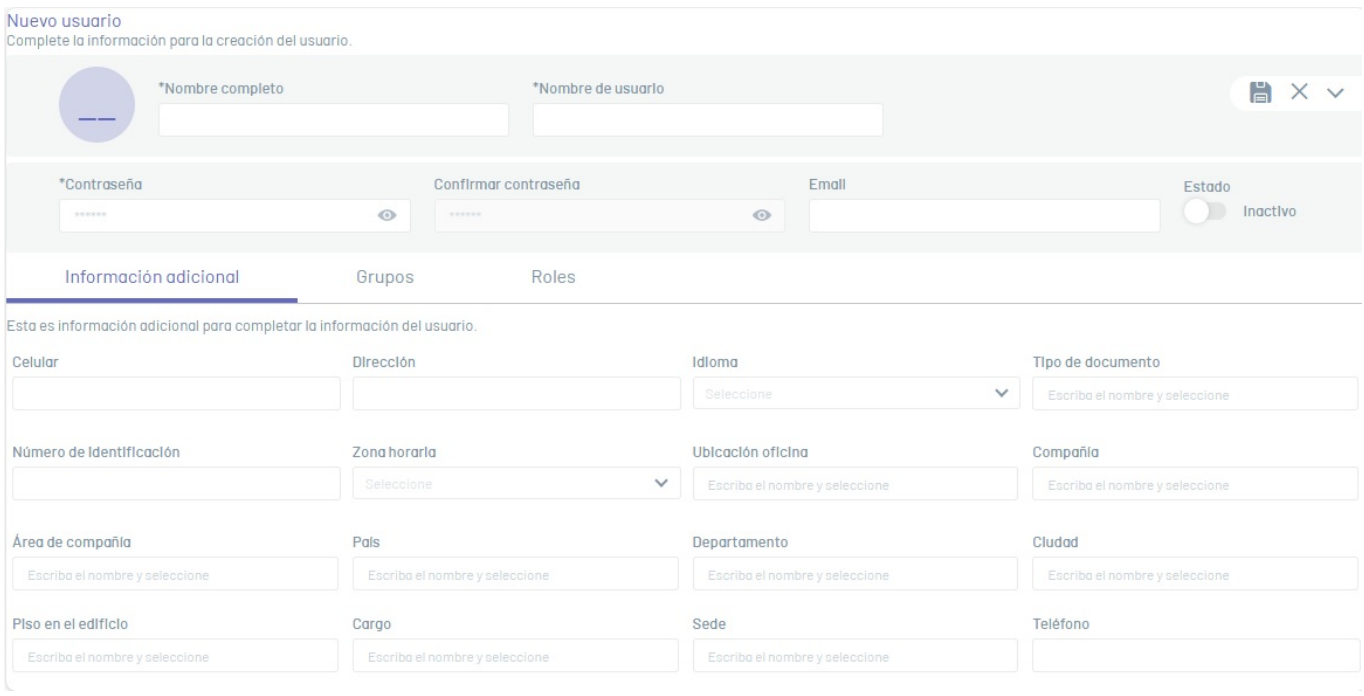


⚐ Nota: No podrá crear un usuario con el mismo nombre de usuario a menos que pertenezca a otro proveedor de autenticación.

Datos Básicos

2. En la ventana que se habilita podrá completar los datos básicos del usuario, información adicional, asociación de grupos y roles.

3. En los datos básicos del usuario podrá ingresar campos como nombre, contraseña, correo y estado. Cada uno de los campos del usuario deben tener en cuenta las especificaciones para campos Common



Informacion Adicional

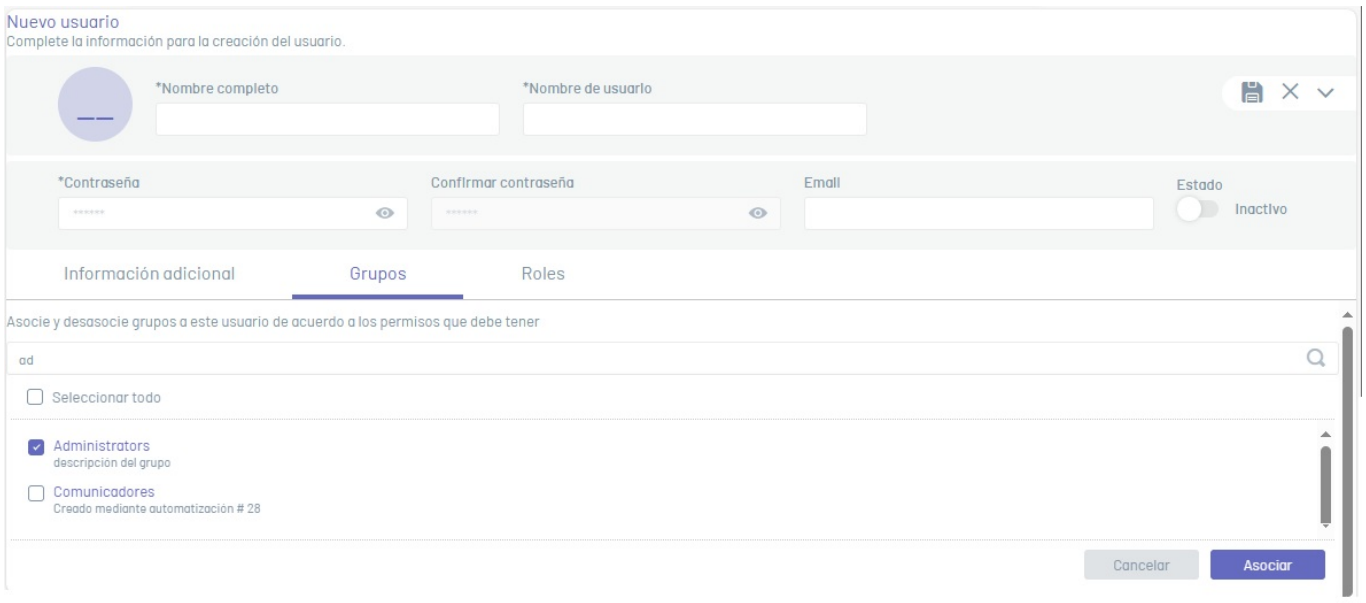
4. En la pestaña Información Adicional ingrese los siguientes campos: Número de celular, dirección, idioma, teléfono, entre otros. Cada uno de los campos del usuario deben tener en cuenta las especificaciones para campos

⚐ Nota: La información Adicional de Usuarios es opcional y no es obligatorio para la creación de usuarios.

Asociación y desasociación de Grupos

4. En la pestaña Grupos, en el campo de búsqueda para asociar grupos, podrá relacionar al usuario, el o los Grupos de usuarios requeridos.

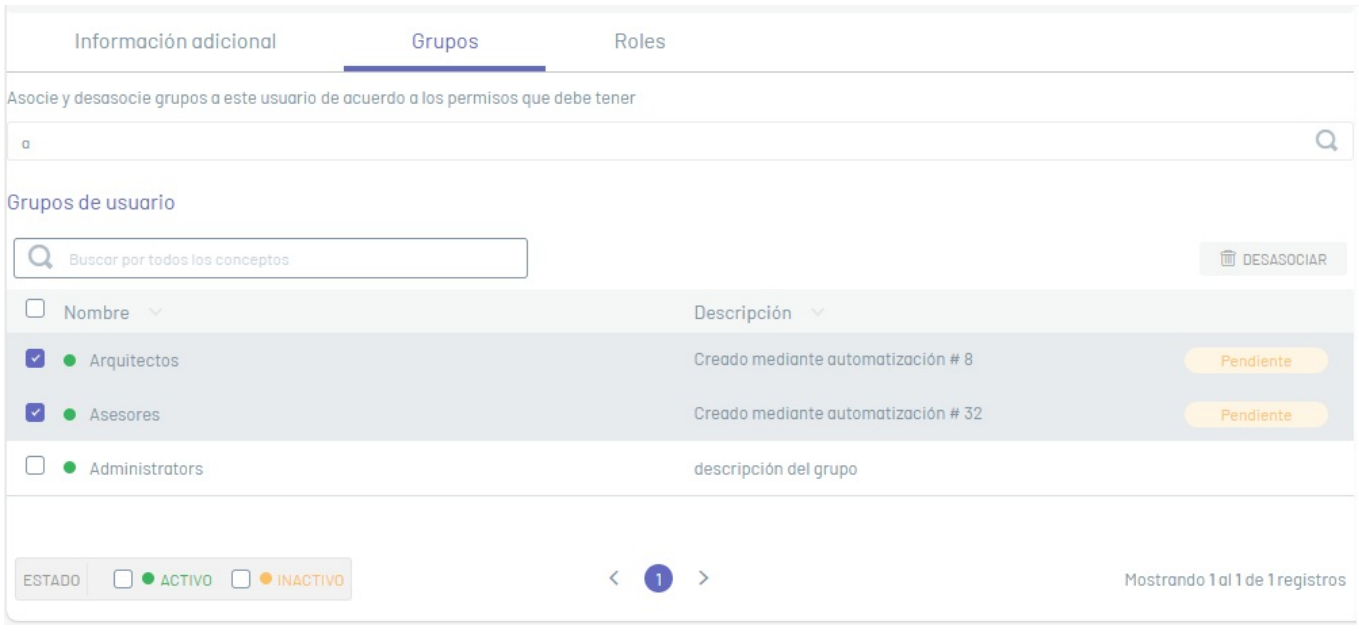
5. Seleccione uno o todos los grupos requeridos y haga clic en el botón Asociar.



6. Los grupos asociados se podrán visualizar en el listado de grupos de usuario.

7. Para buscar los grupos que pertenecen al usuario, podrá utilizar la barra de búsqueda de grupos de usuario. Los grupos en estado pendiente no permiten hacer el filtro, ni la búsqueda por texto.

8. Para desasociar un grupo, seleccione un registro del listado de grupos de usuario y haga clic en el botón Desasociar.



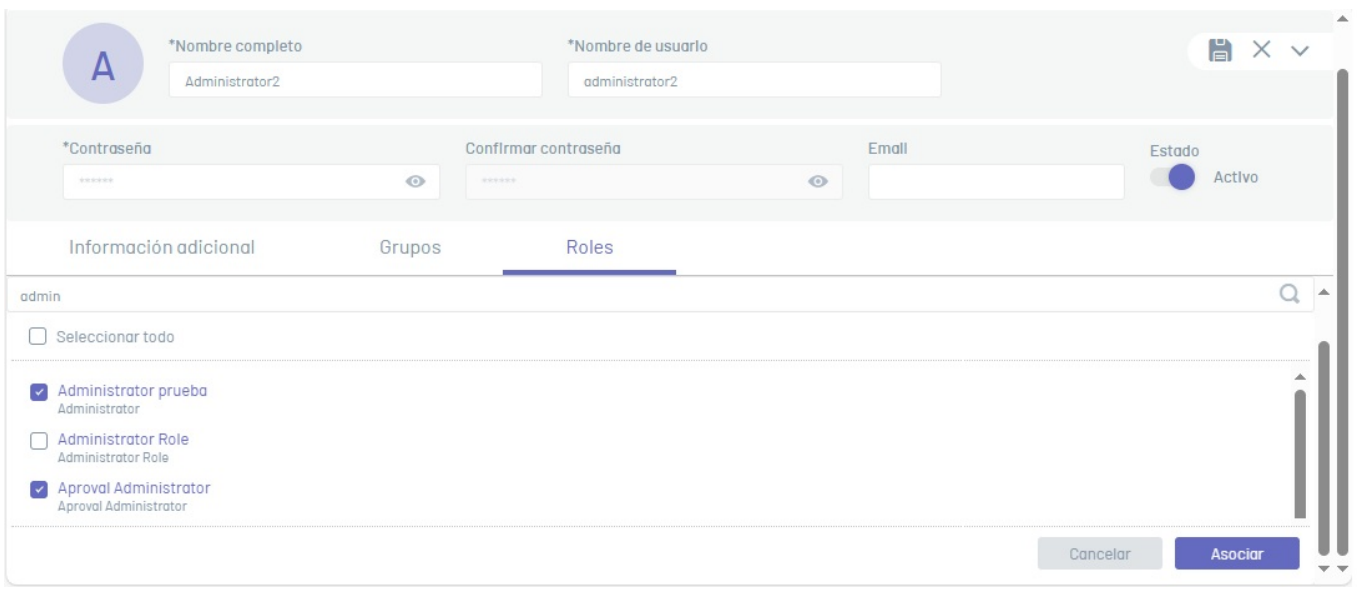
⚐ Nota:

- Todos los roles del grupo serán heredados a los usuarios que pertenezcan a esta agrupación.
- En la lista solo aparecerán grupos que no sean importados y estén activos.
- Si no se han guardado los cambios, aparecerá una columna con el mensaje Pendiente que significa que los cambios no se han guardado y aún no pertenecen al usuario.

Asociación y desasociación de Roles

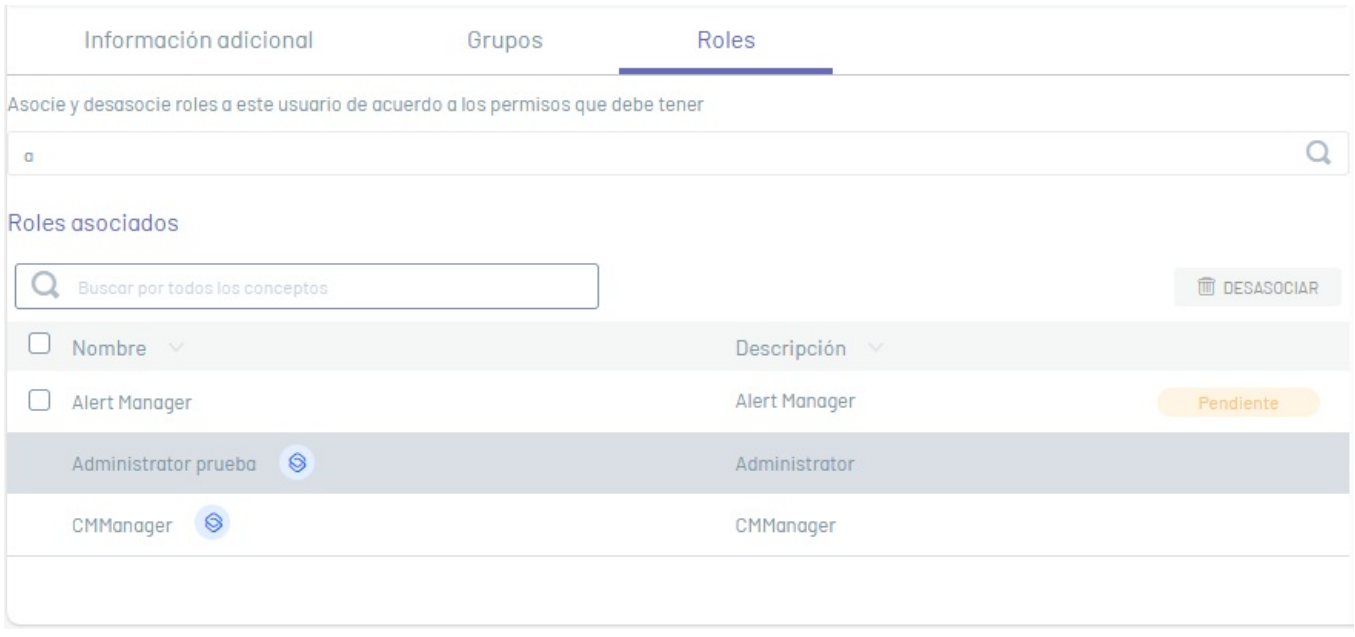
9. En la pestaña Roles, en el campo de búsqueda para asociar roles, podrá asociar los roles al usuario seleccionado, de acuerdo a los permisos establecidos.

10. Seleccione uno o todos los roles que desea relacionar y haga clic en el botón Asociar.



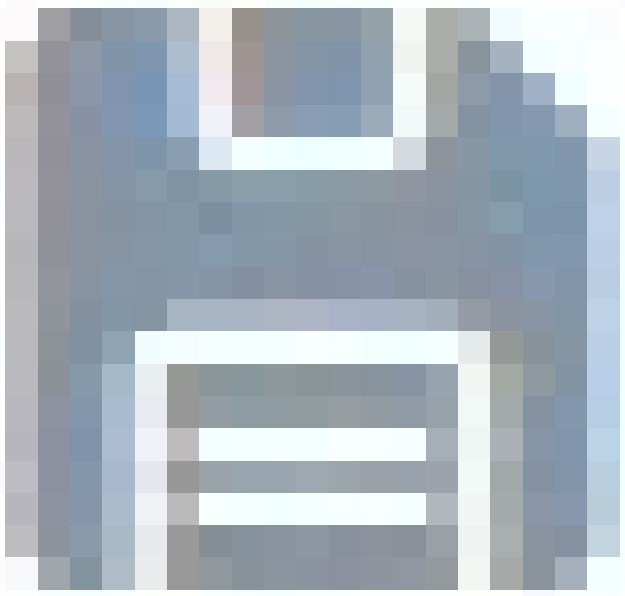
11. Los roles asociados se podrán visualizar en el listado de roles de usuario.

12. Para desasociar un rol, seleccione un registro del listado de roles de usuario y haga clic en el botón Desasociar.



⚐ Nota: : Si el rol se encuentra en estado Pendiente es porque la información del usuario no se ha guardado y por lo tanto no se ha asociado al usuario.

11. Al terminar de configurar el nuevo usuario, haga clic en el ícono Guardar

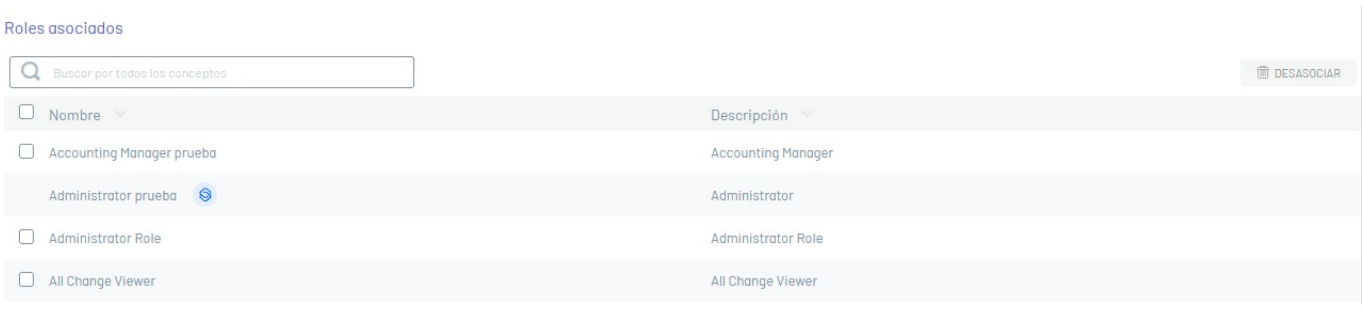


para confirmar los cambios realizados.

⚐ Nota: : Todos los usuarios creados por este medio son de tipo Aranda, este valor se visualiza en la columna Origen en el listado de usuarios.

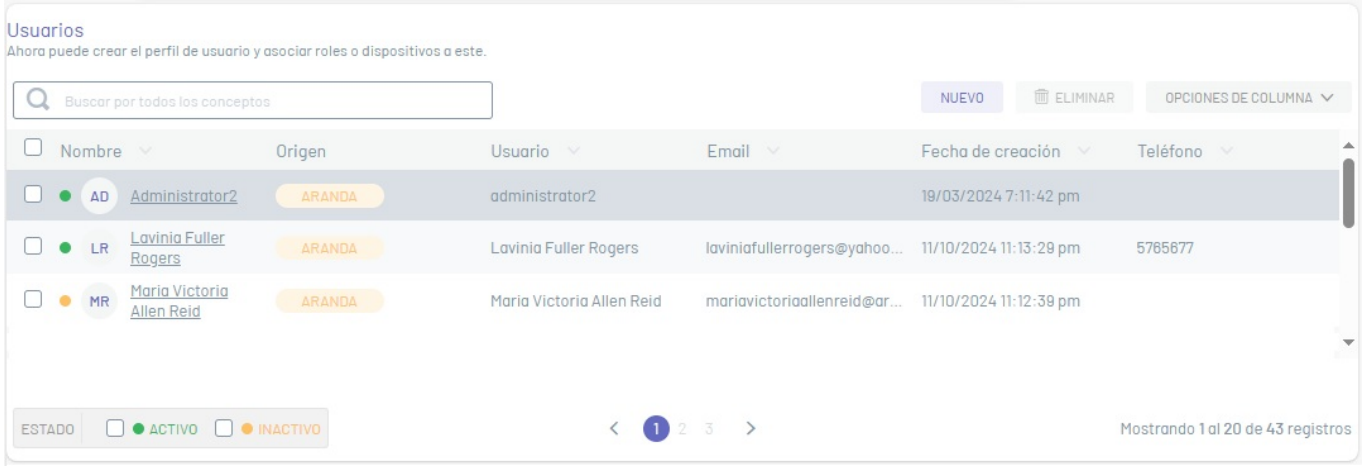
12. Si el usuario pertenece a un grupo, este heredará los roles del grupo. Cada rol se identifica con el ícono

y solo se podrá desasociar removiendo el usuario del grupo.



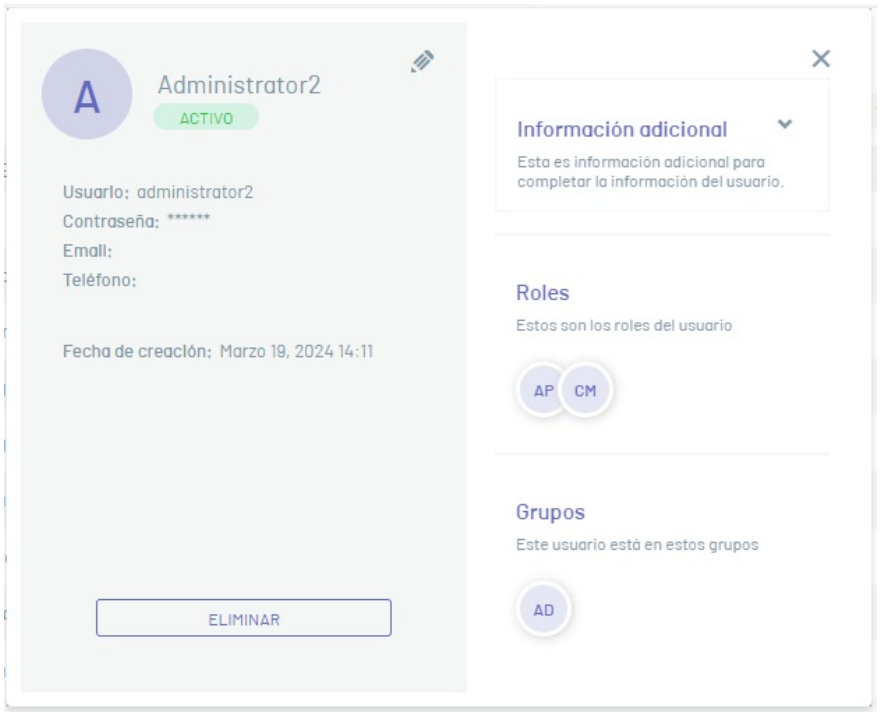
Editar usuarios

1. Para modificar un usuario, en la vista de información de usuarios seleccione un registro del listado de usuarios existentes.

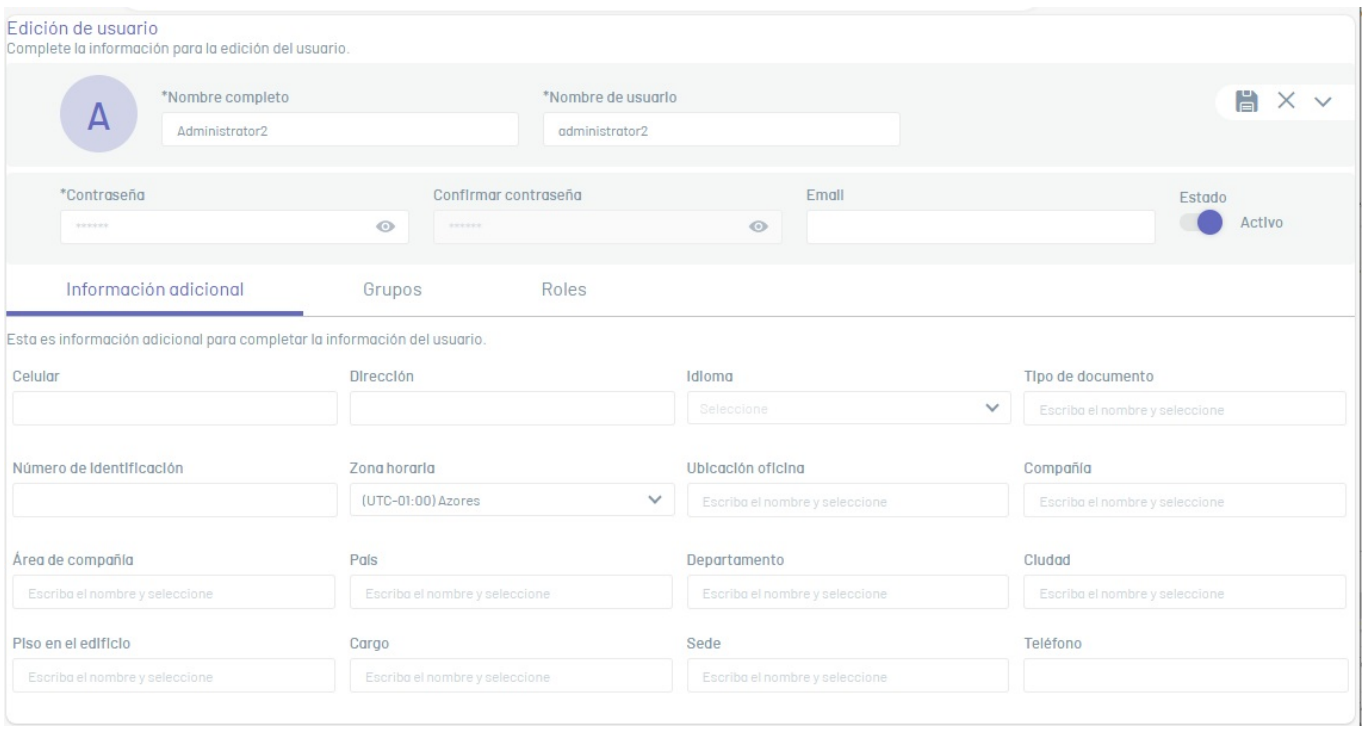


2. En la vista de detalle del usuario, haga clic en el ícono Editar

y modifique la información requerida.

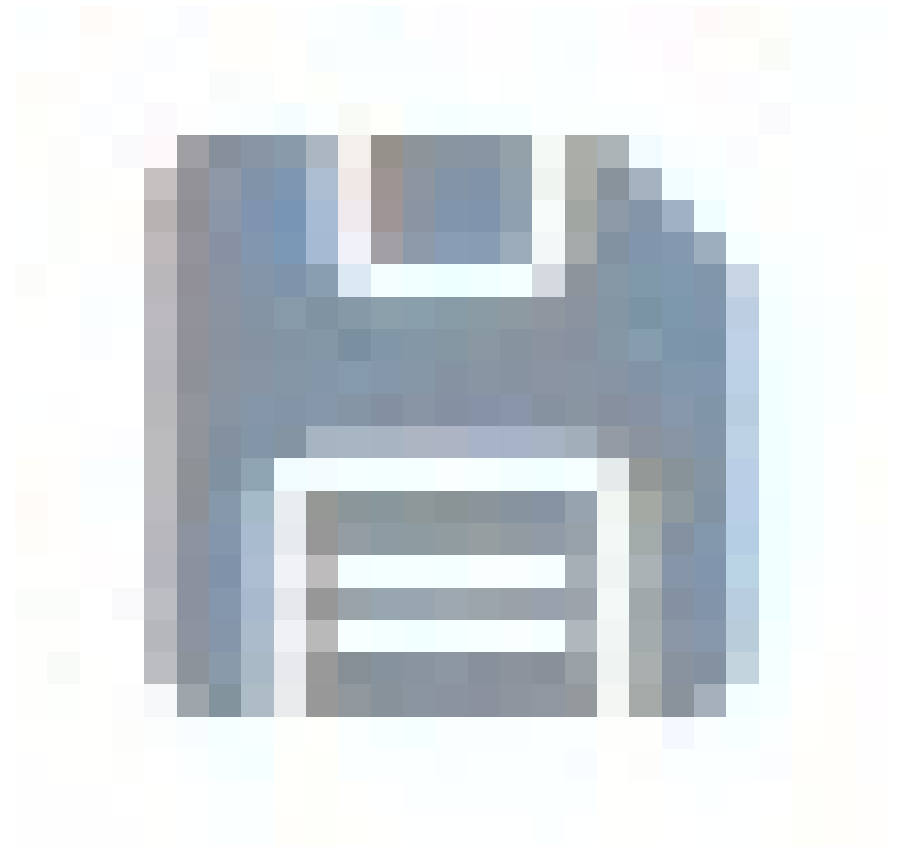


2. En la ventana Edición de Usuario podrá actualizar la información básica y adicional del usuario; así como los grupos y roles asociados al usuario.



⚐ Nota: Solo se podrán modificar los usuarios del proveedor Aranda. Los usuarios importados solo permite asociar y desasociar roles, modificar los campos estado, idioma y la zona horaria.

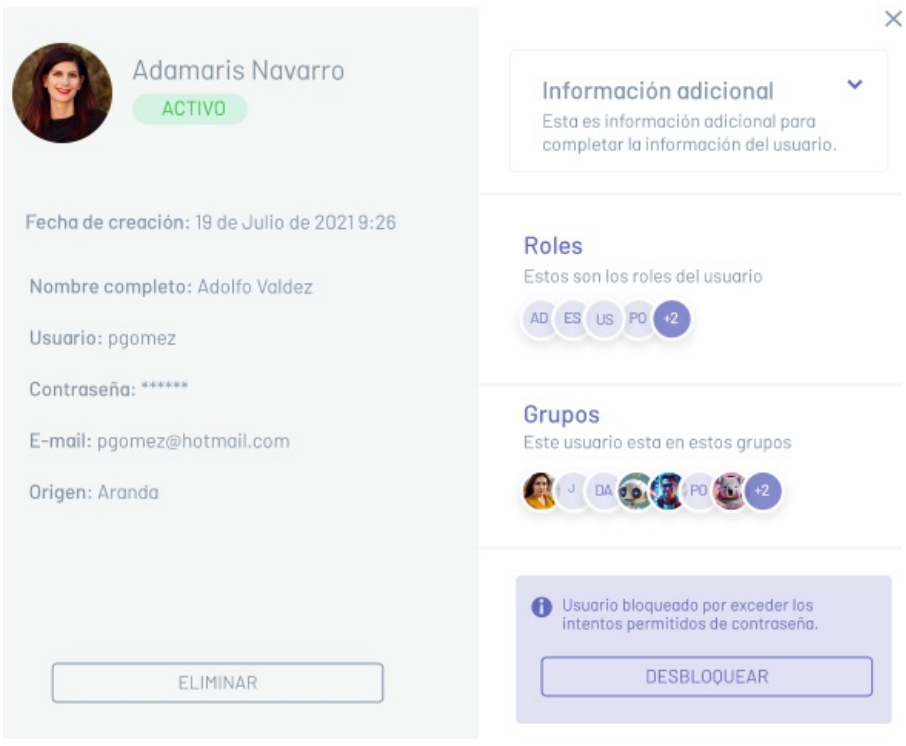
3. Al terminar de editar el usuario, haga clic en el ícono Guardar



para confirmar los cambios realizados.

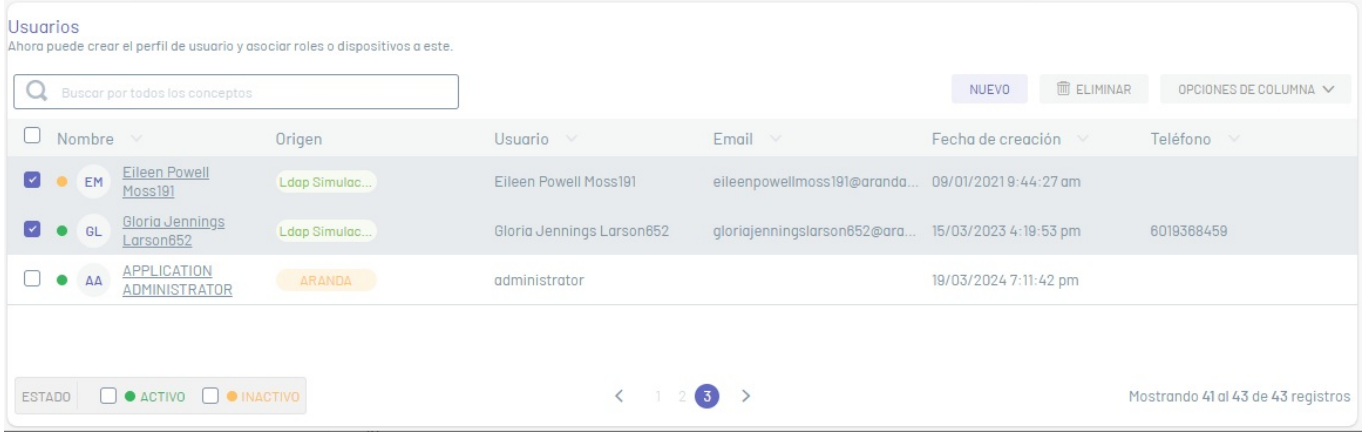
Desbloquear Usuario

⚐ Nota: Cuando un usuario es bloqueado por exceder los intentos permitidos de contraseña, en la vista de detalle del usuario, se activa un mensaje de advertencia y el botón DESBLOQUEAR. Al ejecutar esta acción el usuario bloqueado podrá iniciar sesión de nuevo.



Eliminar usuarios

1. En la vista de información de usuarios seleccione uno o varios registros del listado de usuarios existentes y haga clic en el ícono Eliminar para borrar la información asociada.



2. Podrá visualizar un mensaje de confirmación para validar la acción de borrado.

⚐ Nota:

- Un usuario eliminado no podrá ser restaurado.
- Si el usuario tiene registros asociados en base de datos, la eliminación fallará.
- Los usuarios con el rol de Administrador y hayan iniciado sesión no se les permitirá su eliminación.
- Si elimina usuarios importados, en la siguiente sincronización del servicio de directorio, es posible se creen de nuevo.

Módulo Grupos

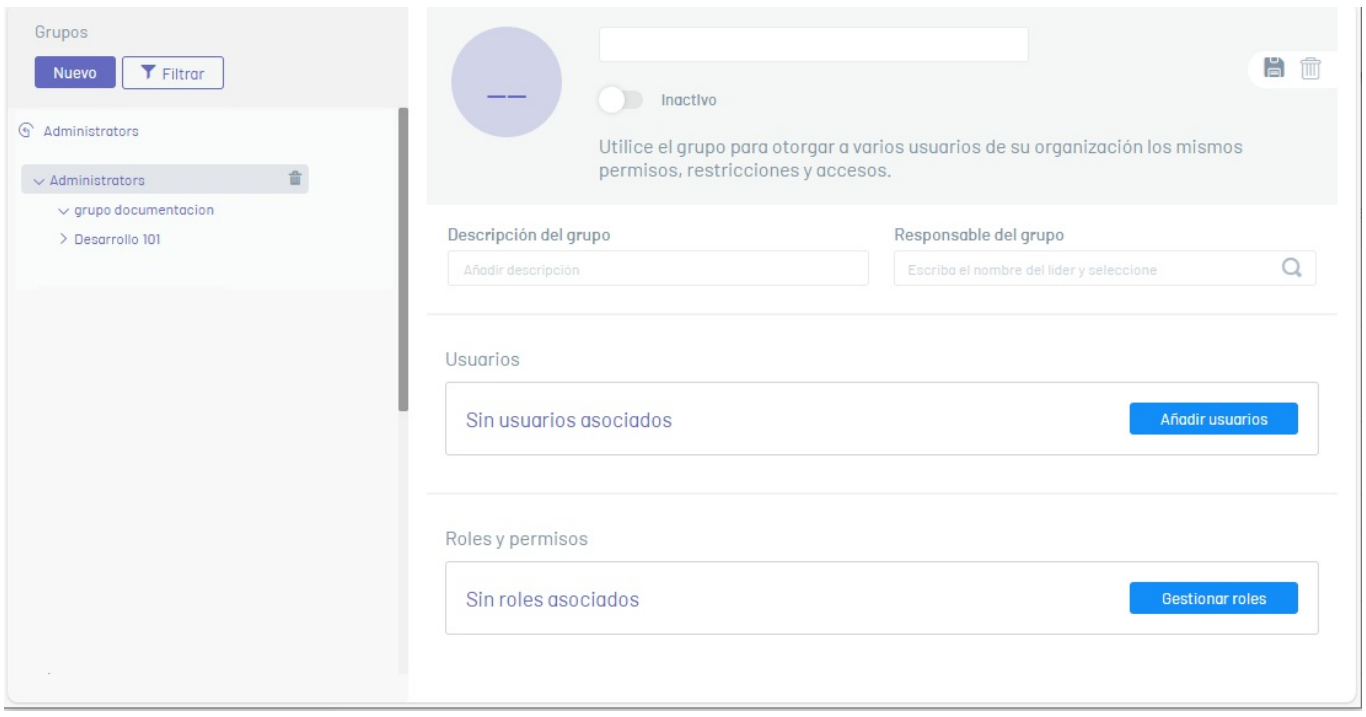
Gestión de grupos

Visualizar Grupos de Usuario

1. En la vista de información de Grupos de Usuario podrá visualizar una estructura tipo árbol con los grupos y subgrupos de usuario registrados o importados.

2. Al seleccionar el nombre de un grupo podrá desplegar la información de los subgrupos relacionados. En la vista de información podrá visualizar la información del grupo en tres secciones:

- Información Básica: Se presenta la información básica del grupo como nombre, estado, descripción del grupos y el responsable del grupo; también podrá editar la información relacionada.
- Usuarios: En esta sección podrá gestionar usuarios al grupo de usuarios.
- Roles y permisos: En esta sección podrá gestionar los roles del grupo de usuarios.



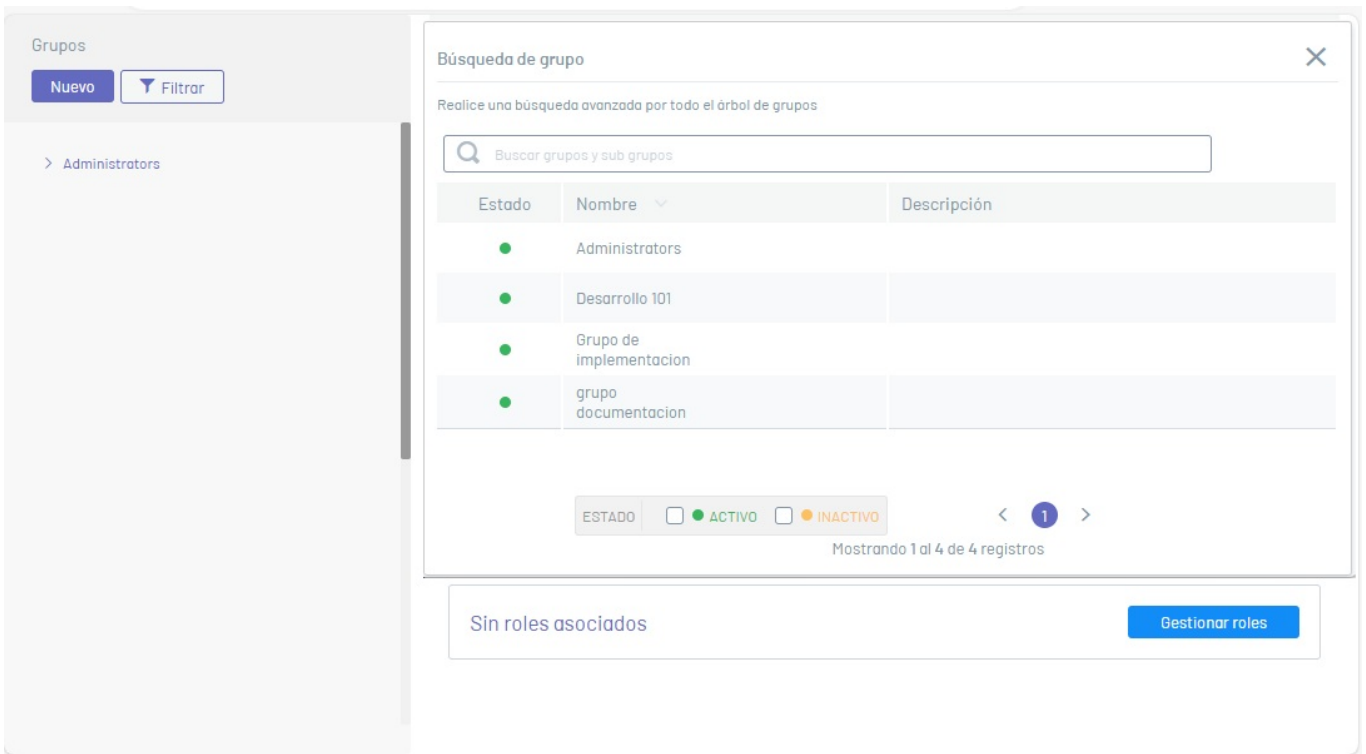
⚐ Nota: Aún si un grupo está deshabilitado se mostrará en el árbol.

2. En la vista de información de grupos, tendrá habilitadas acciones de gestión y organización de la información.[Vista de Información en Entorno Commons]

Filtrado de grupos

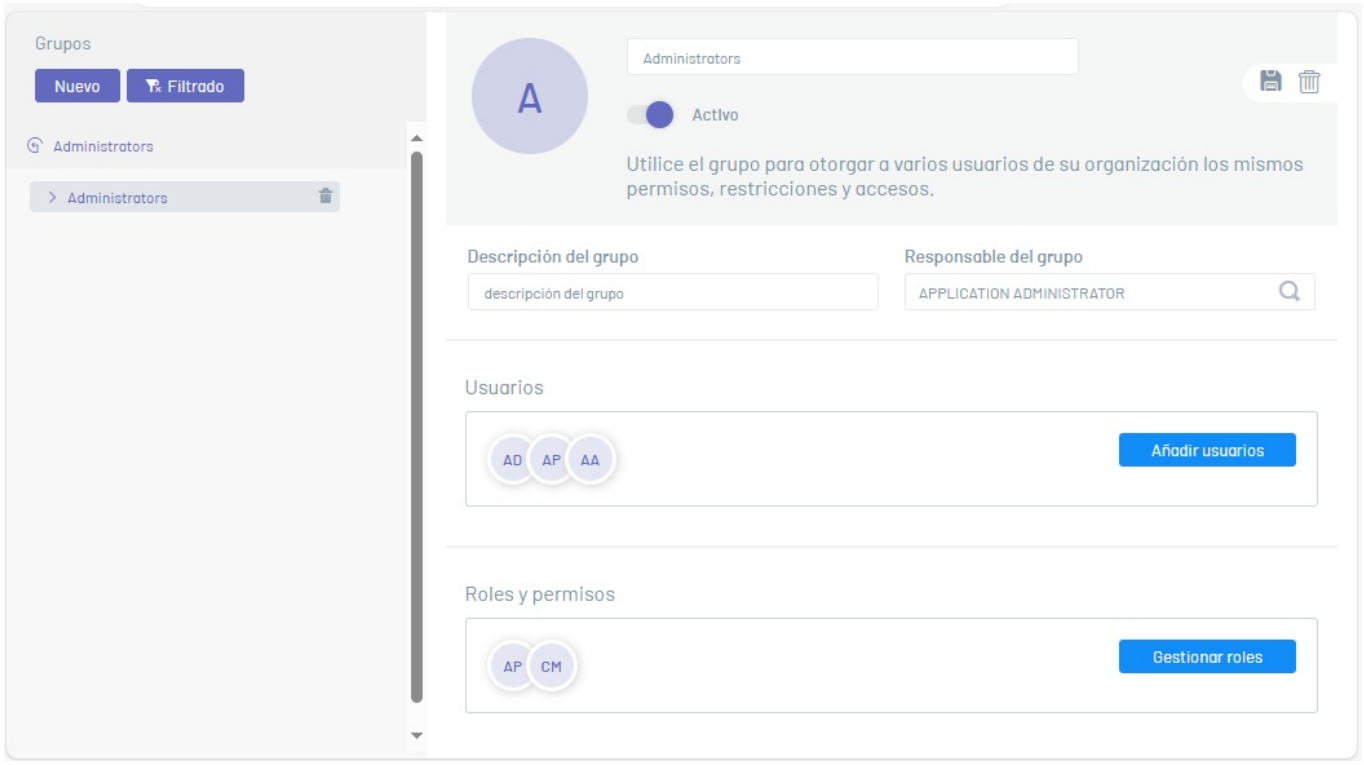
1. En la vista de información de grupos de usuario seleccione el botón Filtrar.

2. Se habilita la ventana Búsqueda de grupo donde podrá realizar la consulta requerida; en el campo Buscar ingrese una palabra clave.



3. Seleccione un registro de los grupos encontrados en la búsqueda. Al hacerlo se habilita la ventana detalles del grupo.

4. En la vista de información de grupos de usuario podrá limpiar la información filtrada haciendo clic en el botón



Enlaces Relacionados:

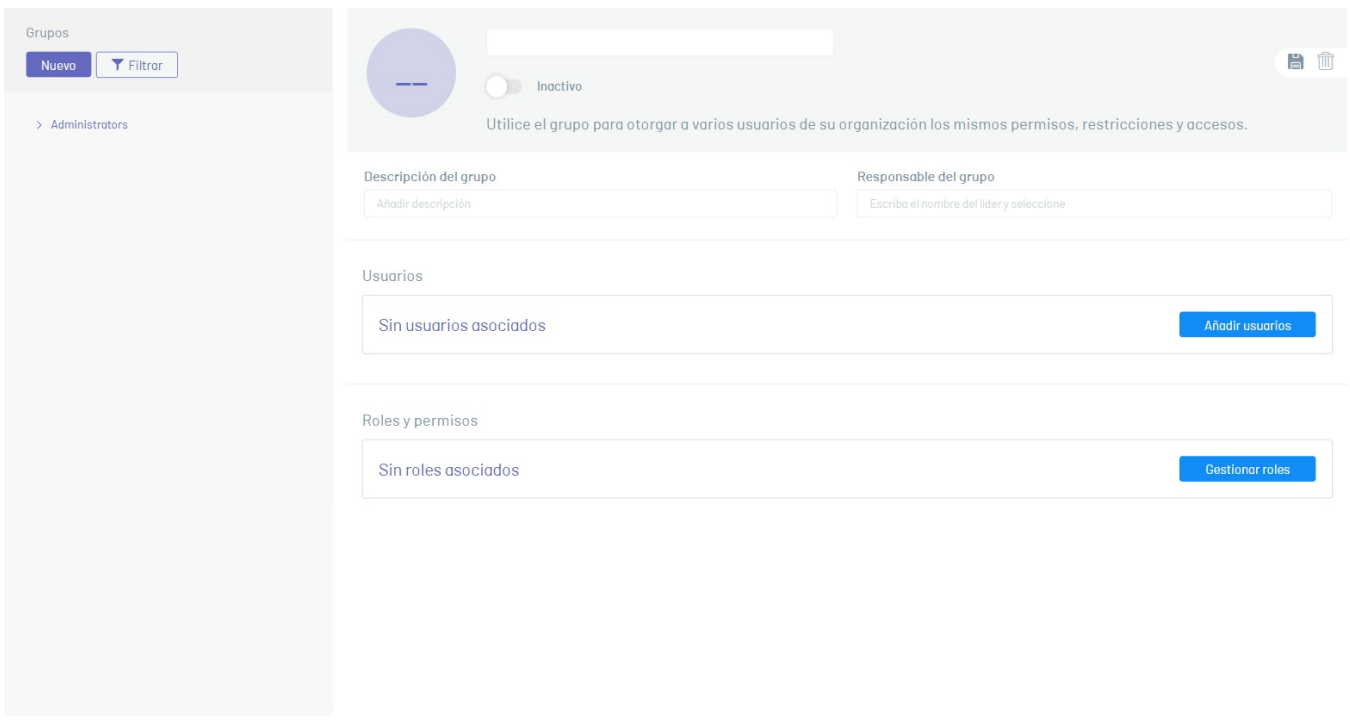
- Crear Grupos
- Editar Grupos
- Eliminar Grupos

Crear grupos

Datos Básicos

1. Para la creación de un grupo sin ninguna jerarquía superior, debe estar ubicado en la raíz del árbol; en la vista de información podrá visualizar el formulario para completar la información requerida (información básica, asociar usuarios y roles).

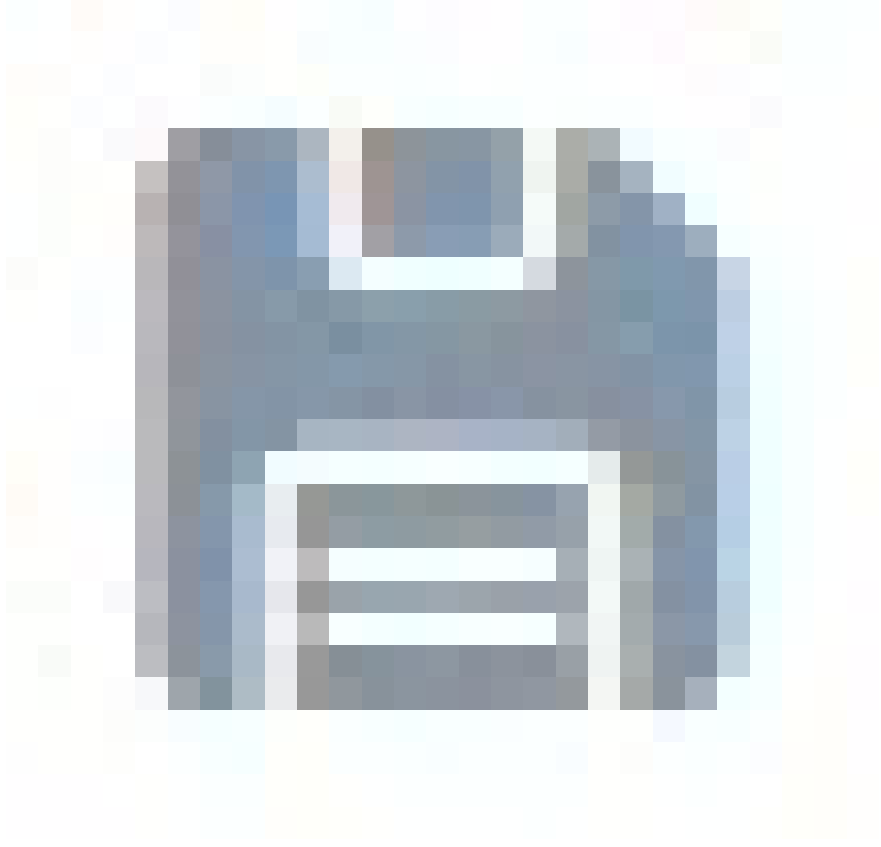
2. Si el grupo a crear debe pertenecer a otro grupo, haga clic en el grupo padre requerido y en el botón Nuevo y complete la información requerida. Cada uno de los campos del grupo deben tener en cuenta las especificaciones para campos Common.



⚐ Nota:

- Los grupos importados no se pueden crear ya que es información recolectada desde el directorio de servicios.
- Podrá crear tantos subgrupos como requiera. Los subgrupos (grupos hijos) no heredan usuarios ni roles del grupo principal (grupo padre).
- Dos grupos no pueden tener el mismo nombre si están en el mismo nivel de jerarquía.

3. Al terminar de configurar el nuevo grupo, haga clic en el ícono Guardar

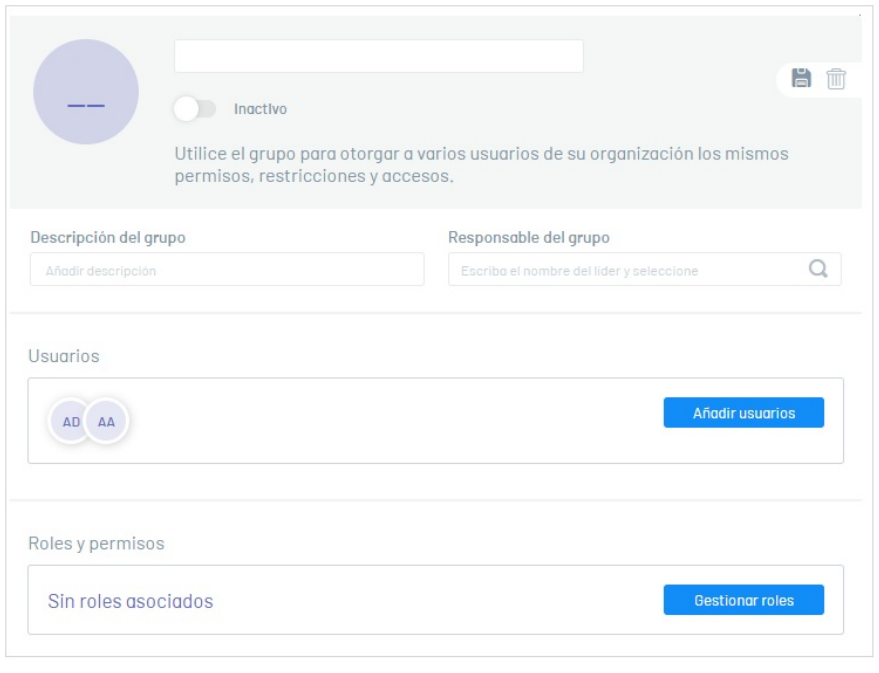


para confirmar los cambios realizados.

4. Una vez creado el grupo de usuarios se mostrará el mensaje que confirma la creación del grupo y se visualiza en el árbol su ubicación

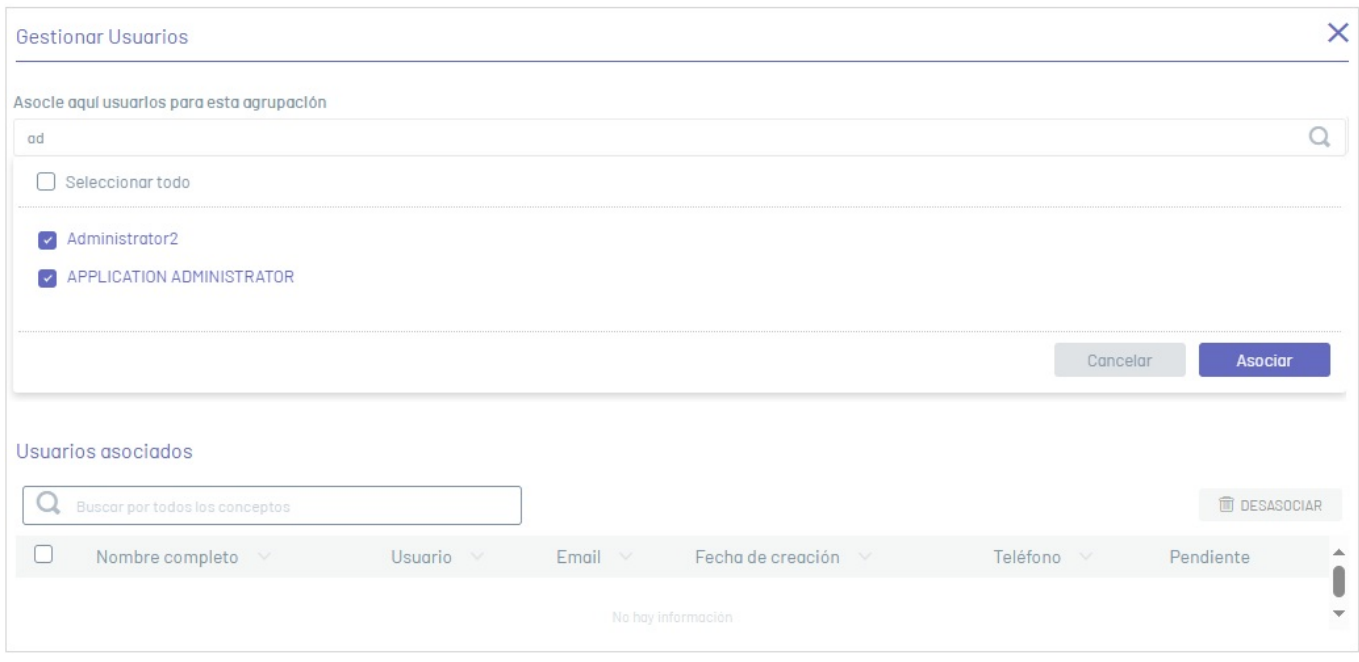
Asociar y desasociar usuarios al grupo

6. Para agregar usuarios, en la vista de información de un grupo de usuario, en la sección Usuarios, seleccione el botón Añadir usuarios.



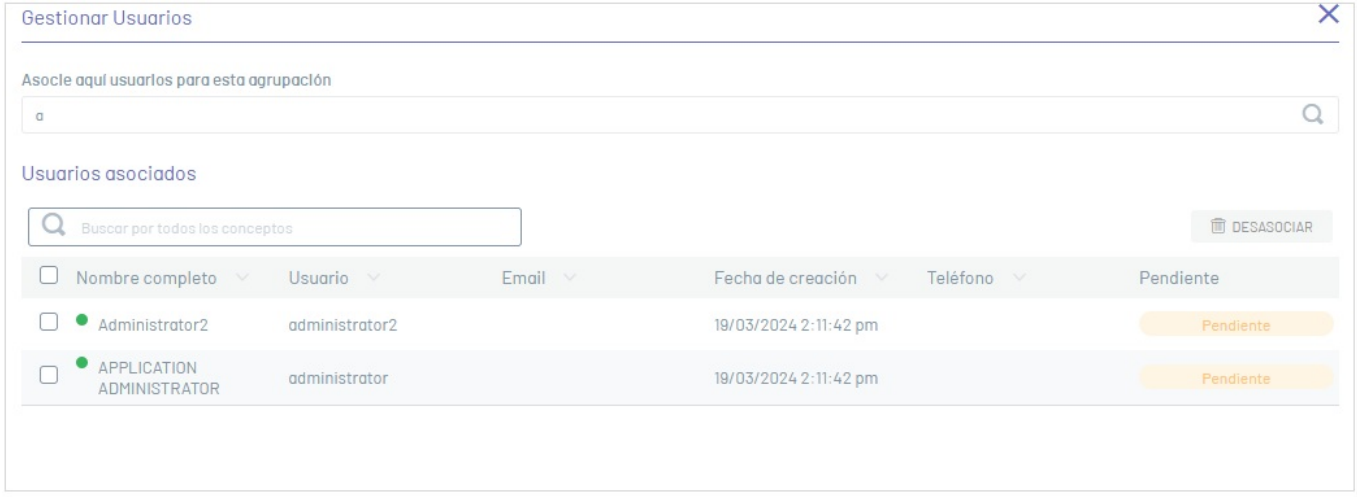
7. Se habilita la ventana Gestionar Usuarios, donde podrá consultar y agregar los usuarios requeridos para el grupo definido. En el campo de búsqueda ingrese el nombre del usuario requerido y en la lista de resultados seleccione el usuario a agregar.

8. Al terminar haga clic en el botón Asociar.



⚐ Notas:

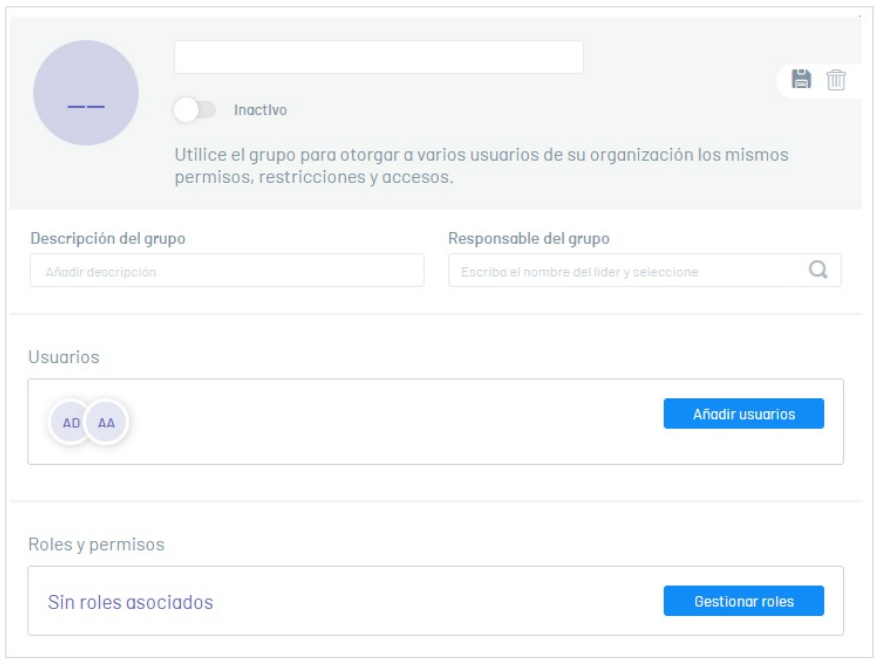
- Solo podrá listar usuarios activos. Los usuarios agregados quedarán con los roles del grupo.
- Una vez asociados los usuarios quedan en estado Pendiente hasta que se guarde el grupo



9. Para remover un usuario de un grupo, en la ventana Gestionar Usuarios seleccione uno o más registros del listado de usuarios y haga clic en el botón Desasociar. Confirme que desea desasociar los usuarios haciendo clic en el botón Aceptar.

Asociar y desasociar Roles

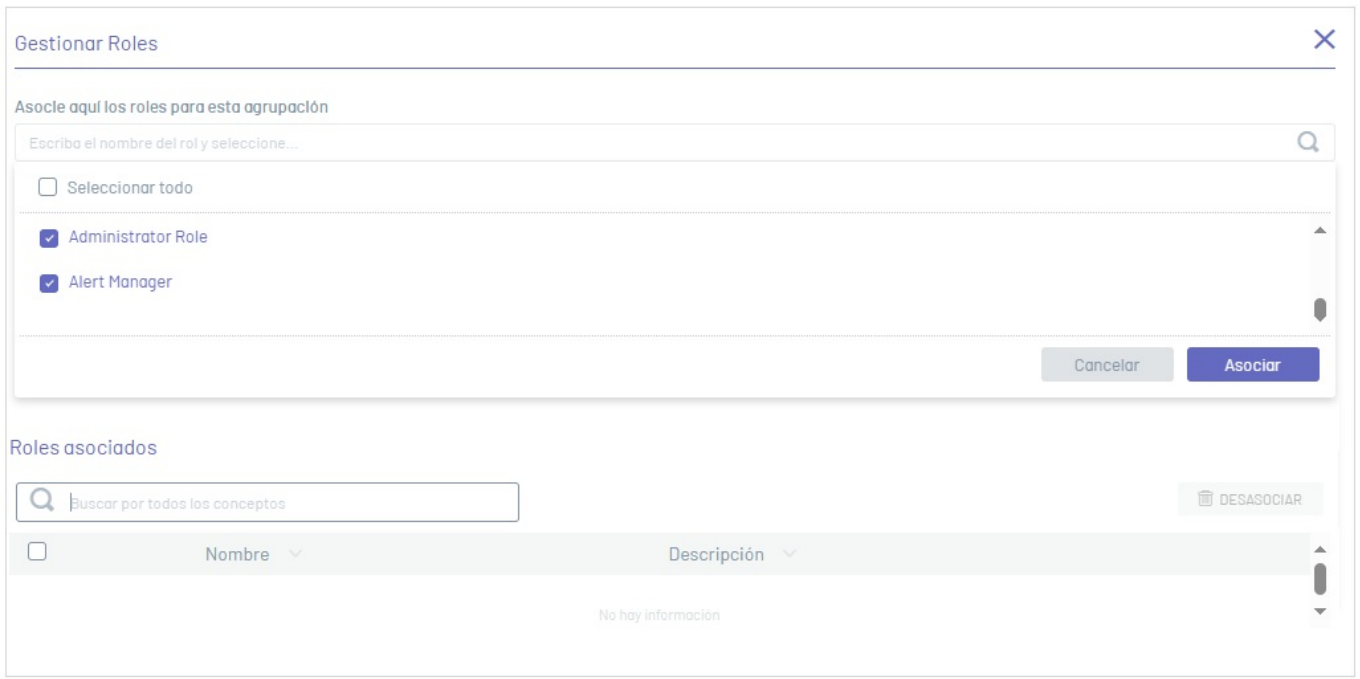
10. Para agregar roles, en la vista de información de un grupo de usuario, en la sección Roles y Permisos, seleccione el botón Gestionar Roles.



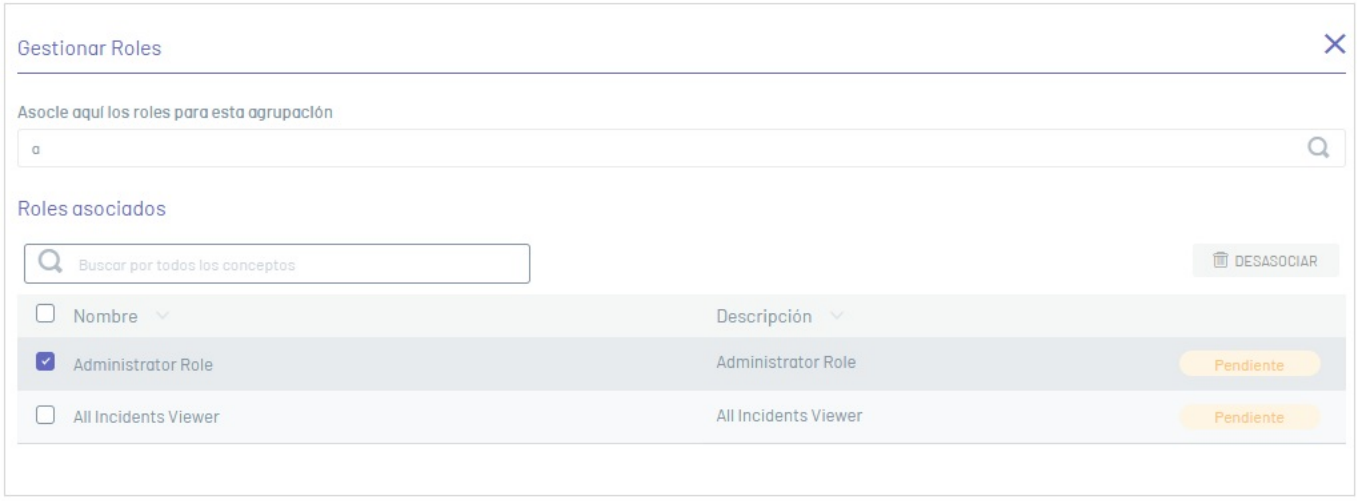
11. Se habilita la ventana Gestionar Roles, donde podrá consultar y agregar los roles requeridos para el grupo definido. En el campo de búsqueda ingrese el nombre del rol requerido y en la lista de resultados seleccione el rol a agregar.

> ⚐ Nota: Solo se listan los roles activos.

12. Al terminar haga clic en Asociar.

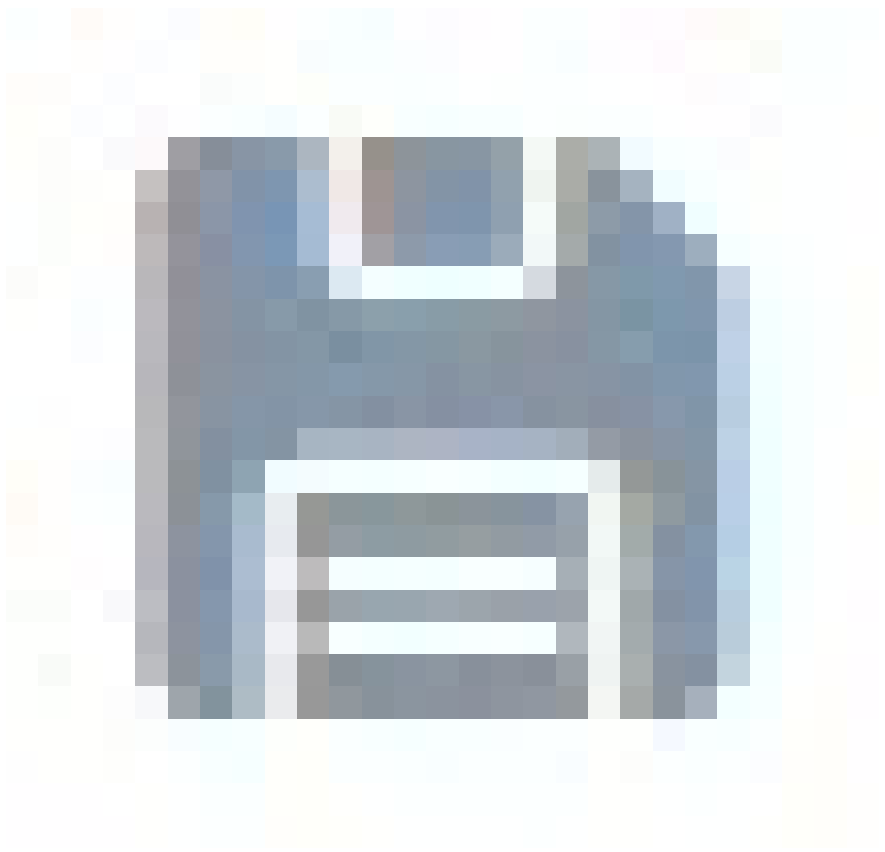


> ⚐ Nota: El estado del rol queda pendiente hasta que se guarden los cambios.



13. Para desasociar roles de un grupo, en la ventana Gestionar Roles seleccione uno o más registros del listado de roles y haga clic en el botón Desasociar. Confirme que desea desasociar los usuarios haciendo clic en el botón Aceptar.

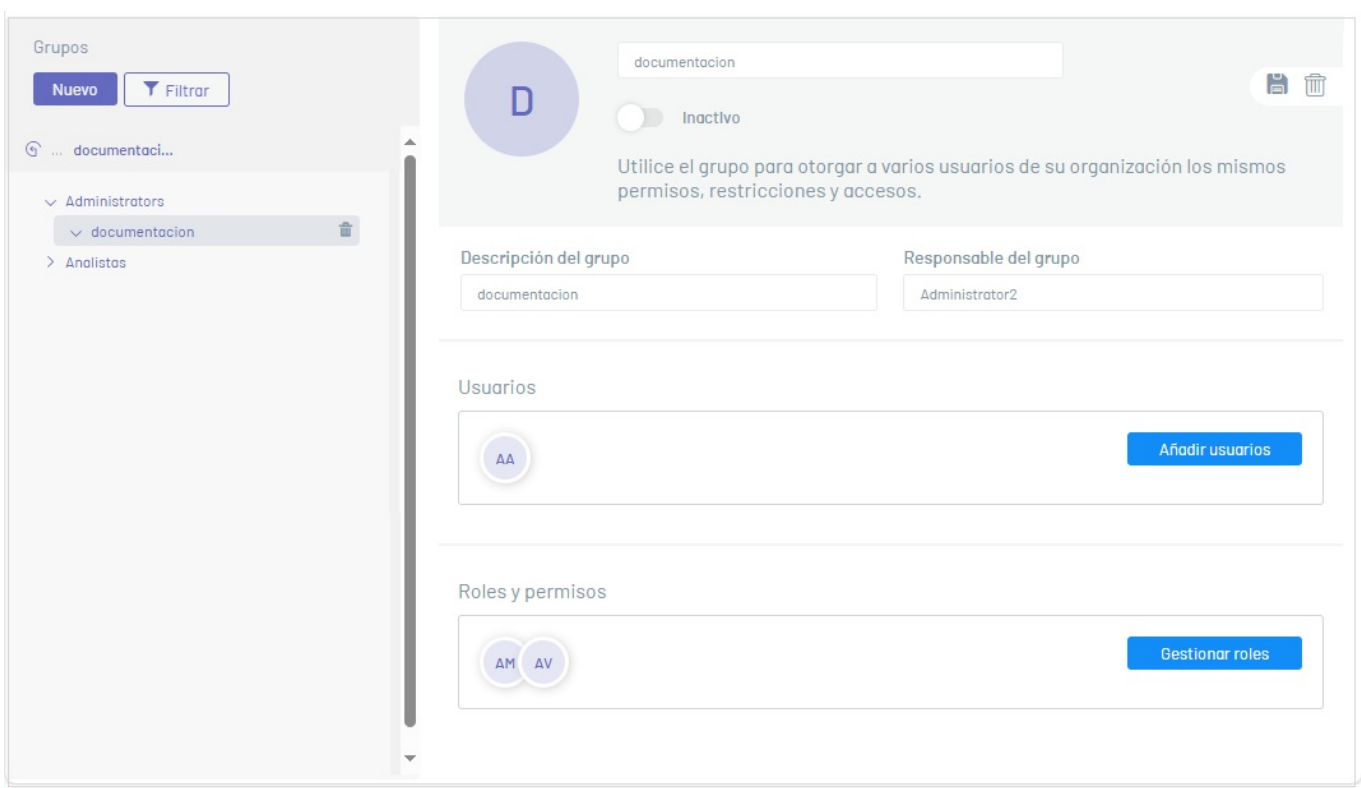
14. Al terminar de configurar el nuevo grupo, haga clic en el ícono Guardar



para confirmar los cambios realizados.

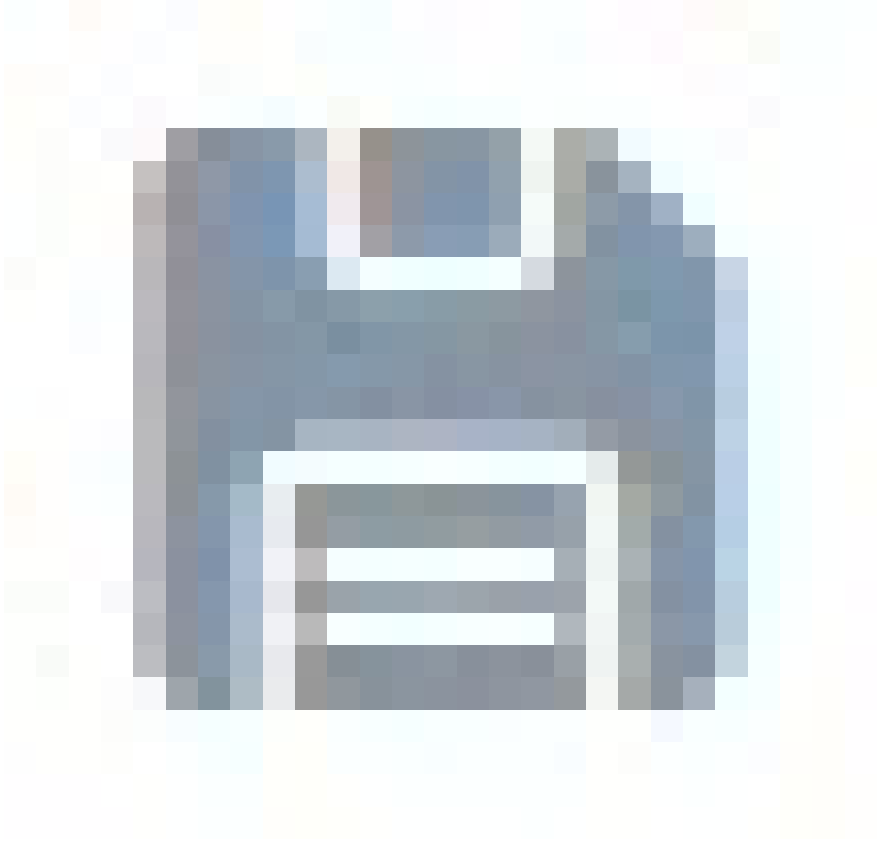
Editar de grupos

1. Para modificar un grupo o subgrupo, en la vista de información de grupos de usuario seleccione un registro del árbol de agrupación; podrá visualizar los detalles del grupo y modificar la información requerida.



⚐ Nota: Si el grupo es importado desde un Directorio Activo, sólo podrá modificar los roles y el estado de un grupo. No se podrán editar los usuarios

2. Al terminar de editar el grupo, haga clic en el ícono Guardar

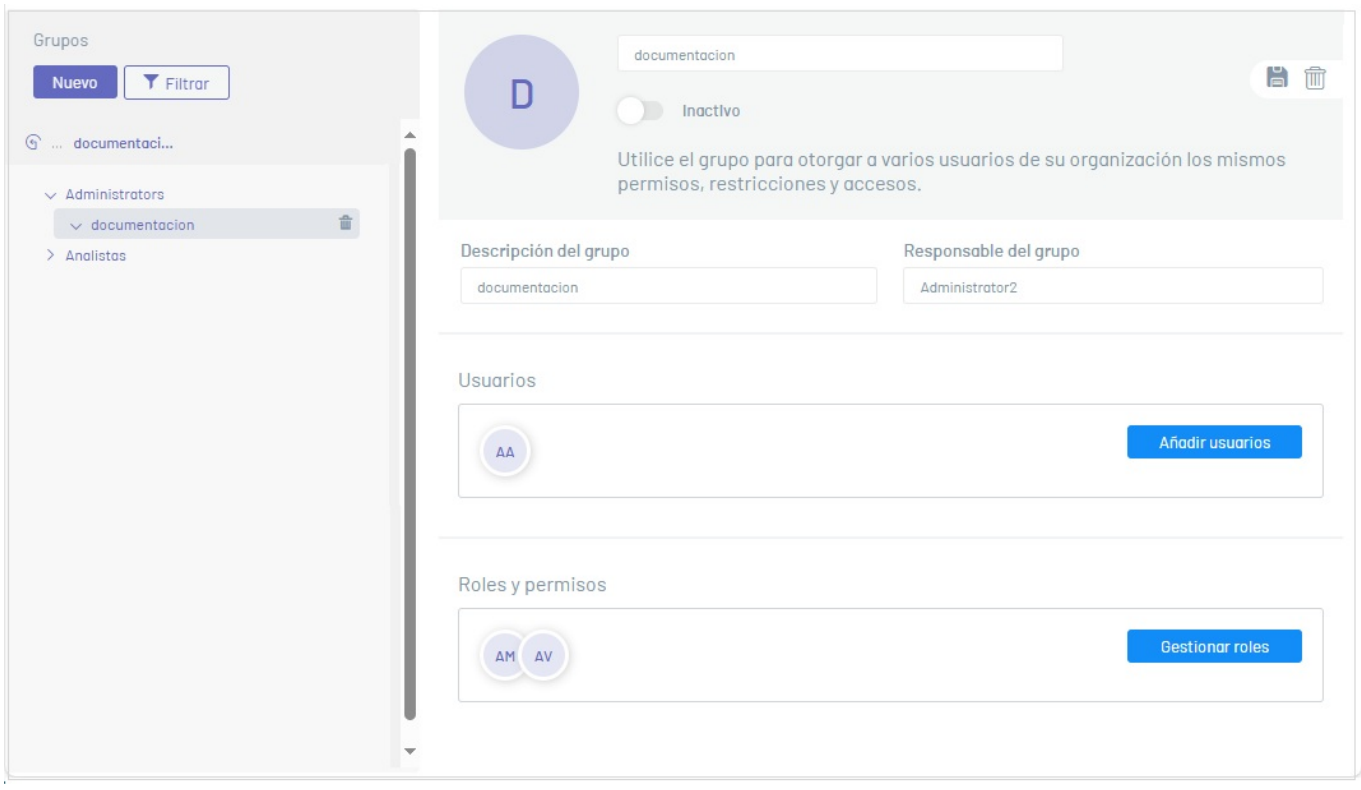


para confirmar los cambios realizados.

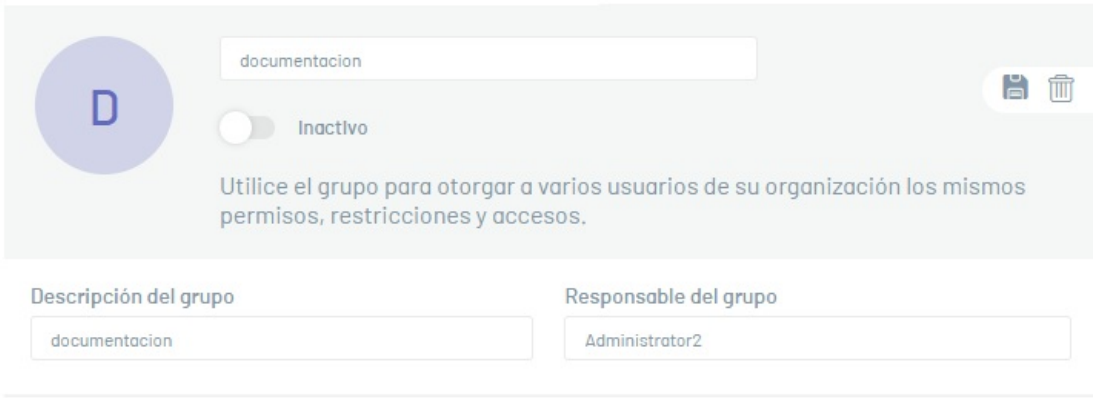
Eliminar de grupos

1. En la vista de información de grupos de usuario seleccione un registro del árbol de agrupación y haga clic en el ícono Eliminar

para borrar la información asociada.



2. De forma alternativa, en la vista detalle del grupo seleccionado, haga clic en el ícono Eliminar para borrar la información asociada.



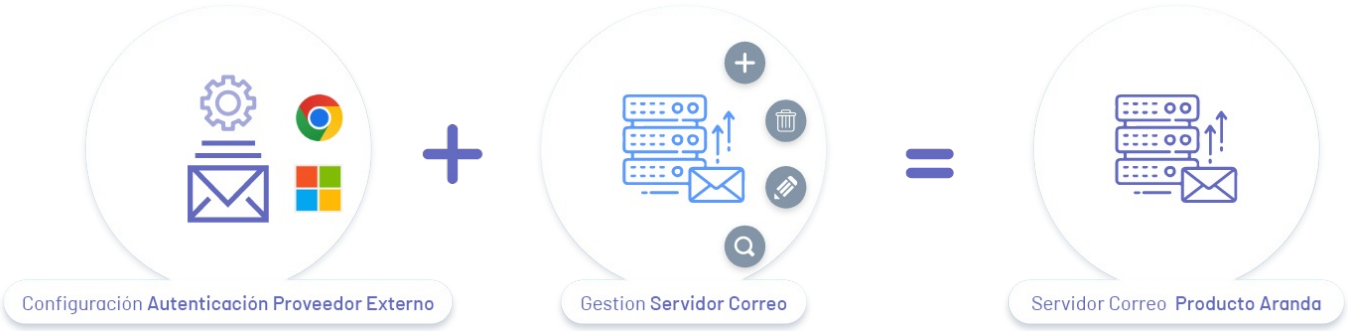
3. Podrá visualizar un mensaje de confirmación para validar la acción de borrado.

⚐ Nota:

- Al eliminar un grupo, si es un grupo padre, se eliminarán los subgrupos que pertenezcan a él.
- No se borran usuarios ni roles si se borra el grupo.
- Si solo se desea eliminar un subgrupo, se debe seleccionar el subgrupo a eliminar.
- Los grupos importados pueden ser eliminados. Sin embargo, existe la posibilidad de que el grupo sea importado de nuevo desde el directorio de servicios.

Módulo Servidor de Correo

Configuración Preliminar Servidor de Correo



1. Configuración Proveedores Externos de Servidor

Configure los proveedores externos (Microsoft Azure, Google) para los procesos de autenticación del servidor de correo.

Para mayor información consulte la Autenticación Moderna Oauth/Microsoft ↪.

Para mayor información consulte la Autenticación Moderna Oauth/Google ↪.

2. Gestión Módulo Servidor de Correo

En el módulo Servidor de correo podrá crear, actualizar y eliminar configuraciones de servidores de correo electrónico para las notificaciones que se enviarán a los usuarios desde la consola web.

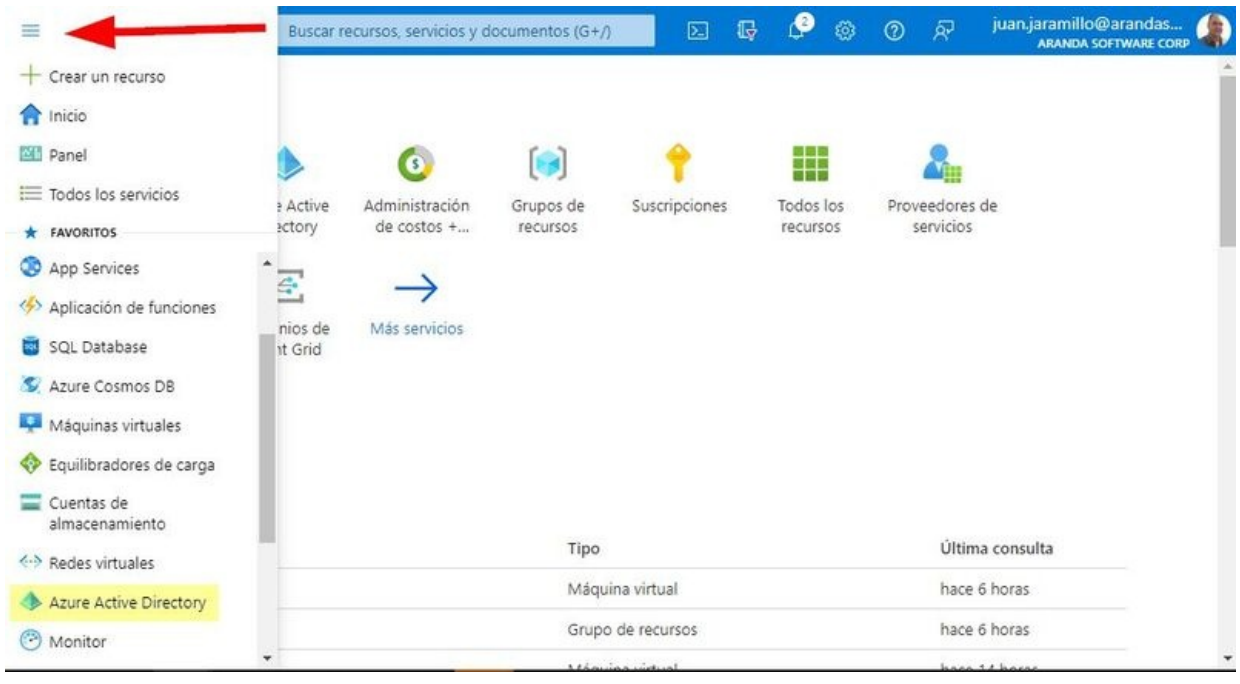
Para mayor información consulte la Gestión Servidor de Correo ↪.

Autenticación OAuth 2.0/Microsoft

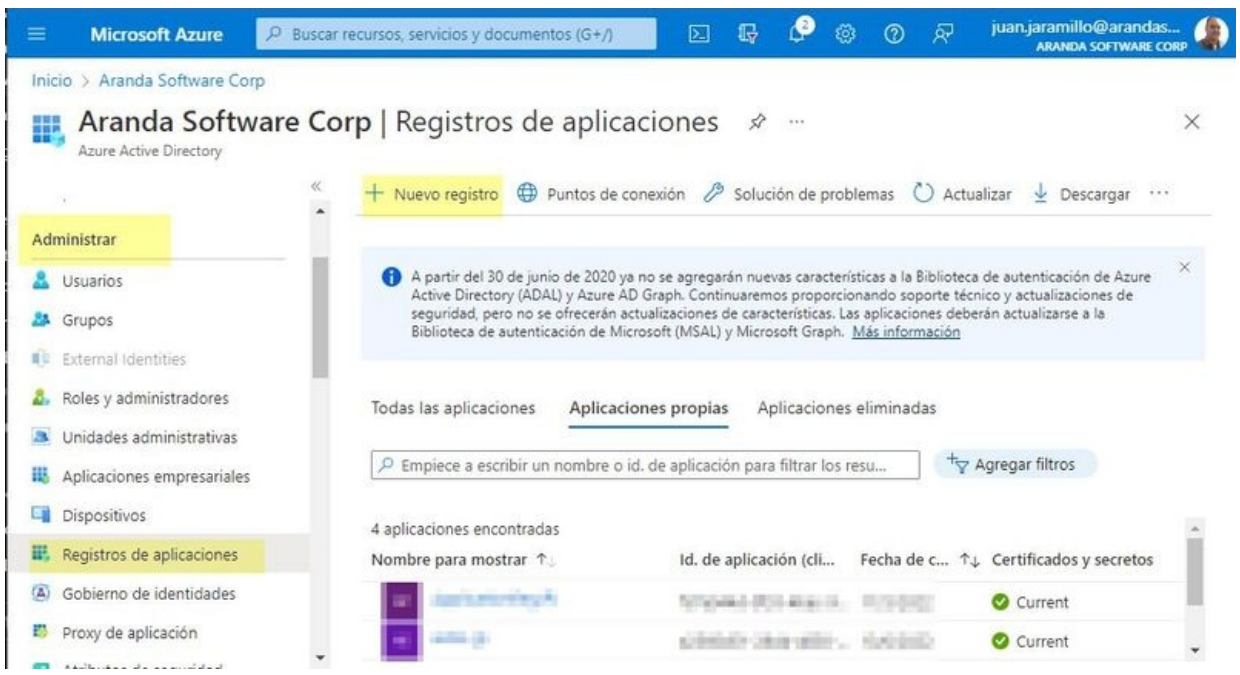
Creacion Aplicación en Azure

▶ Requisitos Autenticación Azure: ❯

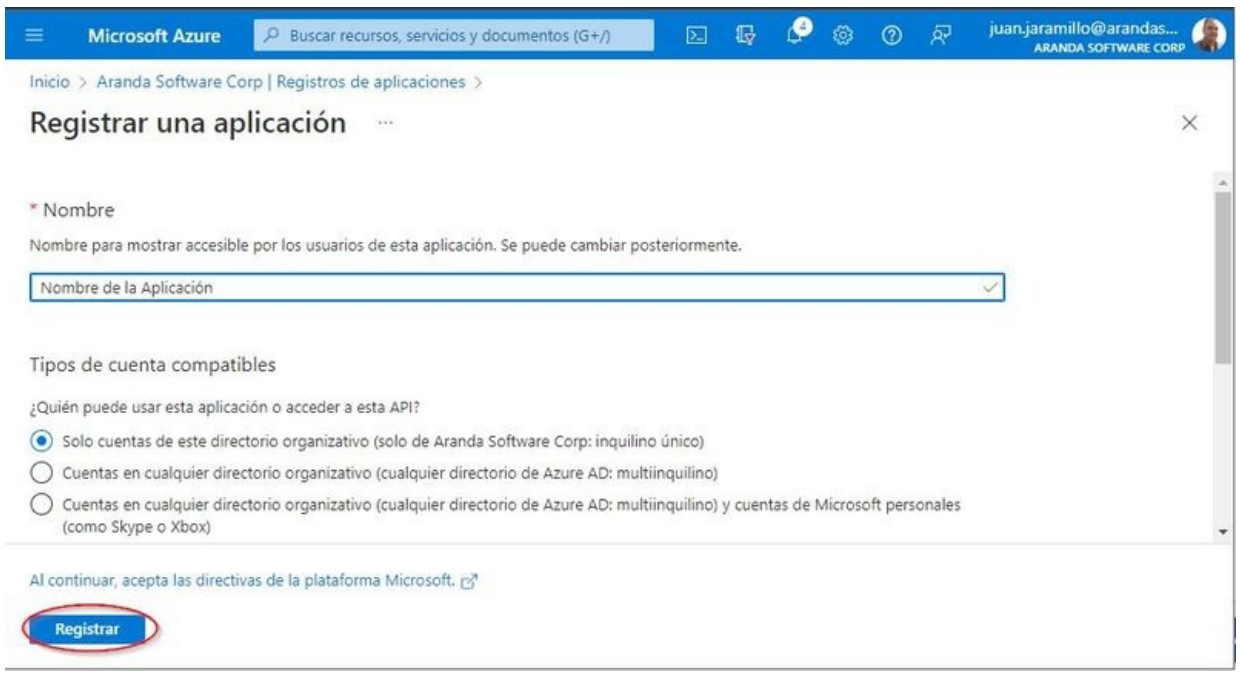
1. Se accede al portal de Azure Ver Microsoft Azure , busque y seleccione Azure Active Directory.



2. . En la sección Administrar busque y seleccione Registros de aplicaciones, haga clic en Nuevo registro.



3. Se diligencia el campo del nombre y se selecciona la opción deseada en (Tipos de cuentacompatibles), clic en Registrar.

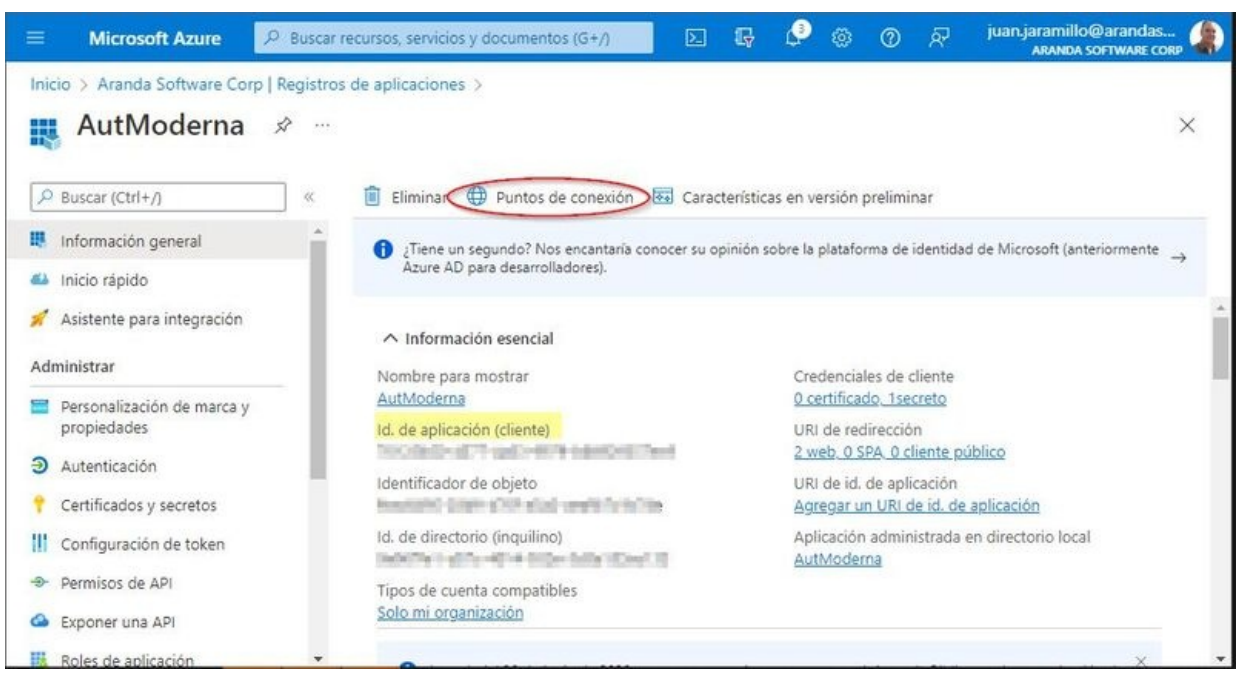


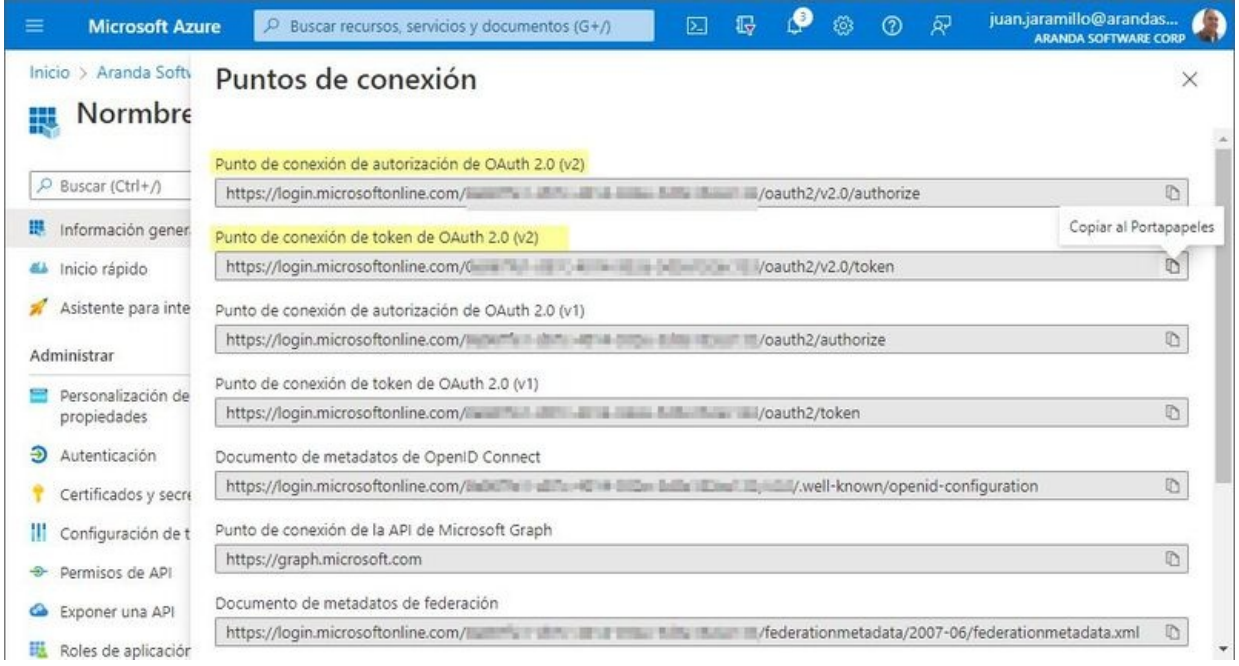
4.Cuando se tenga registrada la aplicación, guarde los siguientes datos que se requieren para la configuración en las aplicaciones de Aranda.

- Id. de aplicación (cliente) -> Identificador de cliente.

Clic en la opción (Puntos de conexión).

- Punto de conexión de autorización de OAuth 2.0 (v2) -> URL autorización.
- Punto de conexión de token de OAuth 2.0 (v2) -> URL del token.





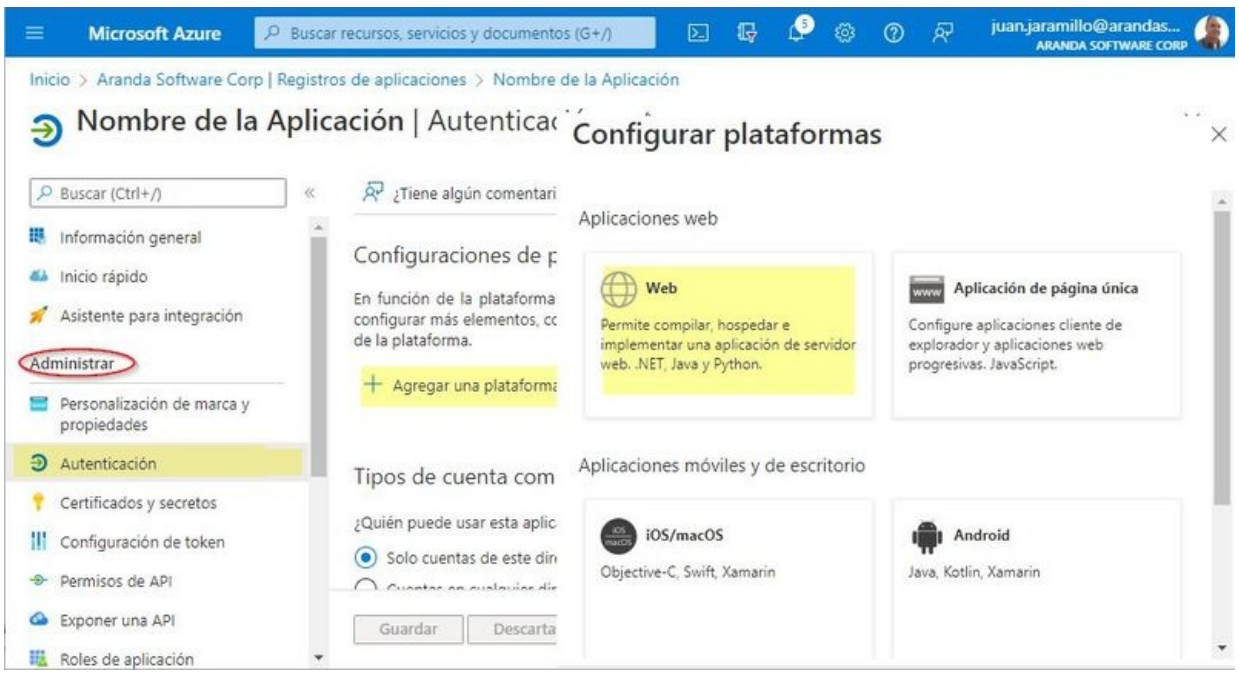
Configuración de la aplicación en el portal Azure

Cuando se tenga la aplicación creada y tenga los datos guardados, se procede a configurar la aplicación de la siguiente manera:

Cómo configurar la autenticación

1. Se ingresa al portal de Azure > Menú > Azure Active Directory > Registros de aplicaciones > seleccionar la aplicación creada del listado que aparece en la vista.

2. En la sección Administrar busque y seleccione Autenticación > luego en Agregar una plataforma, seleccione la opción Web.



3. Para el producto Aranda Service Management ASMS diligencie la URI de redirección de la siguiente manera:

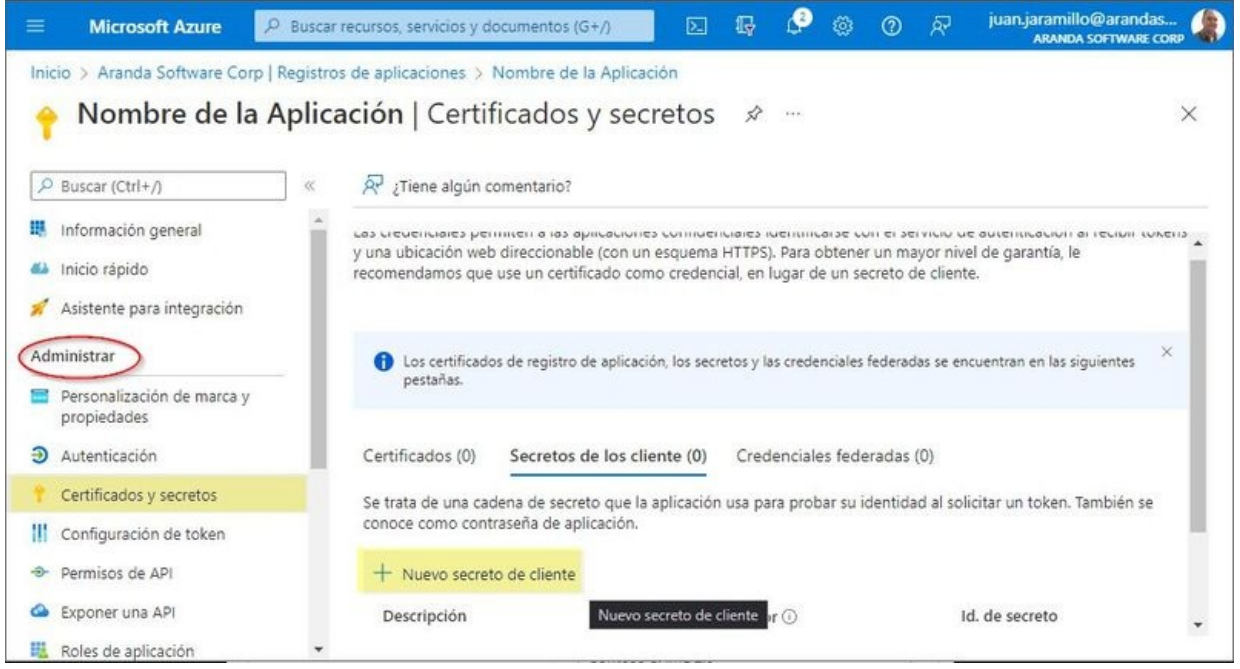
- Servidor de salida: https://[dominio]/[SitioAdministracion]/Main/Pages/OauthToken.aspx
- Servidor de entrada (Case creator): (http://localhost) y realice el proceso manual de generacion del token (Postman).
- Reemplace el [dominio] según corresponda, y luego seleccione Configurar.
- Reemplace [SitioAdministracion] con el nombre del directorio o aplicación del sitio deadministración.
- Nota: Este nombre reconoce entre letras mayúsculas y minúsculas y se debe escribir como está configurado.

4. Para los demás productos Aranda, la Url de redirección es: (https://localhost/smtp) y debe realizar el proceso manual de generacion del token (Postman).

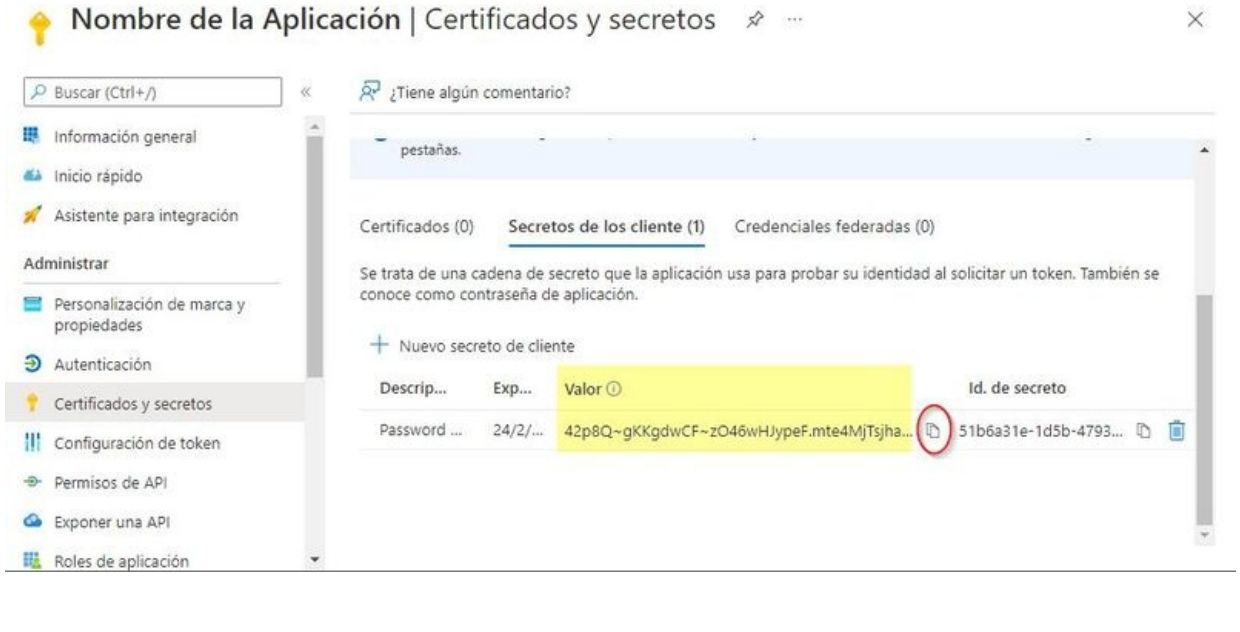
Creación del Secreto

1. Para crear el secreto se ingresa al portal de Azure > Menú > Azure Active Directory > Registros de aplicaciones > seleccionar la aplicación creada del listado que aparece en la vista.

2. En la sección Administrar busque y seleccione Certificados y secretos > luego clic en Nuevo secreto de cliente.



3. En la vista Agregar un secreto de cliente diligencie el campo Descripción, configurare el campo Expira que corresponde a la duración del secreto. Luego selecciona Agregar (Es importante siempre tener presente esta duración dado que, a su vencimiento, si no se actualiza, fallará la autenticación).



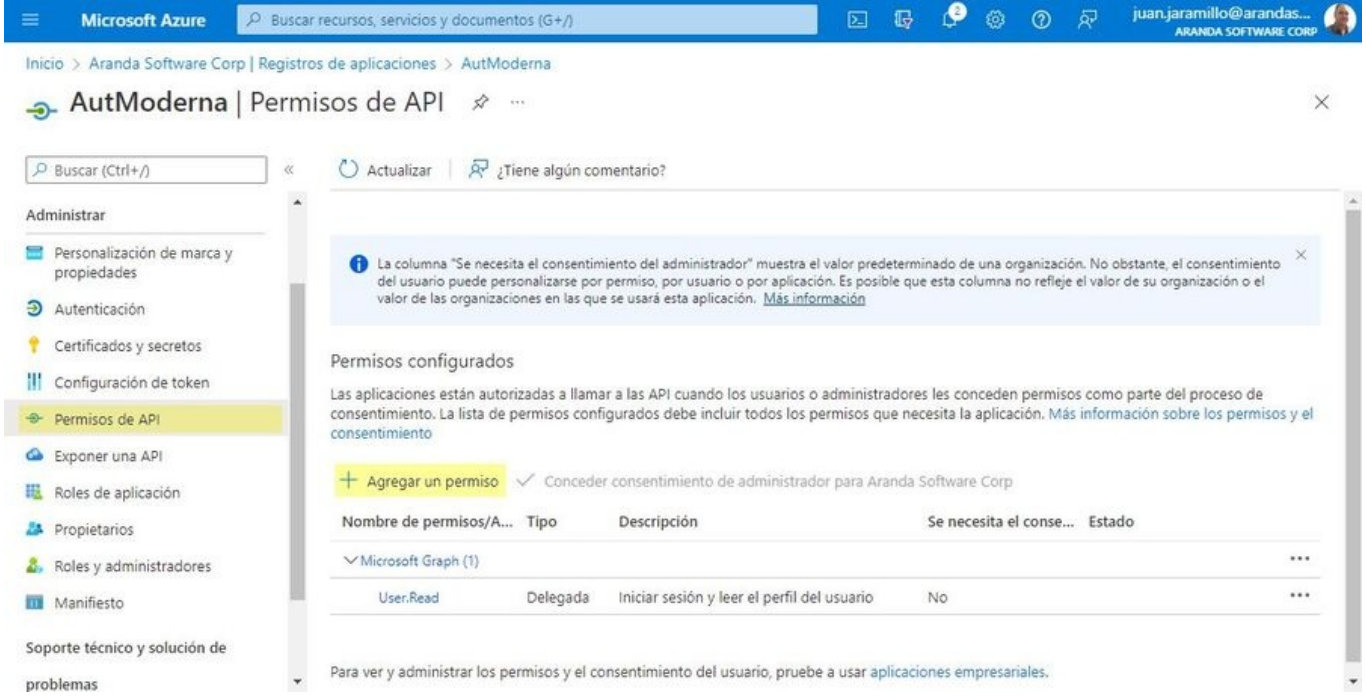
4. El valor del secreto solo es visible cuando se crea, por lo que se debe guardar para usarlo más adelante y conservarlo para las configuraciones que se requieran en los productos de Aranda.

- Valor secreto de cliente -> Secreto cliente.

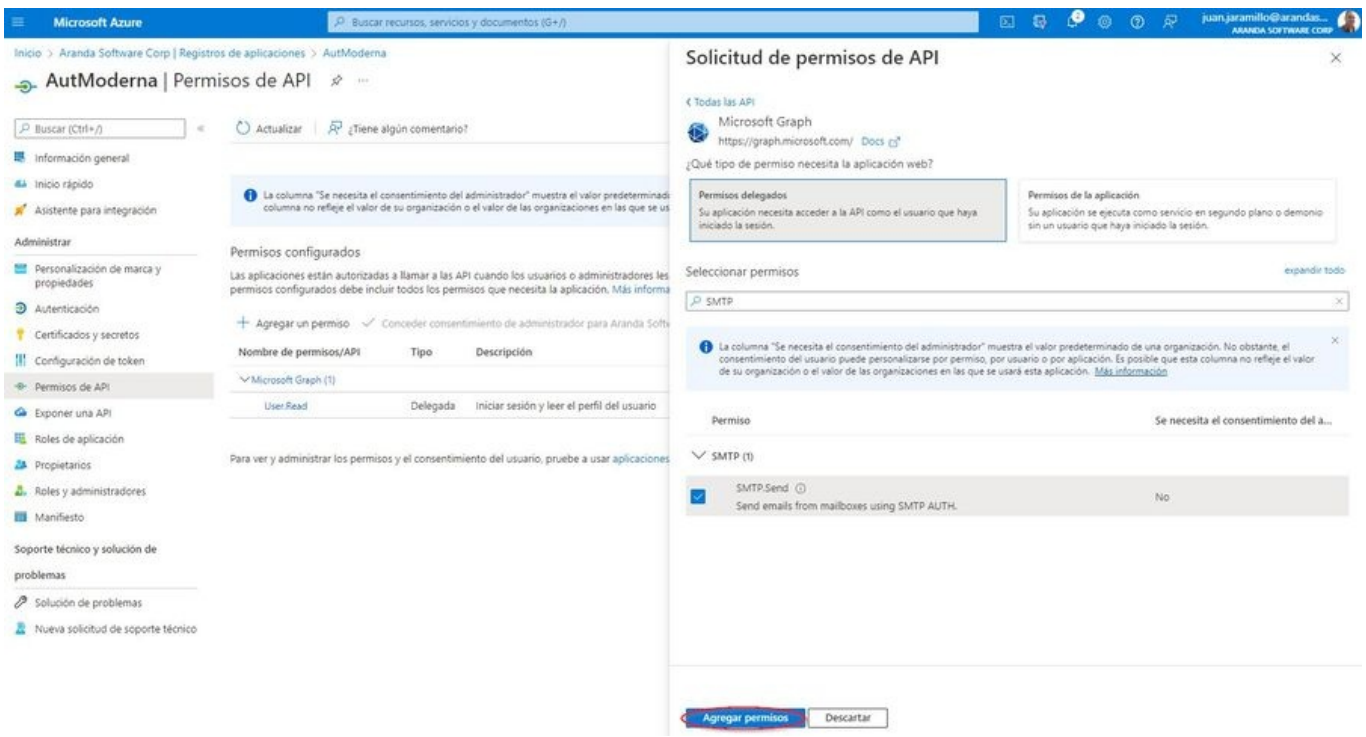
Configurar permisos de API

1. Para configurar los permisos de API se ingresa al portal de Azure > Menú > Azure Active Directory > Registros de aplicaciones > seleccionar la aplicación creada del listado que aparece en la vista.

2. En la sección Administrar busque y seleccione Permisos de API >luego clic en Agregar un permiso.



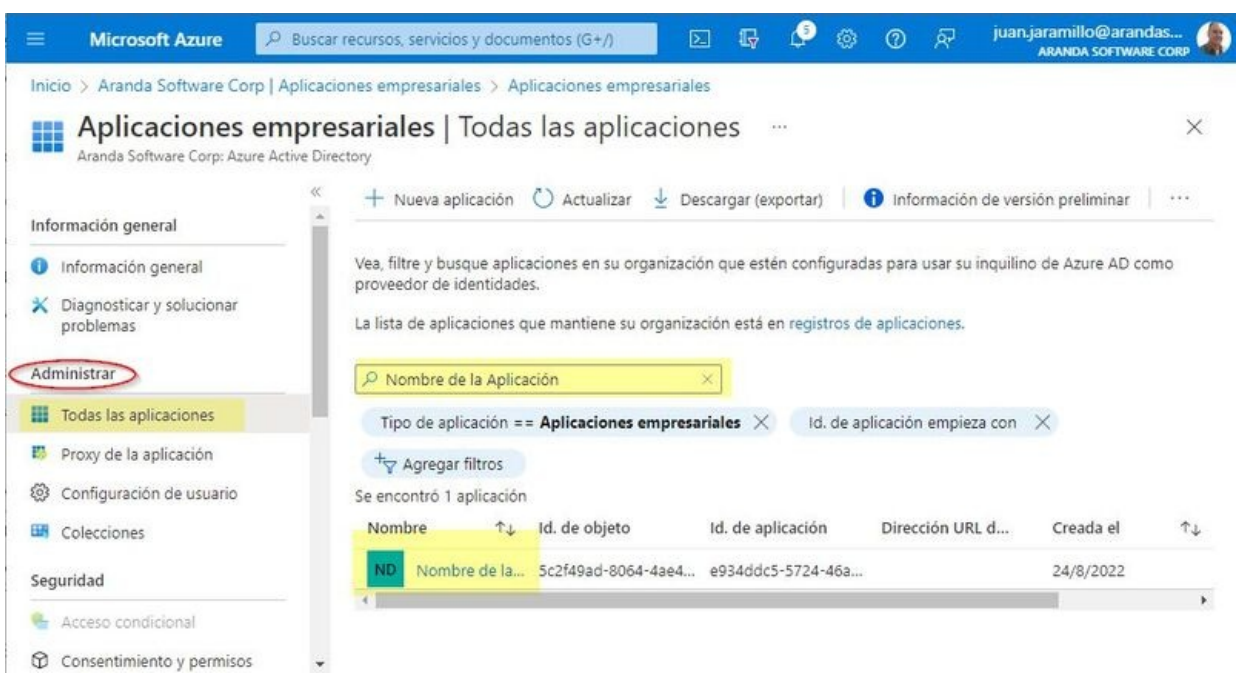
3. En la vista Solicitud de permisos de API, seleccionar Microsoft Graph > luego Permisos delegados, Seleccione los permisos de acuerdo a sus requerimientos: SMTP.Send (Envío de correos), IMAP y POP (Lectura de correos). Clic en Agregar permiso.



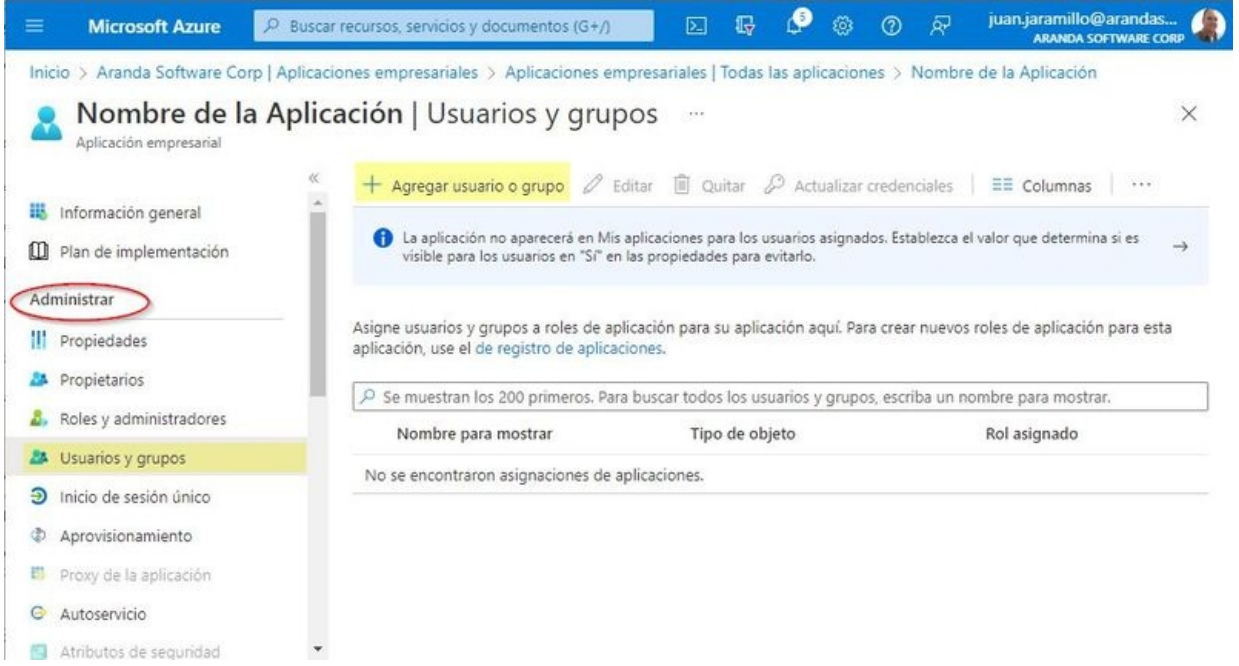
Configuración de usuarios y grupos

En está configuración se asocian el o las cuentas de correo que podrán acceder a la aplicación.

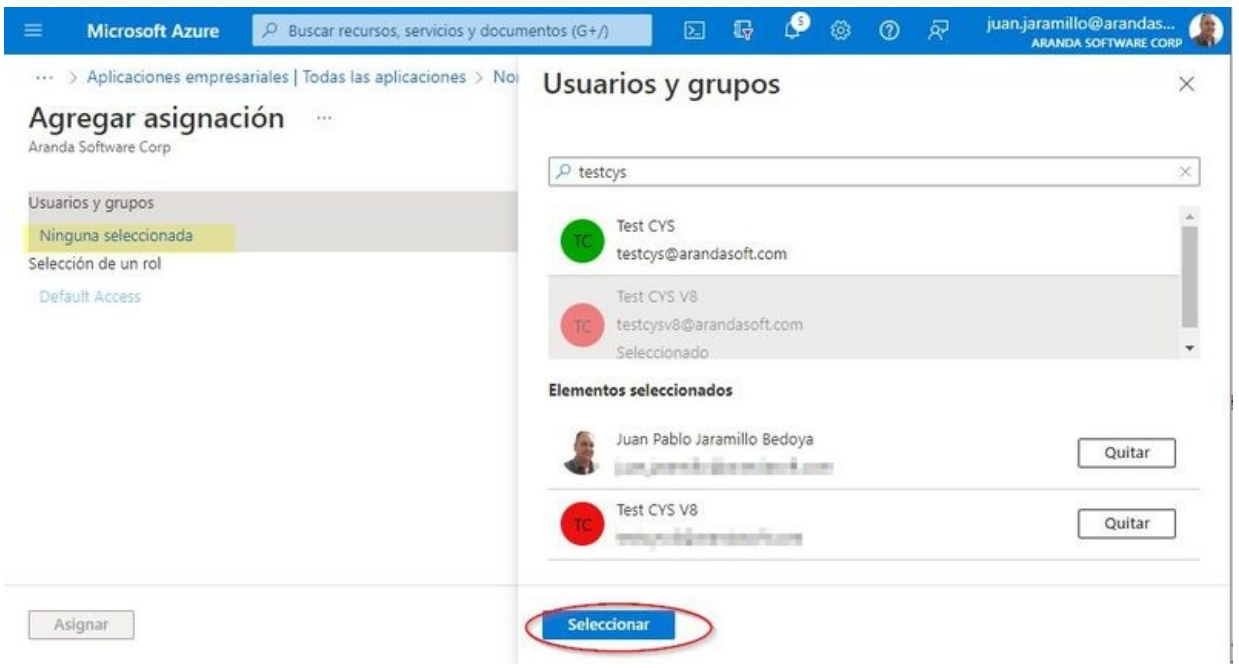
1. Se ingresa al portal de Azure> Menú> Azure Active Directory> Aplicaciones empresariales> seleccionar la aplicación creada del listado que aparece en la vista.



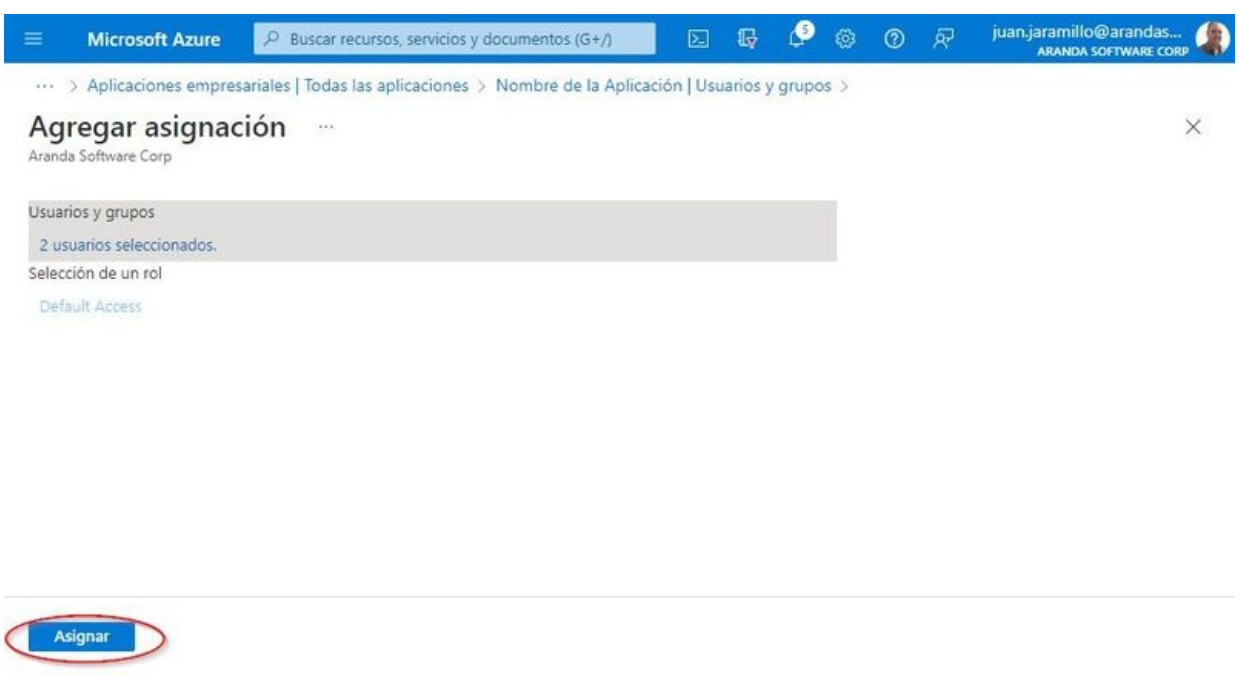
2. En la sección Administrar busque y seleccione Usuarios y grupos> y luego Agregar usuario o grupo.



3. En la vista Agregar asignación seleccione Ninguna Seleccionada> luego busca el o las cuentas de correo que desea agregar, cuando ya se tengan todos los correos seleccionados dar clic en Seleccionar.



4. Finalmente seleccione Asignar.



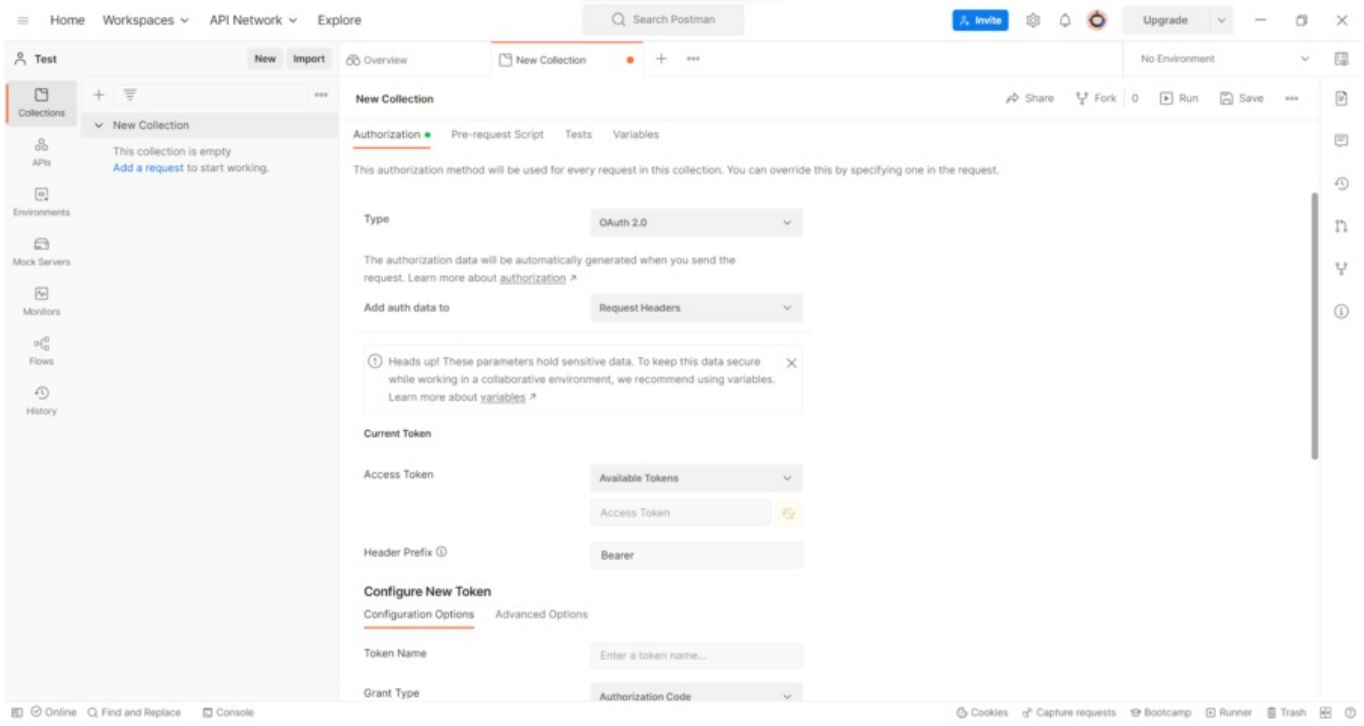
Creación Token Manual

En el proceso de configuración de servidor de correo para la autenticación OAuth, en las diferentes aplicaciones Aranda se obtiene el token de autorización de forma automática. Sin embargo también estará disponible la generación manual del token para temas de autenticación.

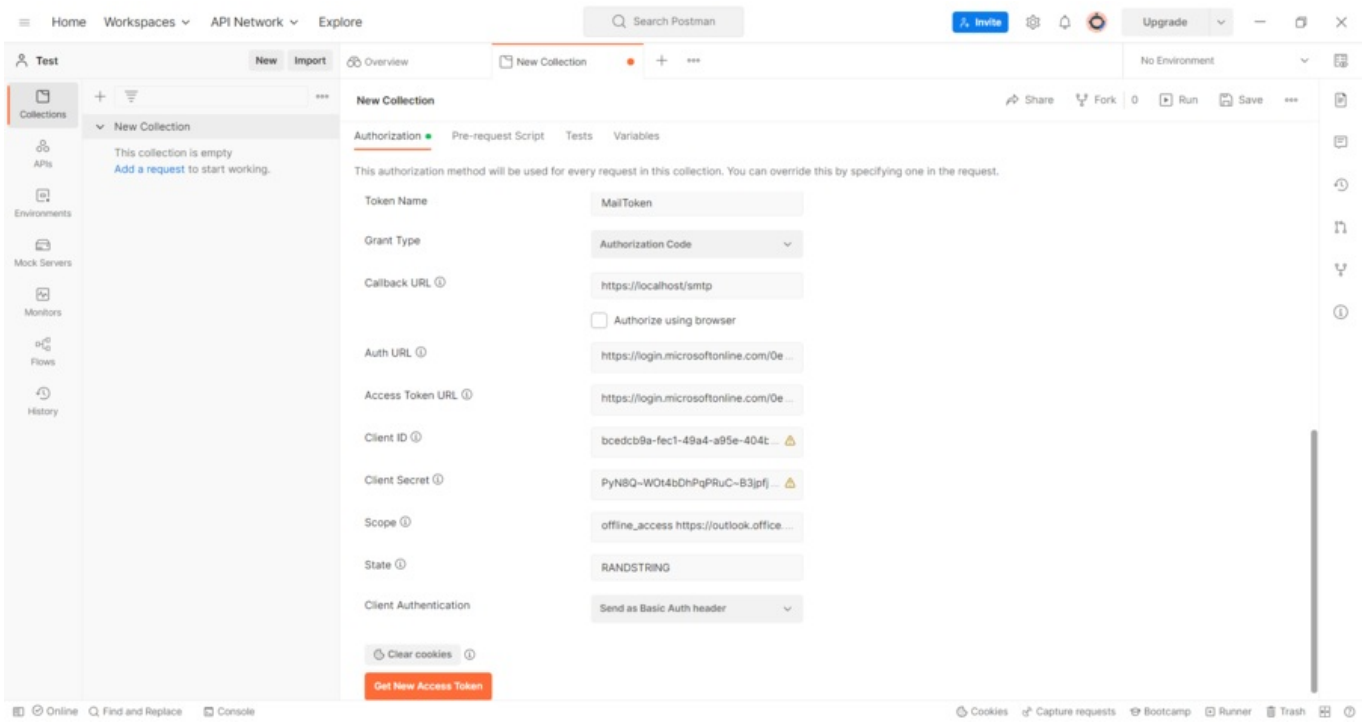
Configuración Token manual

1. Para generar el token manual debe ingresar a la aplicación Postman.

2. En el menú principal después de generar una coleccción, seleccione la pestaña Autorización y en el campo Tipo de autorización, seleccione en el menú desplegable la opción OAuth 2.0

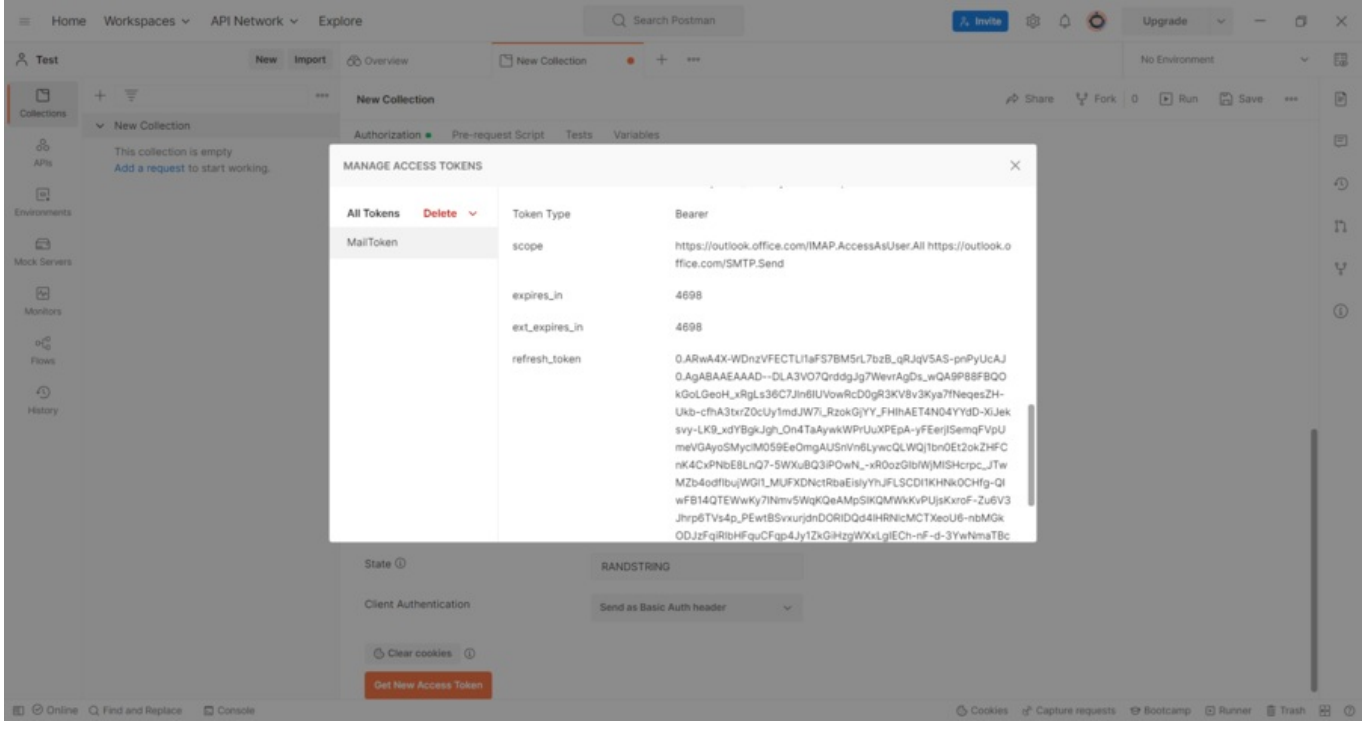


3. En la sección Configurar Nuevo Token, haga clic en el botón Nuevo Token; se habilita el formulario para registrar los siguientes campos:



Campo	Descripción
Grant Type	En esta opción debe seleccionar la opción Authorization code
Callback URL	Ingrese la dirección url que está llamando la aplicación: - Para el servidor de entrada (Case creator) Aranda Service Management: http://localhost - Para el servidor de salida de los demás productos de Aranda: https://localhost/smtp
Auth URL	Ingrese la url de autorización
Access Token URL	Ingrese la url la url del token
Client ID	Ingrese el identificadior del cliente
Client Secret	Ingrese el valor secreto del cliente
Scope	Ingrese la información requerida: - Para el servidor de entrada (Case creator) Aranda Service Management: offline_access https://outlook.office.com/SMTP.Send https://outlook.office.com/IMAP.AccessAsUser.All https://outlook.office.com/POP.AccessAsUser.All - Para el servidor de salida de los demás productos de Aranda: offline_access https://outlook.office.com/SMTP.Send
Client Authentication	En el menú despliegable utilice el valor por defecto (Send as Basic Auth header)

4. Seleccione el botón Get New Access Token, para generar el token (guarde el refresh_token para su configuración).



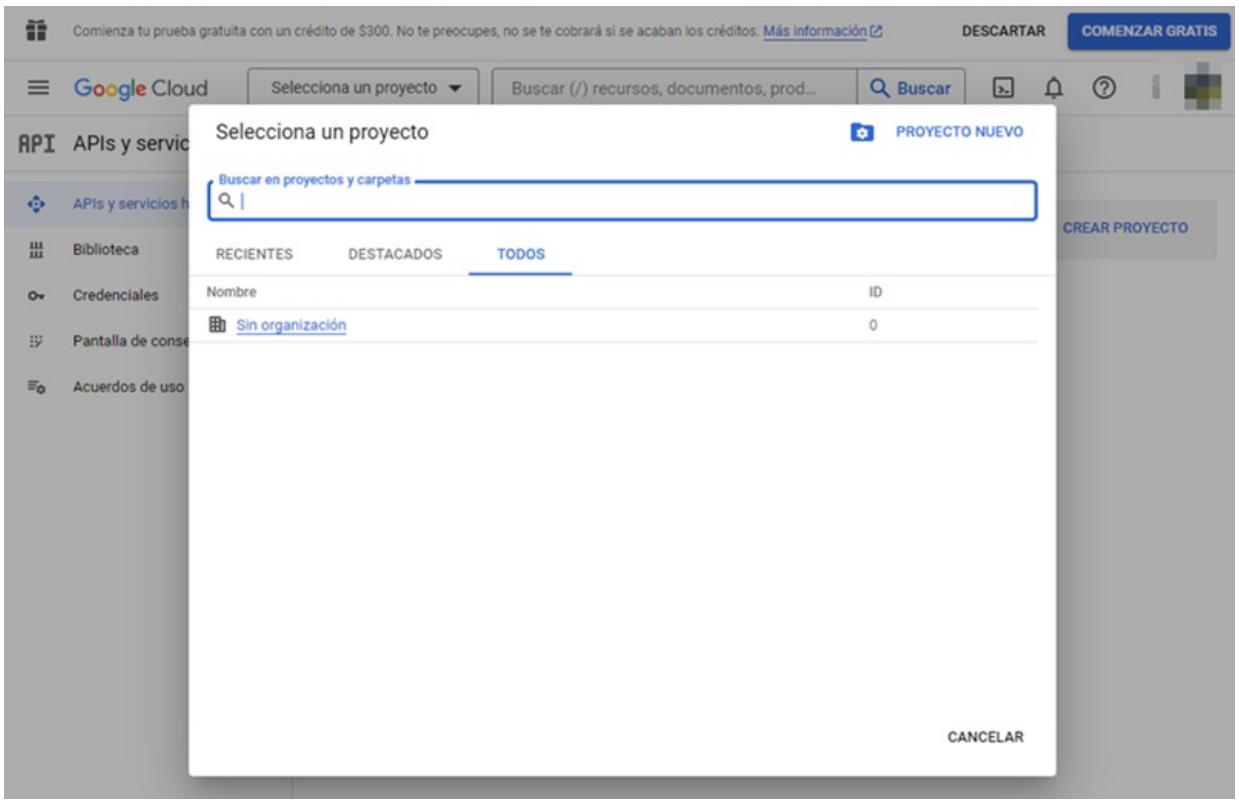
⚐ Nota:Después de realizar la configuración, el mailer enviará los correos respectivos de notificación.

Autenticación OAuth 2.0/Google

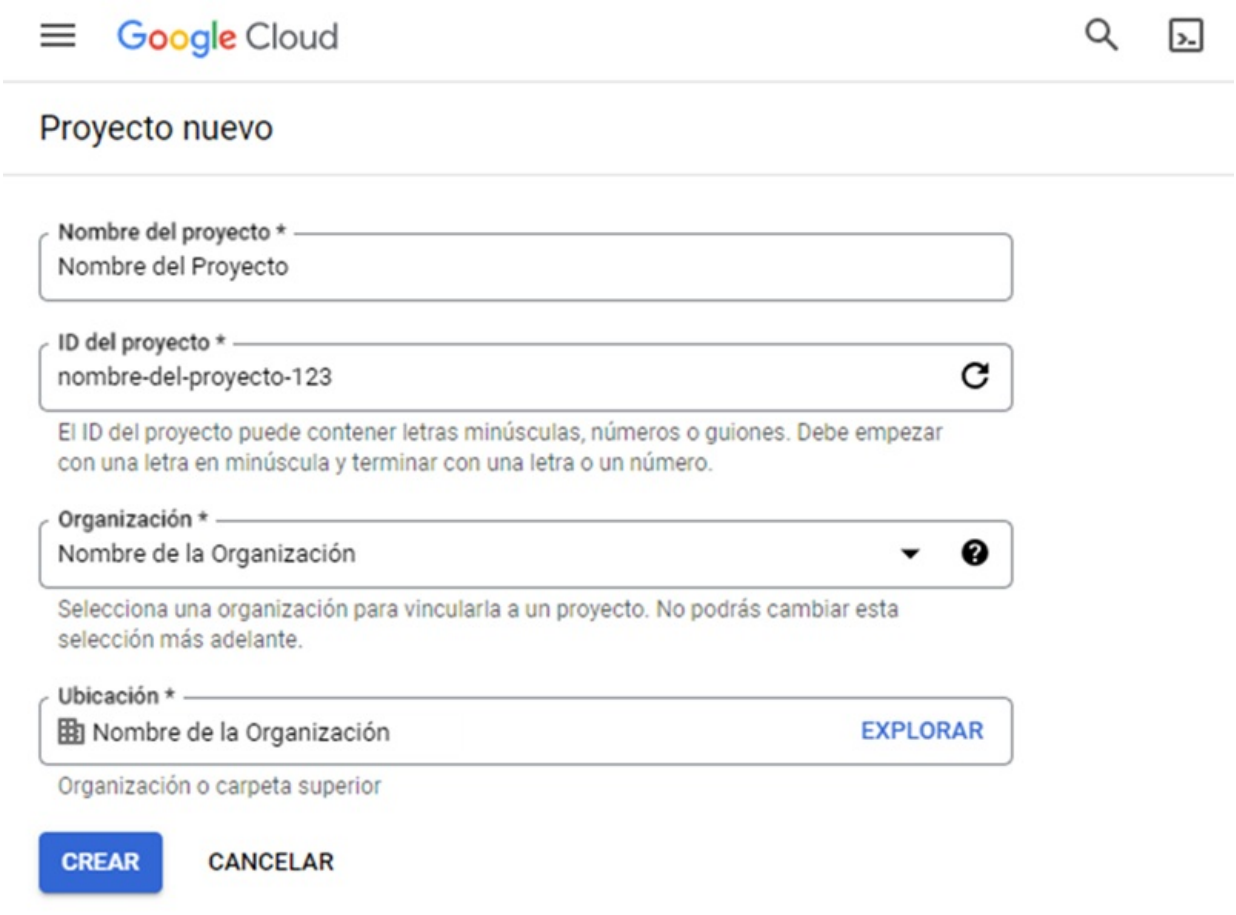
Creación de proyecto en Google

⚐ Nota: Si ya se cuenta con un proyecto configurado en Google, se puede omitir este paso.

1. Se accede a la consola de Google Cloud con la cuenta de Google destinada para este proceso, seleccione el menú desplegable Selecciona un proyecto en el menú de navegación superior. Luego, haga clic en el botón PROYECTO NUEVO.

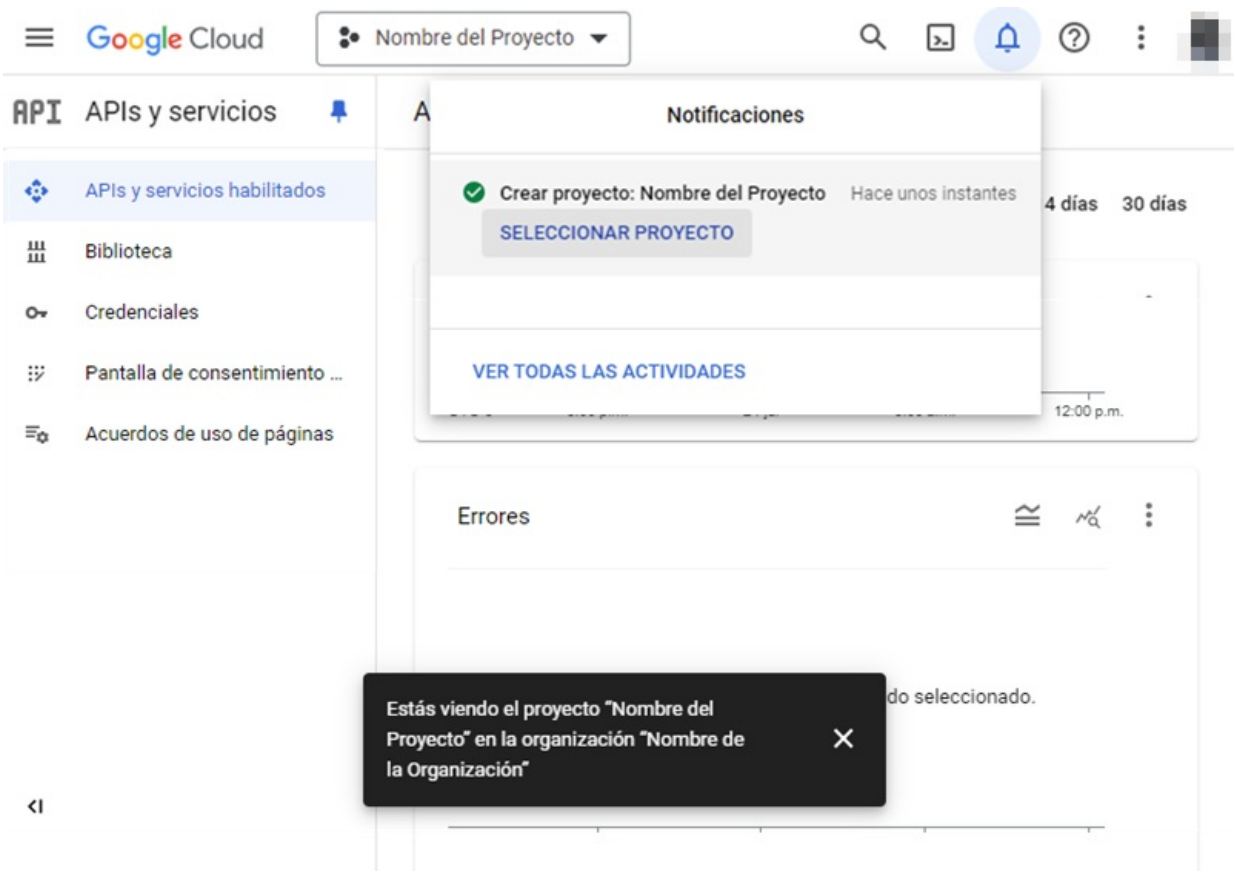


2. En la ventana Proyecto nuevo ingrese los cuatro campos solicitados siguiendo las recomendaciones y haga clic en el botón CREAR.



⚐ Nota: Si en el campo Organización solo se lista la opción Sin organización es que el usuario con el que se está creando el proyecto no cuenta con los permisos requeridos.

3. Se habilita la ventana Notificaciones. Haga clic en el botón SELECCIONAR PROYECTO para el proyecto creado:



4. En el menú desplegable Selecciona un proyecto podrá visualizar el nombre del proyecto creado.

Creación y configuración de aplicación en Google

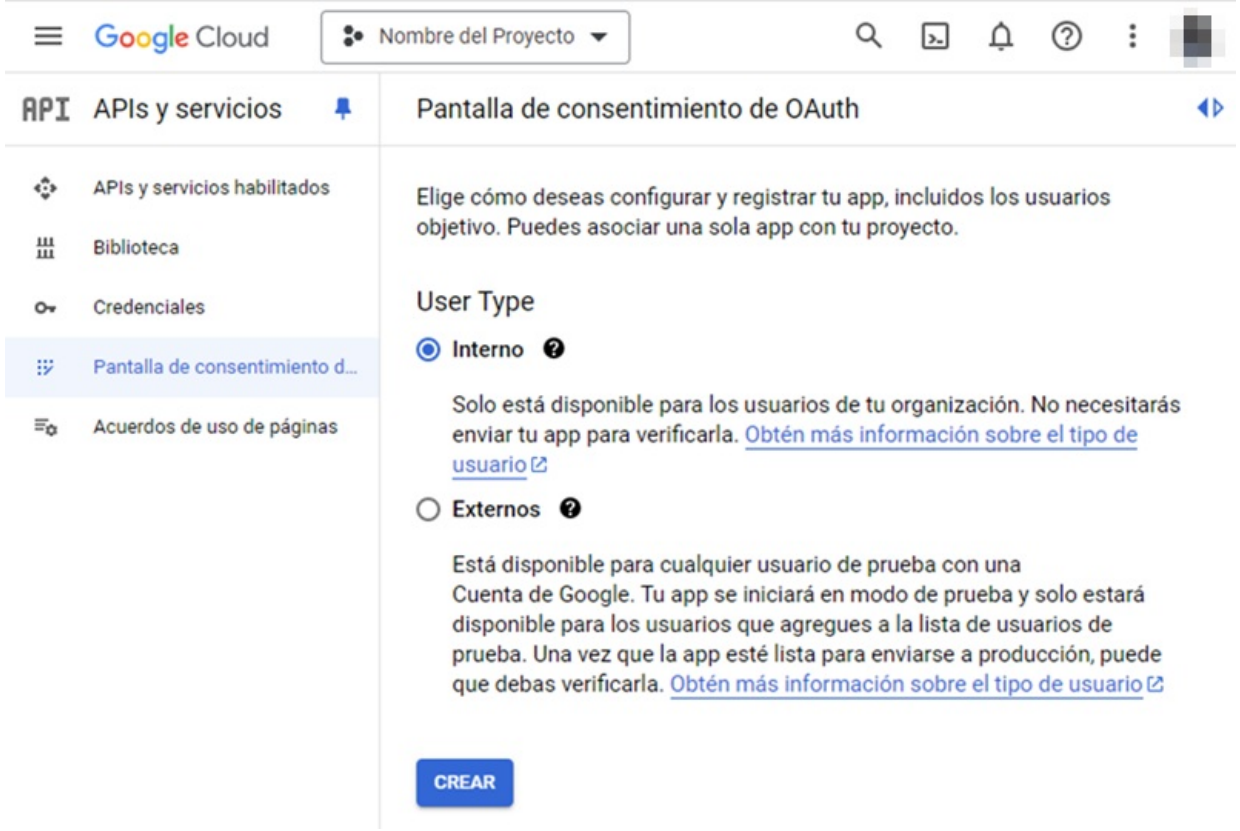
▶ Requisitos Autenticación GOOGLE: ❯

Cuando se tenga el proyecto creado y seleccionado, se procede con la creación de una aplicación OAuth la siguiente manera:

Cómo crear una aplicación en Google

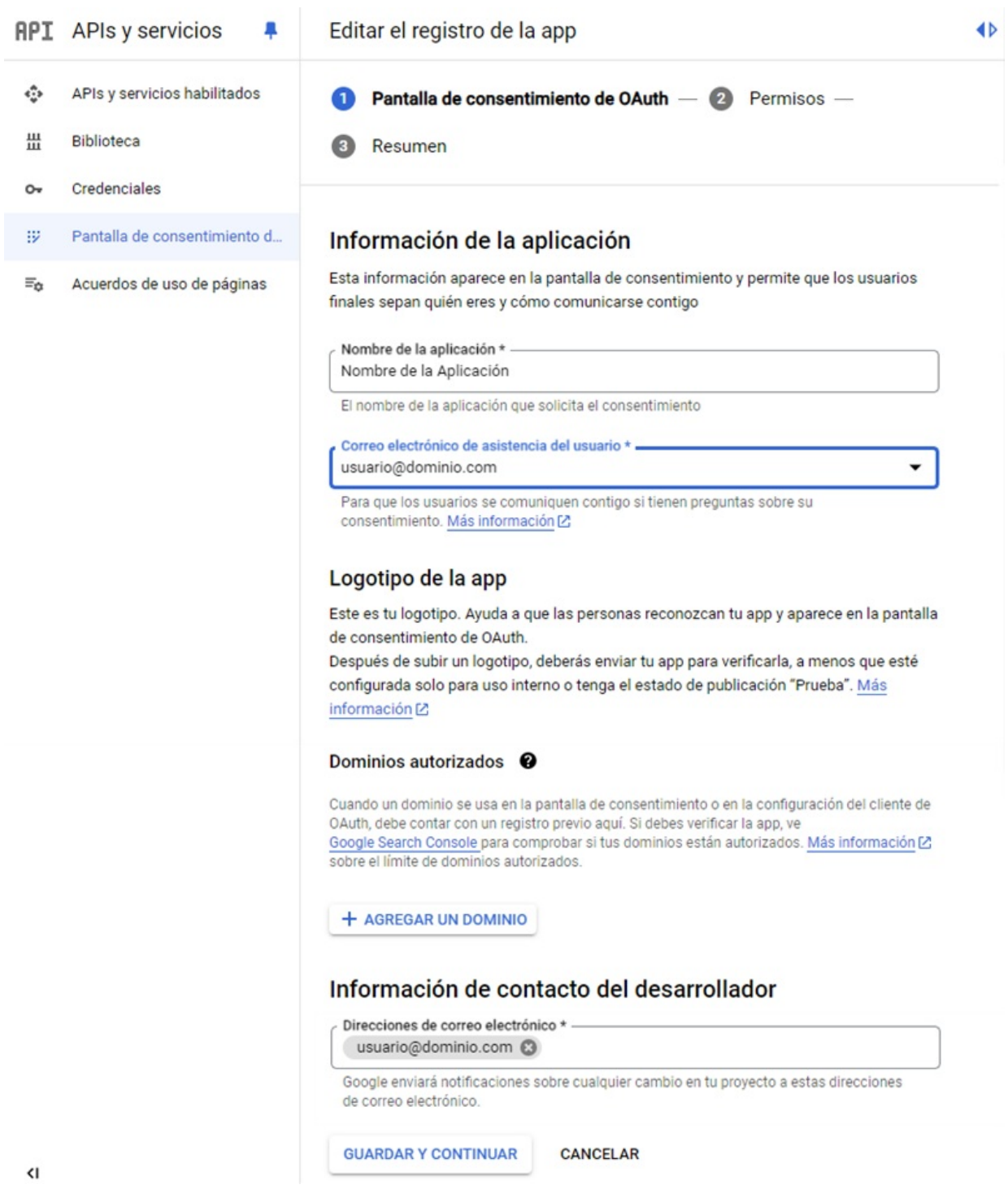
1. En la consola de Google Cloud en la sección APIs y servicios seleccione la opción Pantalla de consentimiento de OAuth y el tipo de usuario

- Seleccione Interno si está utilizando un inquilino administrador de GSuite y va a crear la aplicación exclusivamente para su organización.
- Seleccione Externo si está probando con una cuenta de Gmail independiente.

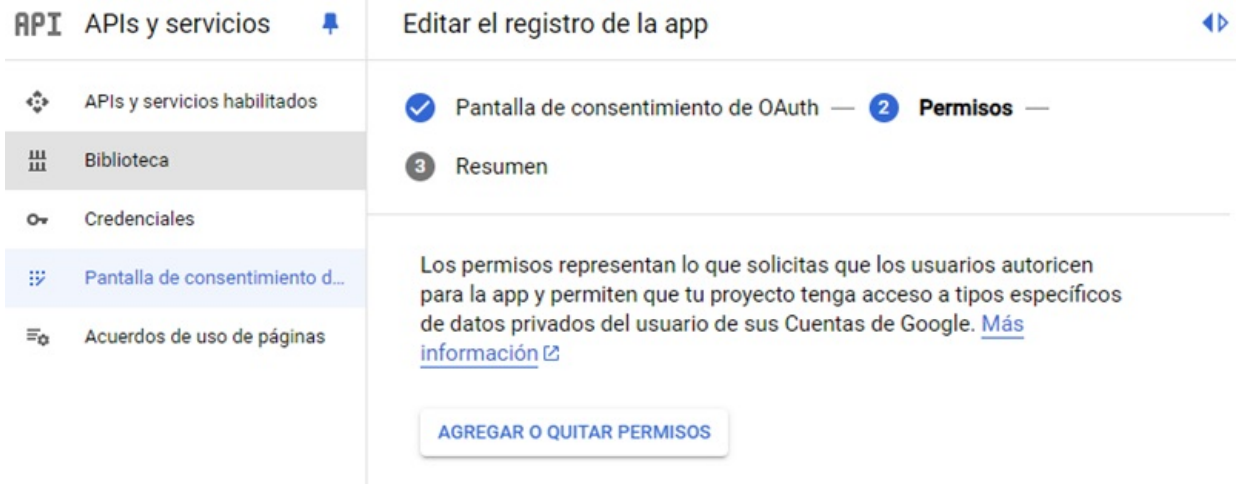


2. Haga clic en el botón CREAR.

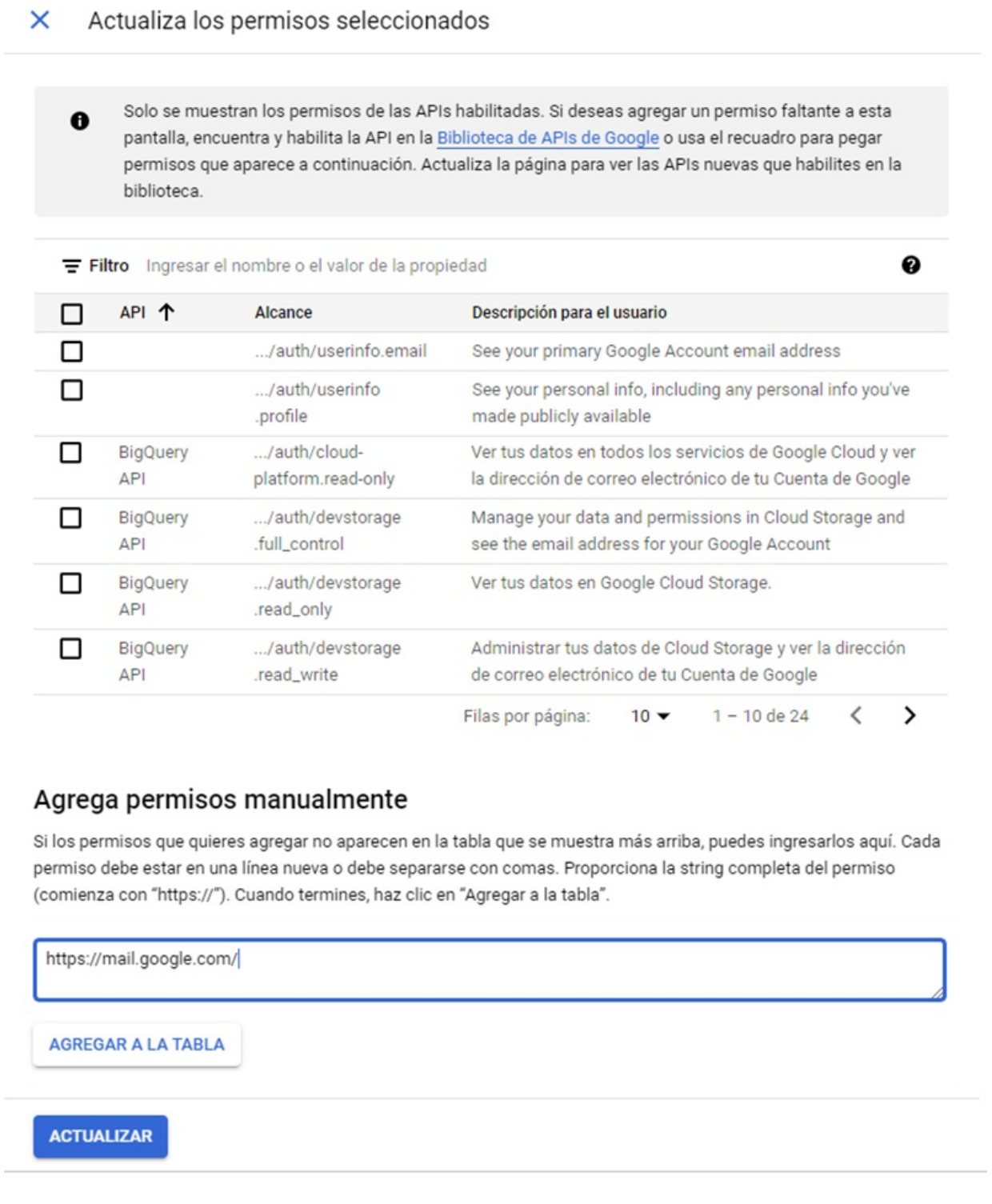
3. En la ventana Pantalla de consentimiento de OAuth ingrese los campo Nombre de la aplicación, Correo electrónico de asistencia del usuario en la sección Información de la aplicación y Direcciones de correo electrónico en la sección Información de contacto del desarrollador según las recomendaciones de cada campo (los demás campos son opcionales). Luego, haga clic en el botón GUARDAR Y CONTINUAR.



4. En la ventana Permisos haga clic en el botón AGREGAR O QUITAR PERMISOS.

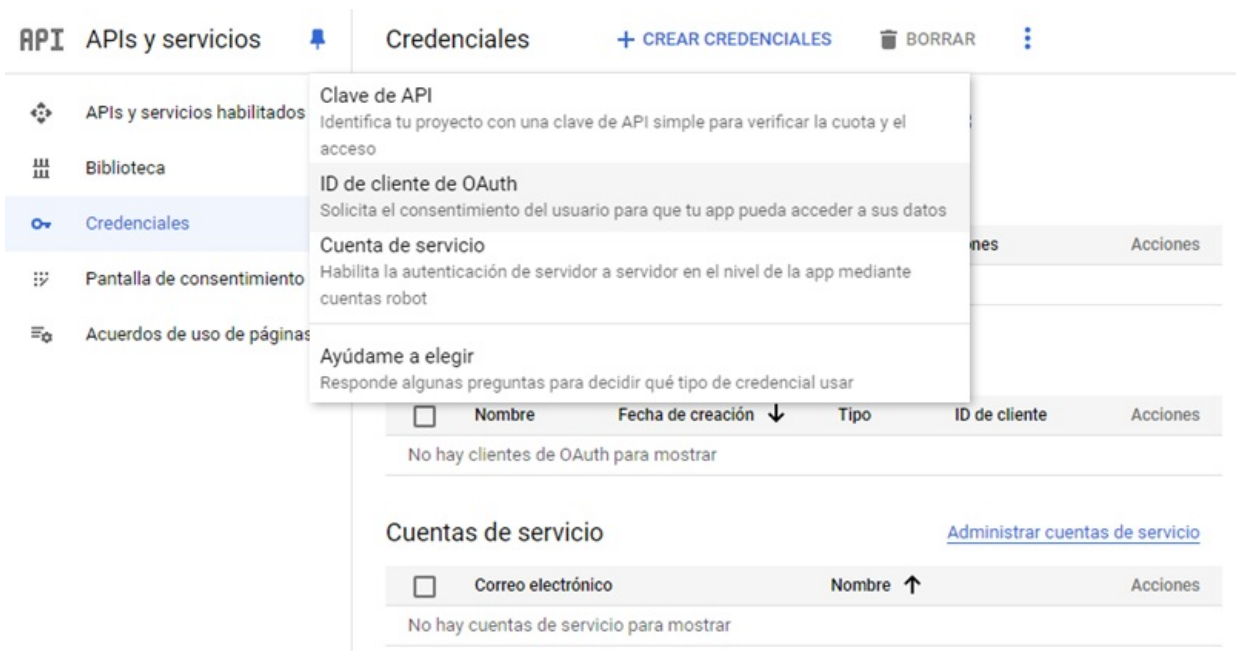


5. En la ventana Actualiza los permisos seleccionados en la sección Agrega permisos manualmente ingresa el valor https://mail.google.com/ y haga clic en el botón AGREGAR A LA TABLA. Luego en ACTUALIZAR.

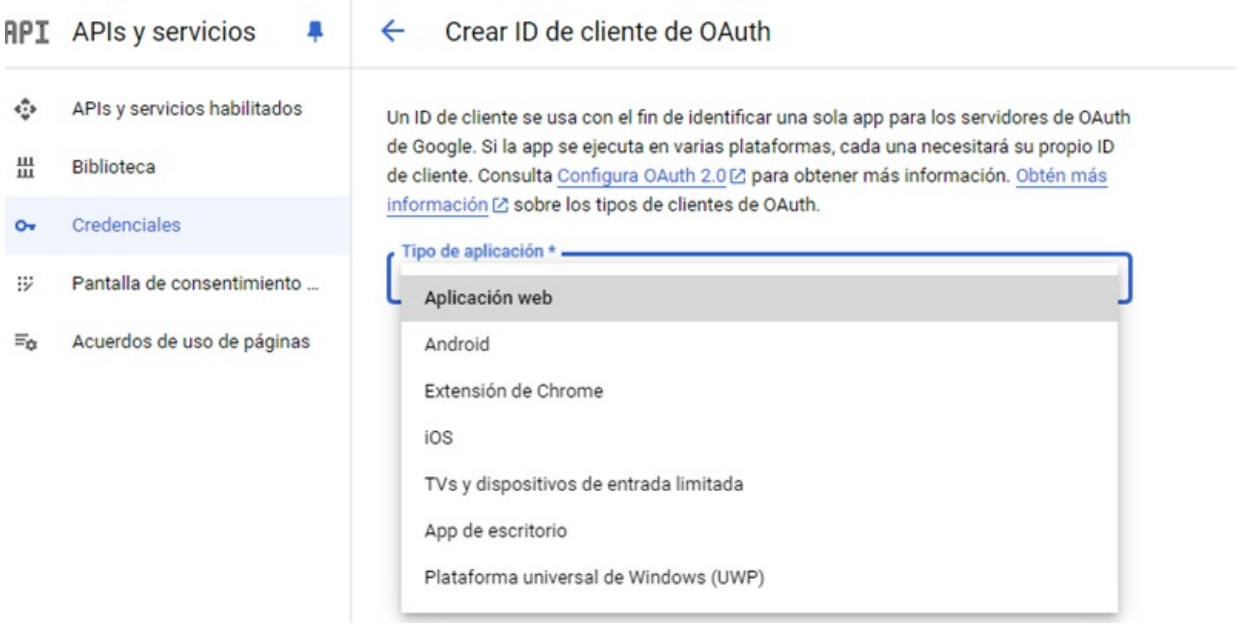


6. En la ventana Permisos verifique que el permiso se haya agregado en la sección Tus permisos restringidos y haga clic en el botón GUARDAR Y CONTINUAR para avanzar a la ventana Resumen donde podrá visualizar los datos de la nueva aplicación.

7. Seleccione la opción Credenciales, haga clic en el botón CREAR CREDENCIALES y seleccione la opción ID de cliente de OAuth.



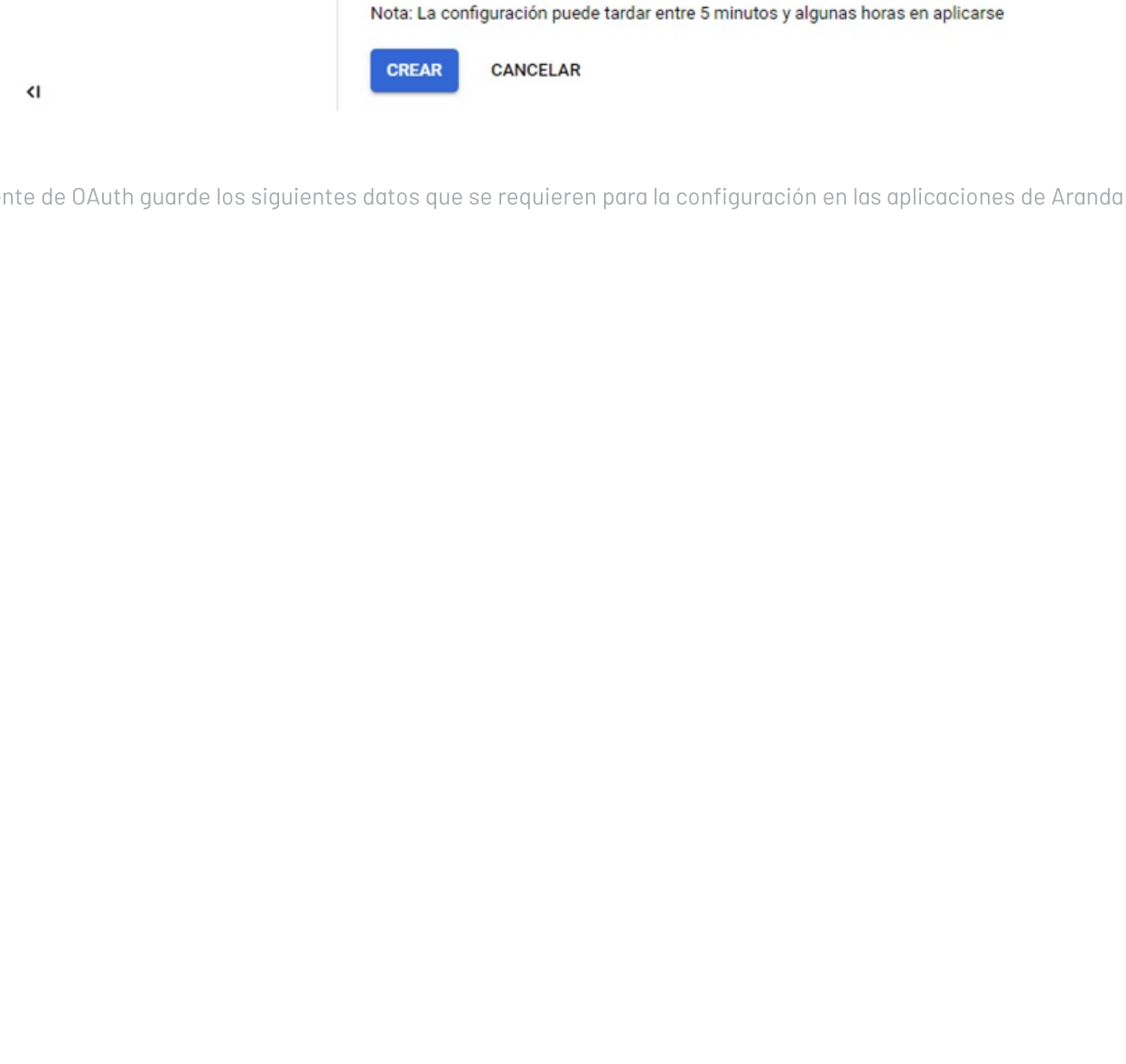
8. En la ventana Crear ID de cliente de OAuth en el campo Tipo de aplicación, seleccione la opción Aplicación web.



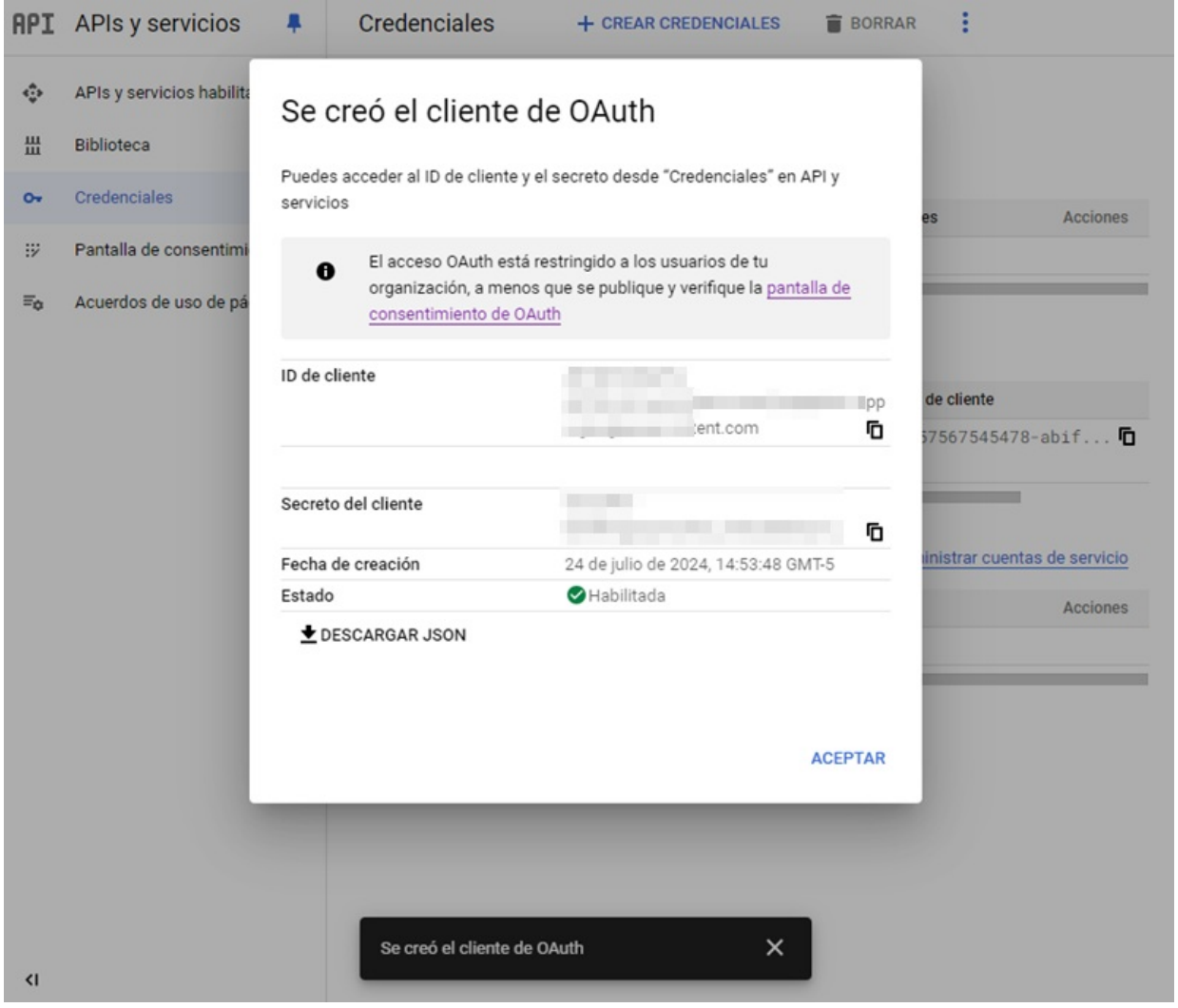
9. En la ventana Crear ID de cliente de OAuth en la sección URI de redireccionamiento autorizados, ingrese la URI correspondiente para el producto Aranda Service Management (ASMS) de la siguiente manera:

- Servidor de salida: https://[dominio]/ASMSAdministrator/Main/Pages/OauthToken.aspx
- Servidor de entrada (Case creator): (http://localhost)

Finalmente, haga clic en el botón CREAR.



10. En la ventana Se creó el cliente de OAuth guarde los siguientes datos que se requieren para la configuración en las aplicaciones de Aranda y en la generación del Refresh Token.

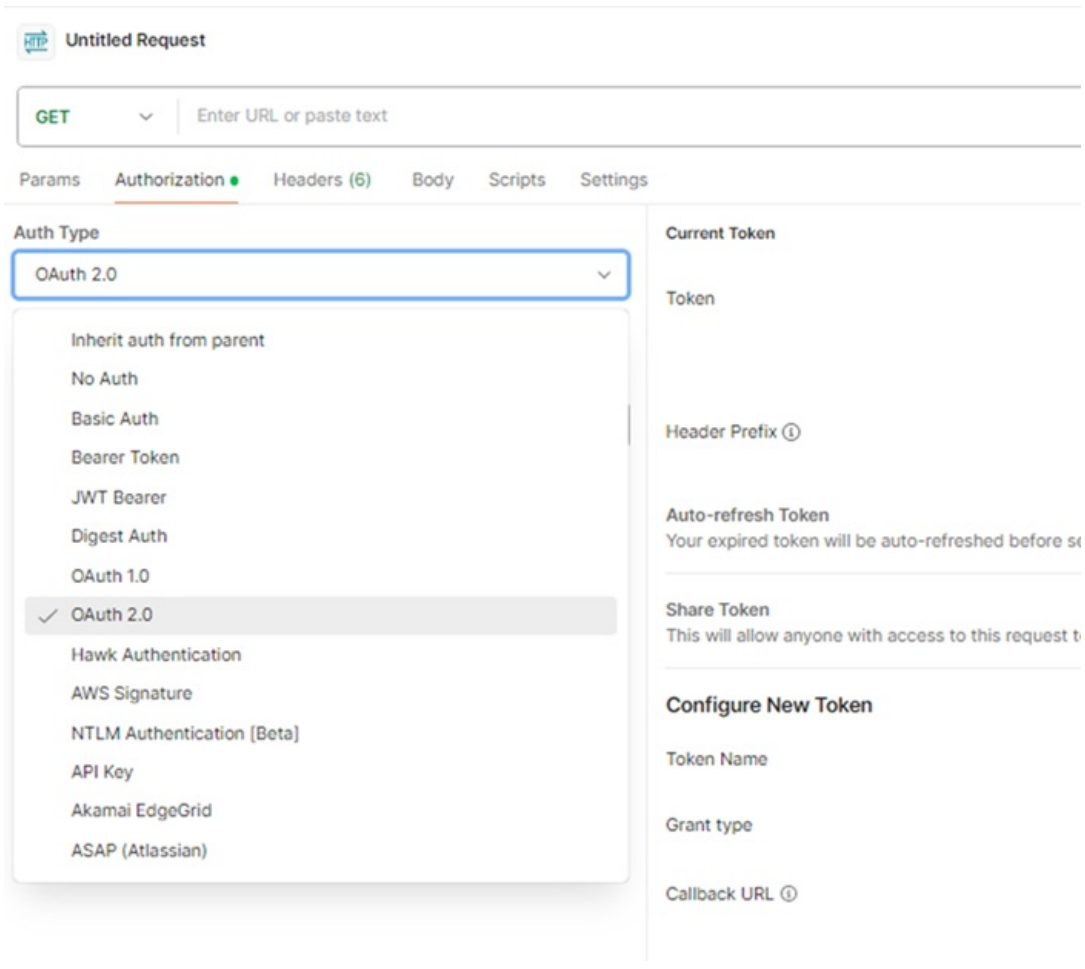


- Identificador de cliente -> ID de cliente.
- Valor secreto de cliente -> Secreto del cliente.
- Url del token -> https://oauth2.googleapis.com/token.
- Url de autorización -> https://accounts.google.com/o/oauth2/v2/auth

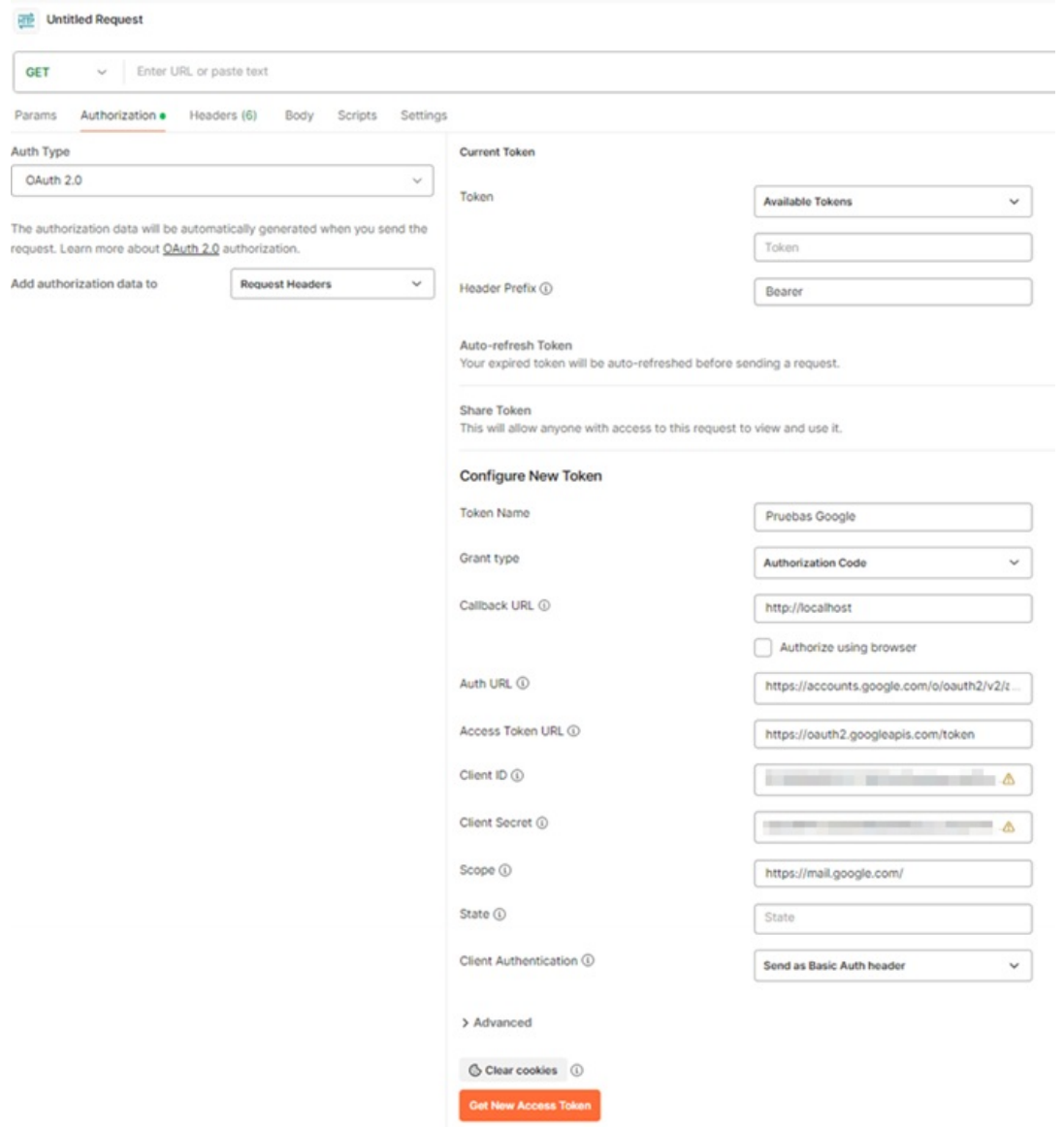
Solicitud Refresh Token Google

Para la solicitud del refesh_ token se debe utilizar el aplicativo de escritorio Postman y realizar las siguientes acciones:

1. Crea una nueva colección en Postman y en el tipo de autorización seleccionar OAuth 2.0.



2. En la vista ingrese los campos de la siguiente manera:

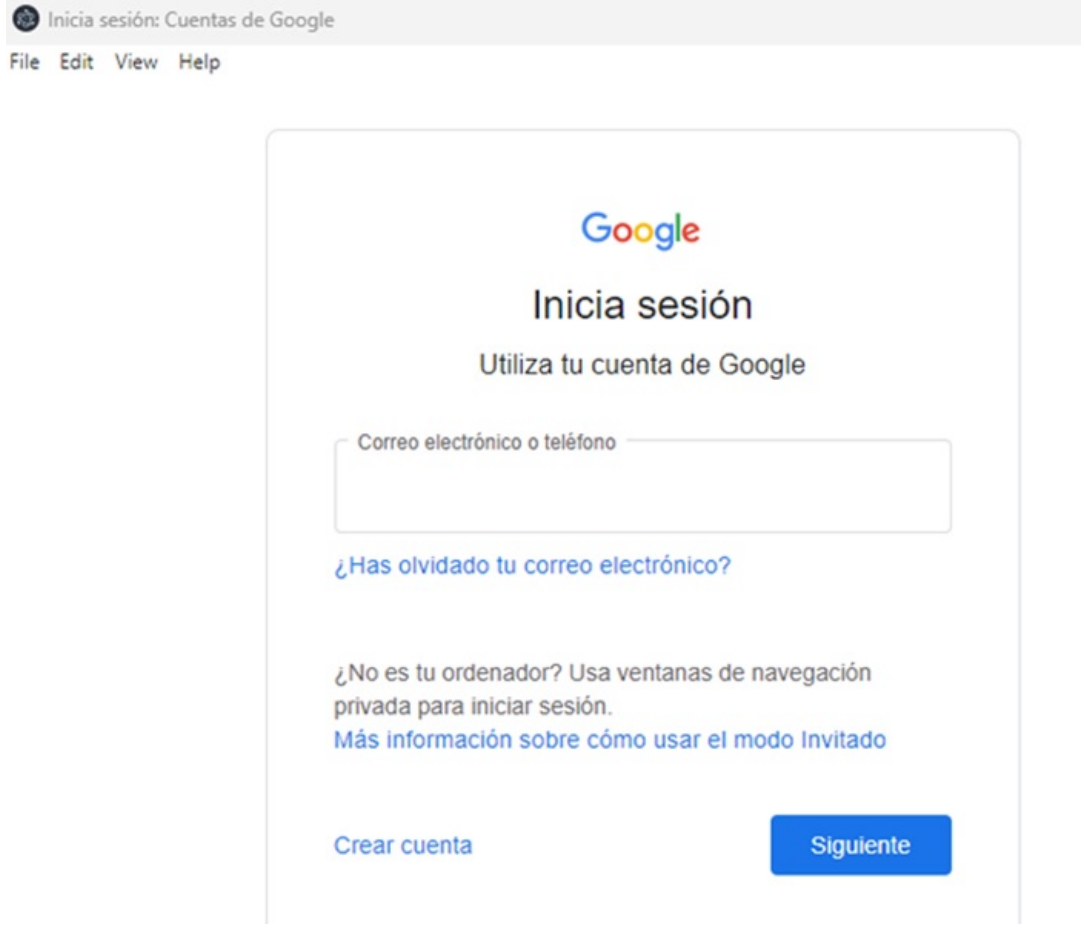


Campo	Descripción
Type	OAuth 2.0
Add auth data to	Request Headers
Acces Token	Availabe Token
Header Prefix	Bearer
Token Name	Nombre que desee para el token
Gran Type	Autorization Code
Callback URL	http://localhost
Auth URL	https://accounts.google.com/o/oauth2/v2/auth?access_type=offline
Access Token URL	https://oauth2.googleapis.com/token
Client ID	Ingrese el valor de Id. de aplicación (cliente).
Client Secret	Ingrese Valor secreto de cliente.
Scope	https://mail.google.com/
State	Se puede dejar en blanco.
Client Authentication	Send as Basic Auth header

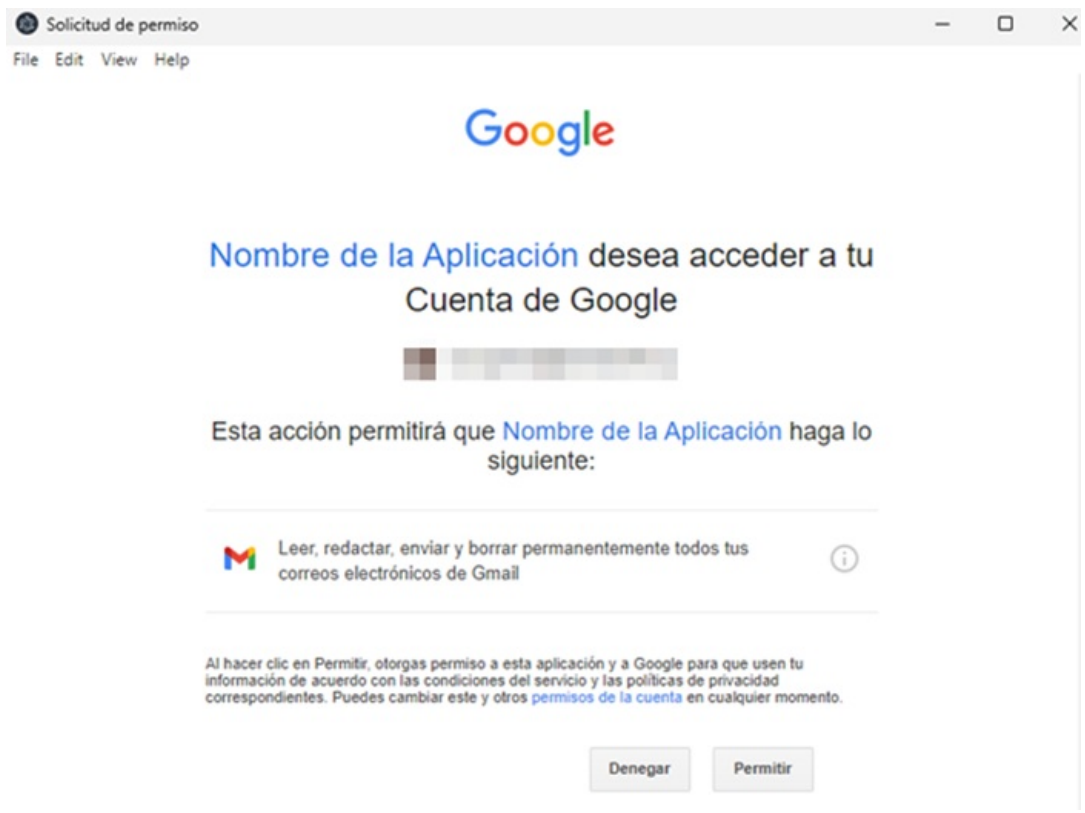
3. Al ingresar toda la información seleccione Get New Access Token.

> ⚐ Nota: Para garantizar la generación correcta del Refresh_Token, verifique las URLs ingresadas y asegúrese que no contengan saltos de línea ni espacios en blanco, tanto al inicio como al final.

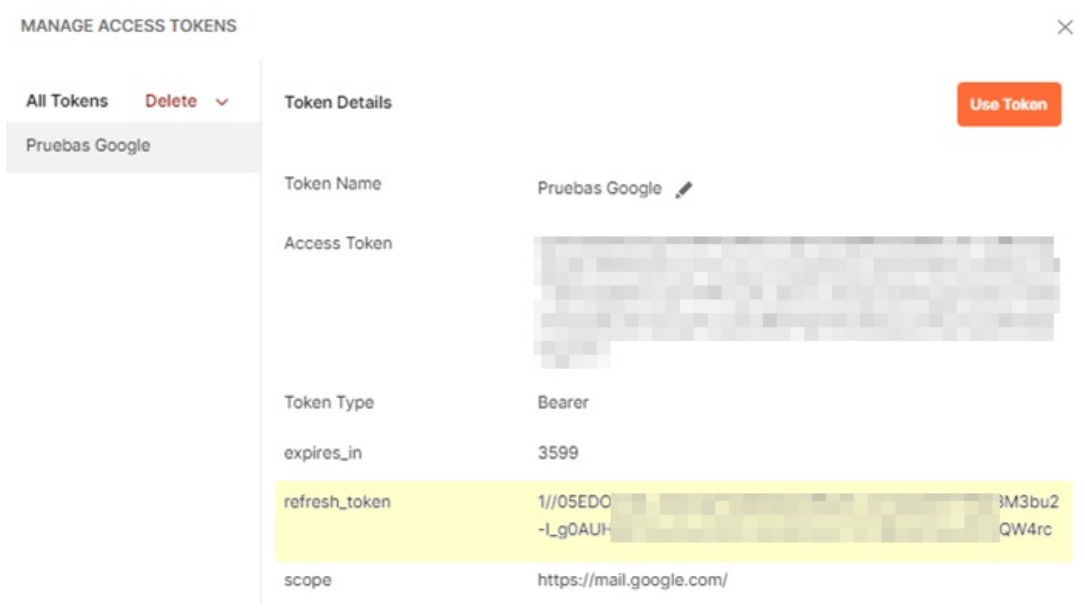
4. Se habilita la ventana de inicio de sesión en cuentas de Google; ingrese el correo y contraseña al que se requiere generar el refresh token.



5. La sesión se debe realizar con cuentas asociadas a la organización; si el ingreso es correcto, la sesión solicita que acepten los permisos requeridos.



5. Al aceptar los permisos, copie y guarde el refresh_token, ya que será utilizado en las configuraciones de Correo y Case creator en las aplicaciones de Aranda.

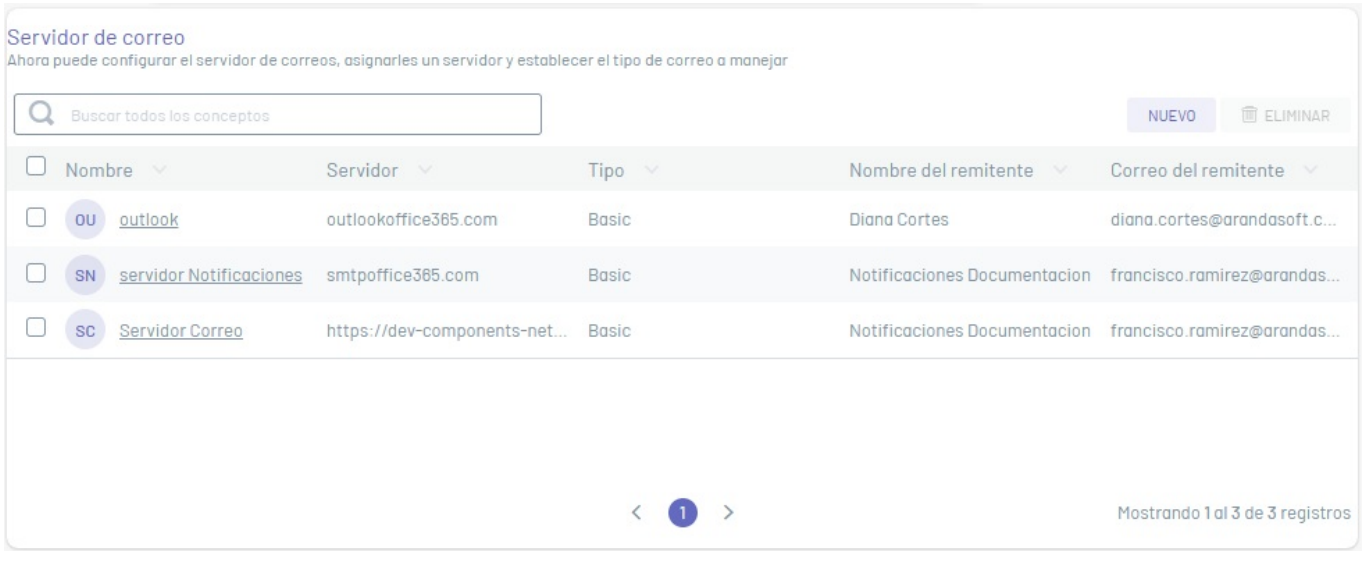


⚐ Nota: Un token de actualización (refresh token) puede dejar de funcionar por motivos como:
- El usuario revoque los permisos a la aplicación.
- El token de actualización no es utilizado durante seis meses..
- El usuario cambió la contraseña y el token de actualización contiene permisos de Gmail..
- La cuenta de usuario excedió la cantidad máxima de tokens de actualización (en vivo) otorgados.
Para ampliar mayor información consulte la documentación de Google: Actualiza el vencimiento del token

Gestión Servidor de Correo

Visualizar Servidor de Correos

1. En la vista de información de Servidor de Correos podrá visualizar el listado de servidores agrupados por datos básicos del servidor de correo y el tipo de autenticación.



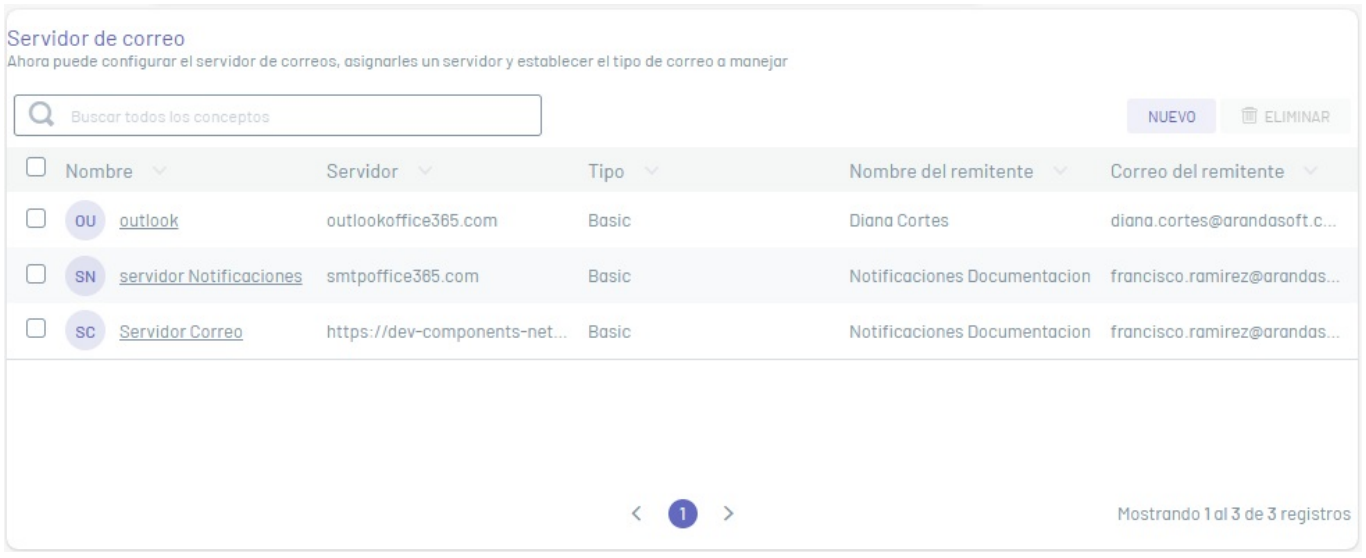
2. En la vista de información de servidor de correo, tendrá habilitadas acciones de gestión y organización de la información.Vista de Información en Entorno Commons

Enlaces Relacionados:

- Crear Servidor de Correo
- Editar Servidor de Correo
- Eliminar Servidor de Correo

Crear Servidor de Correo

1. En la vista de información del servidor de correo, seleccione el botón Nuevo

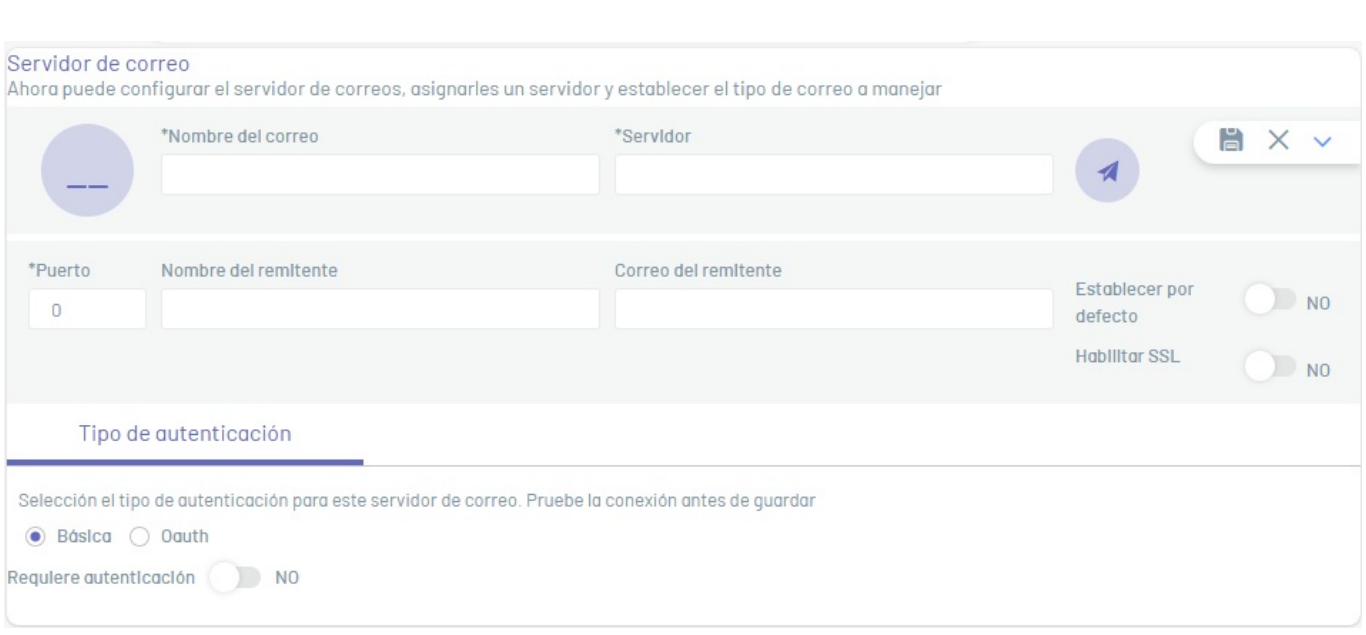


Datos Básicos

2. En la ventana que se habilita podrá completar los datos básicos del servidor de correo y el tipo de autenticación

3. En los datos básicos del servidor podrá ingresar campos como nombre, servidor, puerto, nombre y correo del remitente.

Cada uno de los campos de servicios de directorio deben tener en cuenta las especificaciones para campos Common

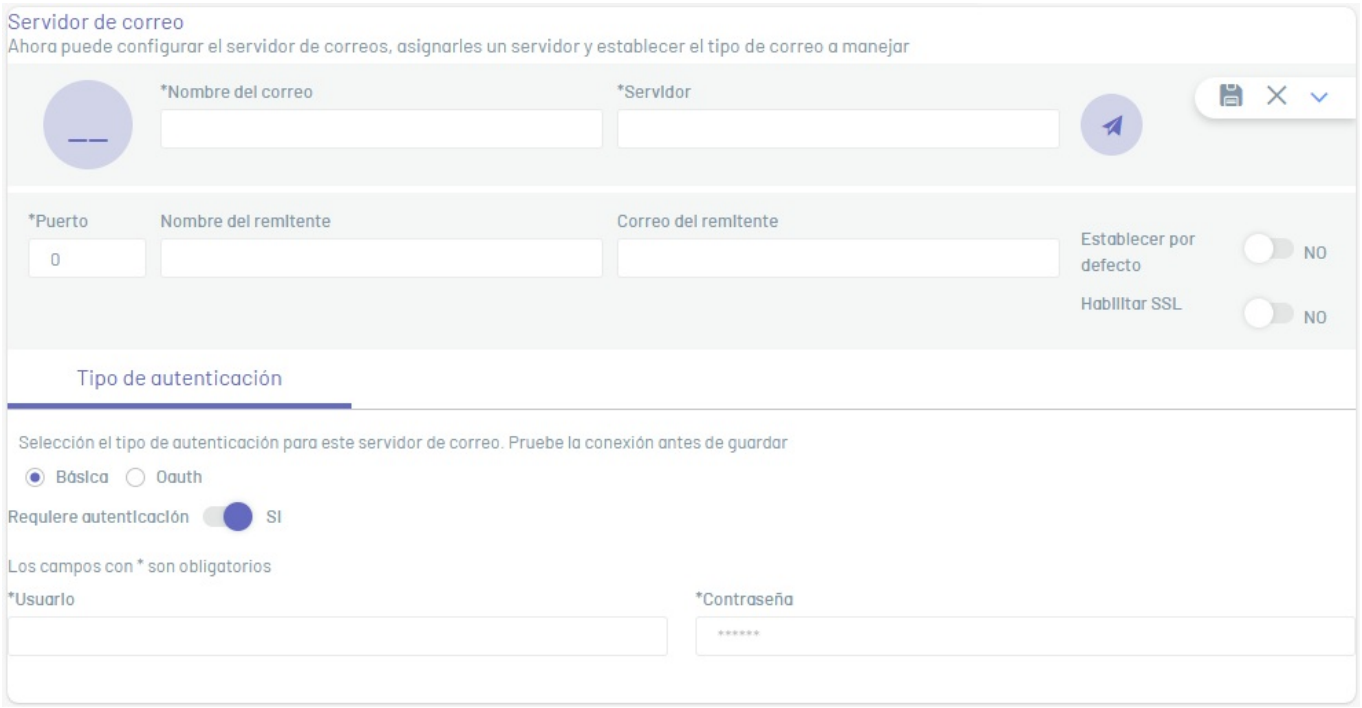


4. En la pestaña Tipo de Autenticación, podrá estabalecer las opciones disponibles por tipo de proveedor:

- Autenticación Básica
- Autenticación Oauth

Autenticación Básica

5. Para la autenticación básica, active la opción Requiere Autenticación e ingrese el usuario de acceso al servidor de correo y la contraseña requerida.



Autenticación Oauth (Open Authorization)

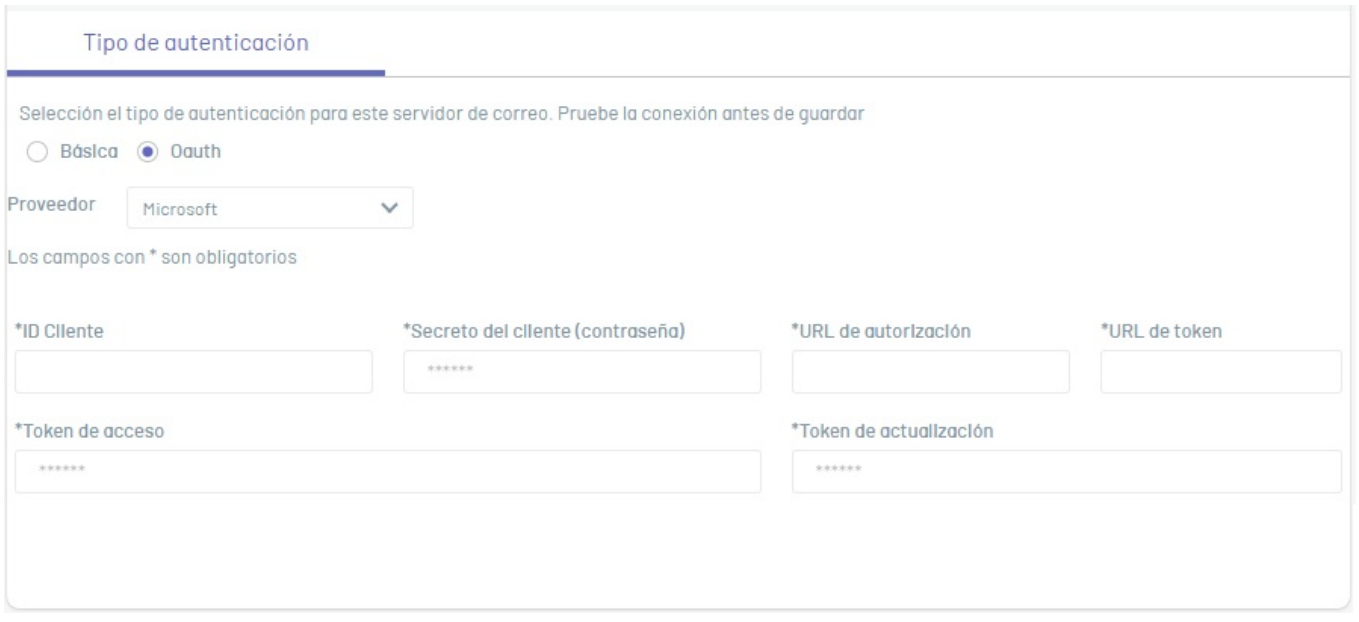
6. Para la autenticación OAuth defina un proveedor de autenticación (Microsoft, Google, Configuración Manual).

⚐ Nota: Si Microsoft es el proveedor de Autenticación, configure previamente la informacion relevante al proveedor de correo Oauth en el portal de Azure, generando los parámetros requeridos para los campos de autenticacion del servidor de correo:

- ID del cliente, url de autorización y url de token
- Secreto del cliente
- Token de acceso y Token de actualización.

⚐ Nota: Si Google es el proveedor de Autenticación, configure previamente la informacion relevante al proveedor de correo Oauth en el portal de Google, generando los parámetros requeridos para los campos de autenticacion del servidor de correo:

- ID del cliente, url de autorización, url de token y Secreto del Cliente
- Token de acceso y Token de actualización.

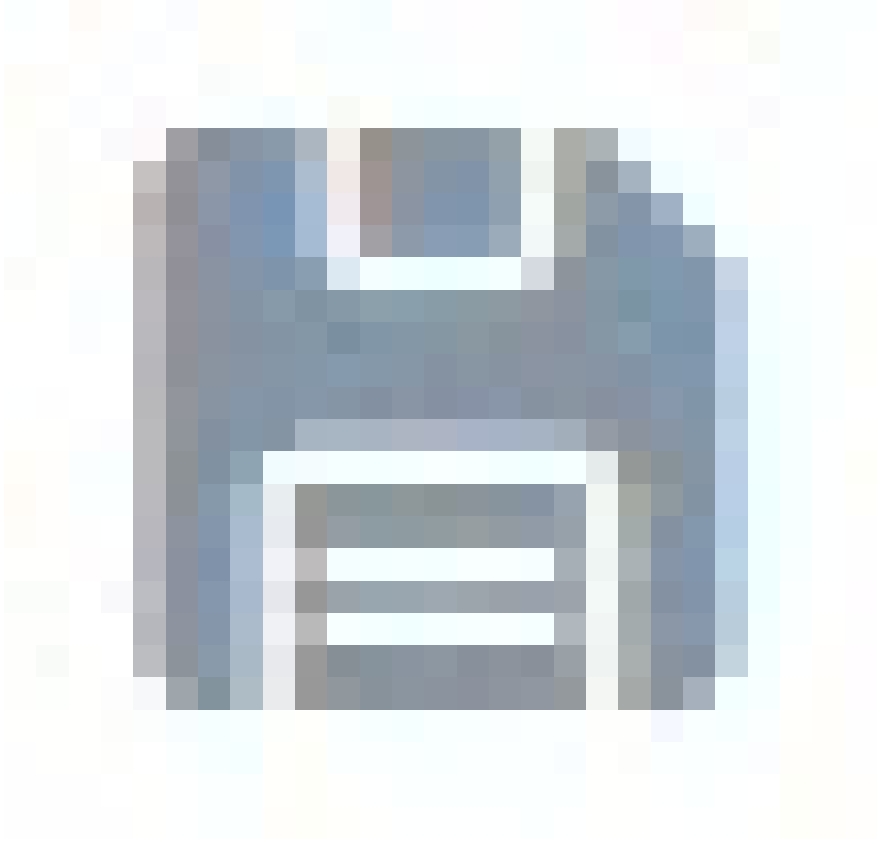


7. Si la conexión es con un proveedor diferente a Microsoft ó Google, podrá establecer la Configuración Manual

8. Para cada proveedor podrá definir los campos requeridos como ID del cliente, secreto del cliente, url de autorización, entre otros.

Cada uno de los campos del servidor de correo para el tipo de autenticación Oauth, deben tener en cuenta las especificaciones para campos Common.

9. Al terminar de configurar el servidor de correo, haga clic en el ícono Guardar

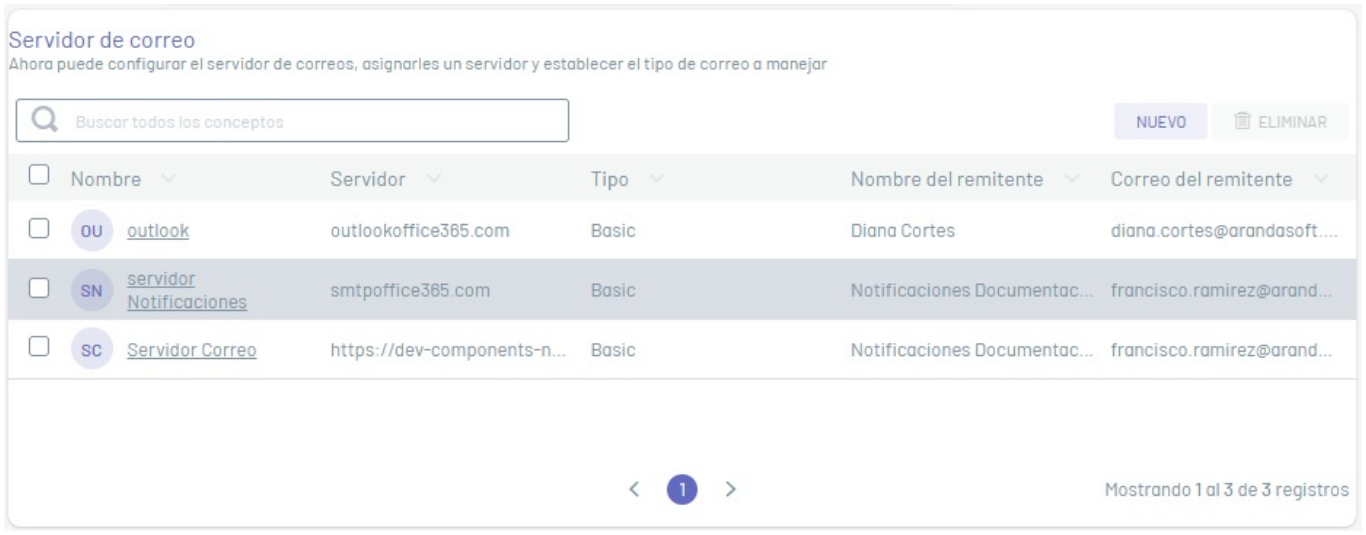


para confirmar los cambios realizados.

⚐ Nota: Si ha creado más de una configuración de servidor de correo, sólo una de ellas puede estar marcada como configuración Por defecto.

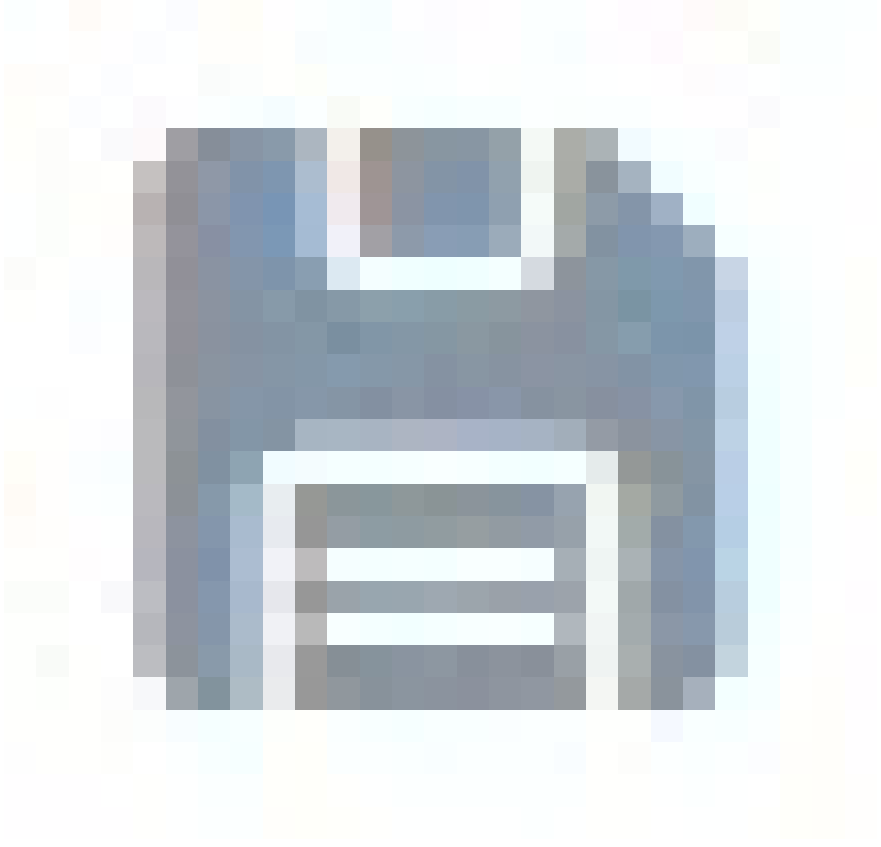
Editar Servidor de Correo

1. Para editar un servidor de correo, en la vista de información del servidor, seleccione un registro del listado de correos existentes.



2. Se habilita la ventana servidor de correo, donde podrá modificar los datos básicos del servidor de correo o del tipo de autenticación.

3. Al terminar de editar el servidor de correo, haga clic en el ícono Guardar

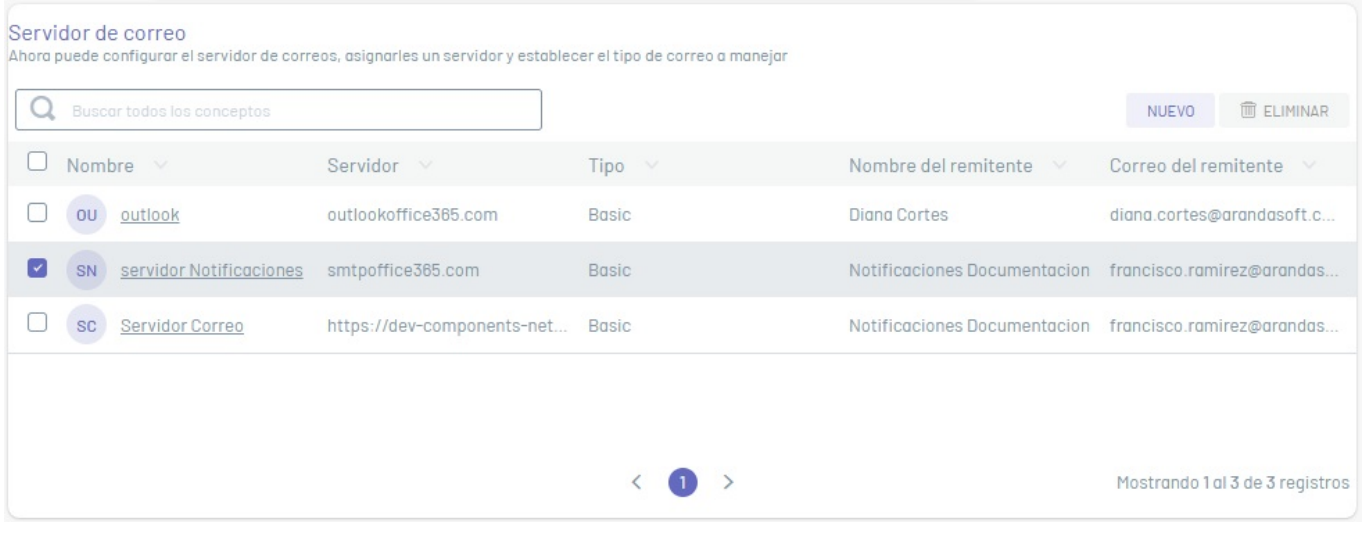


para confirmar los cambios realizados.

Eliminar Servidor de Correo

1. En la vista de información de servidores de correo, seleccione un registro del listado de servicios de correos que desea eliminar y haga clic en el botón

.



2. Podrá visualizar un mensaje de confirmación para validar la acción de borrado.

Módulo Servicio de Directorios

Configuración Previa Servicios de directorio

1. Configuración Proveedores de Autenticación

Configure los proveedores (LDAP, Microsoft Entra ID) para los procesos de sincronización de usuarios del directorio activo.

Para mayor información consulte la Sincronización Ldap/Microsoft Entra ID ↪.

2. Configuración reCAPTCHA (Opcional)

Configure un nivel de seguridad en los procesos de autenticación, definiendo la configuración del reCAPTCHA de Google para usarla al momento de loguearse los usuario.

Para mayor información consulte la Configuración de Seguridad reCAPTCHA ↪.

3. Gestión Módulo Servicios de Directorio

En el módulo Servidor de Directorios podrá crear, actualizar y eliminar configuraciones de servidores de correo electrónico para las notificaciones que se enviarán a los usuarios desde la consola web.

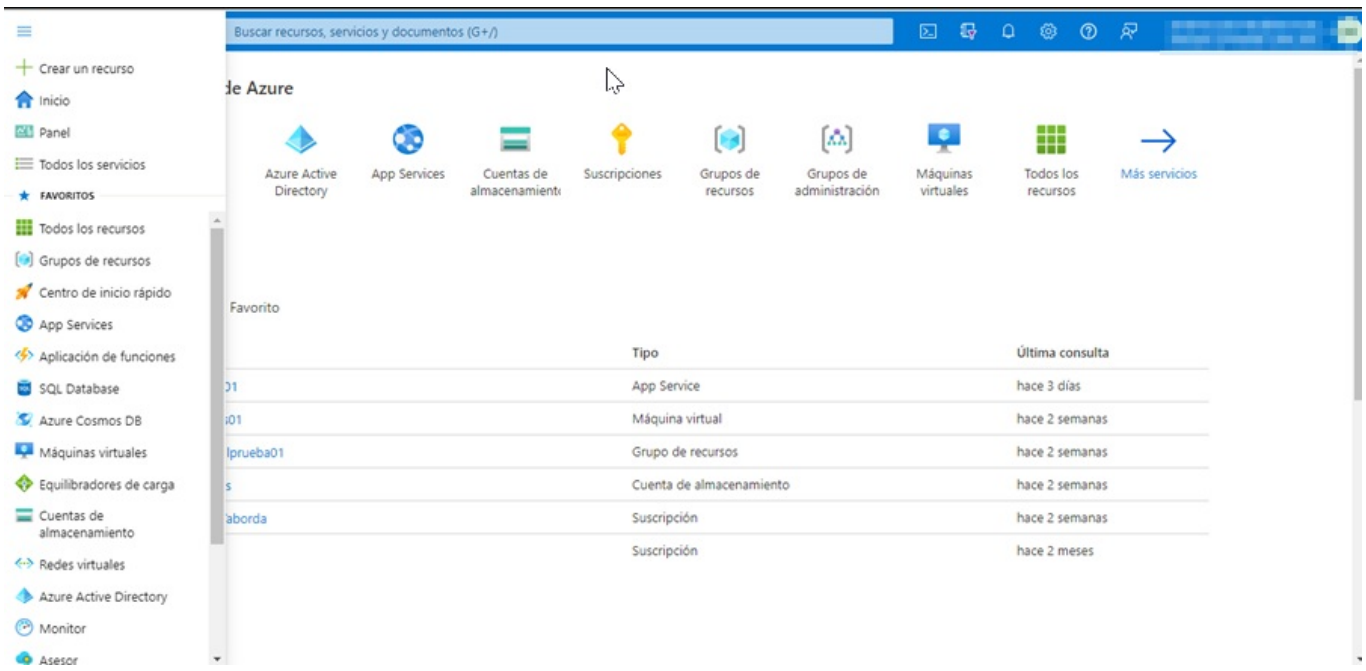
Para mayor información consulte la Gestión Servicio de Directorios ↪.

Sincronización Ldap/Microsoft Entra ID

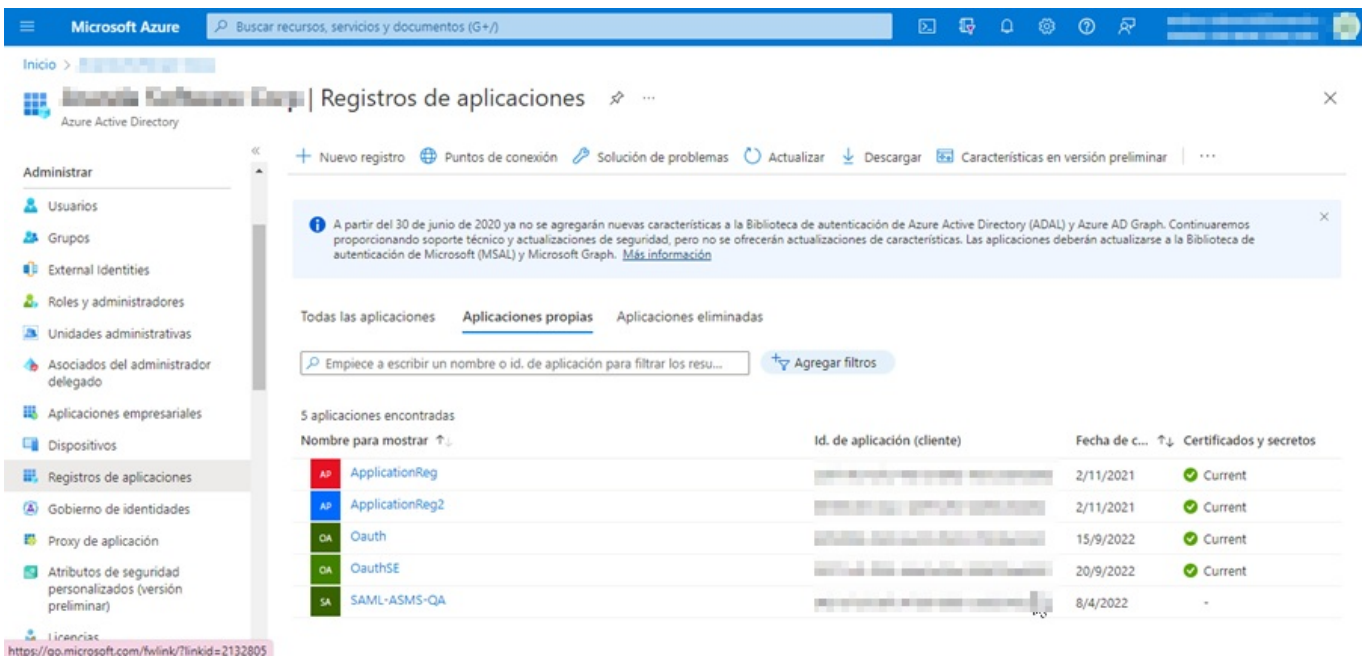
Crear Aplicación en Azure

▶ Requisitos Autenticación Azure: ❯

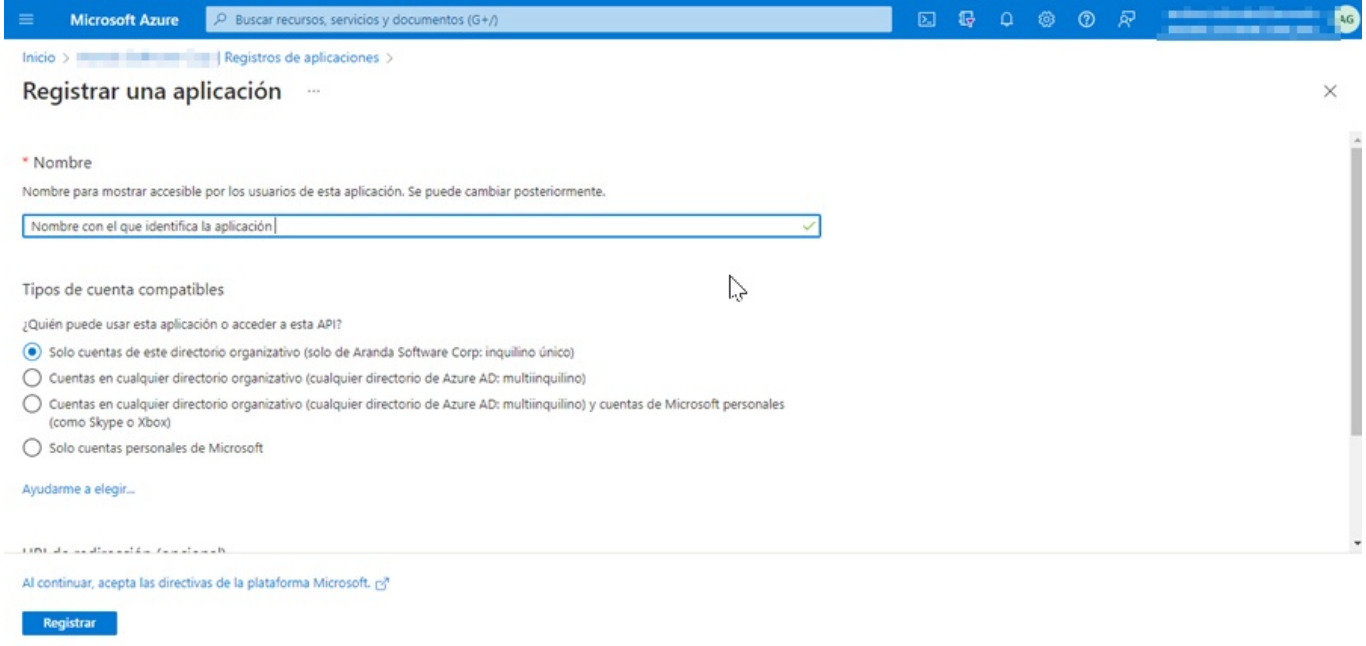
1. Se accede al portal de Azure Ver Microsoft Azure , busque y seleccione Microsoft Entra ID.



2. . En la sección Administrar busque y seleccione Registros de aplicaciones, haga clic en Nuevo registro.



3. Se diligencia el campo del nombre y se selecciona la opción deseada en (Tipos de cuentas compatibles), clic en Registrar.

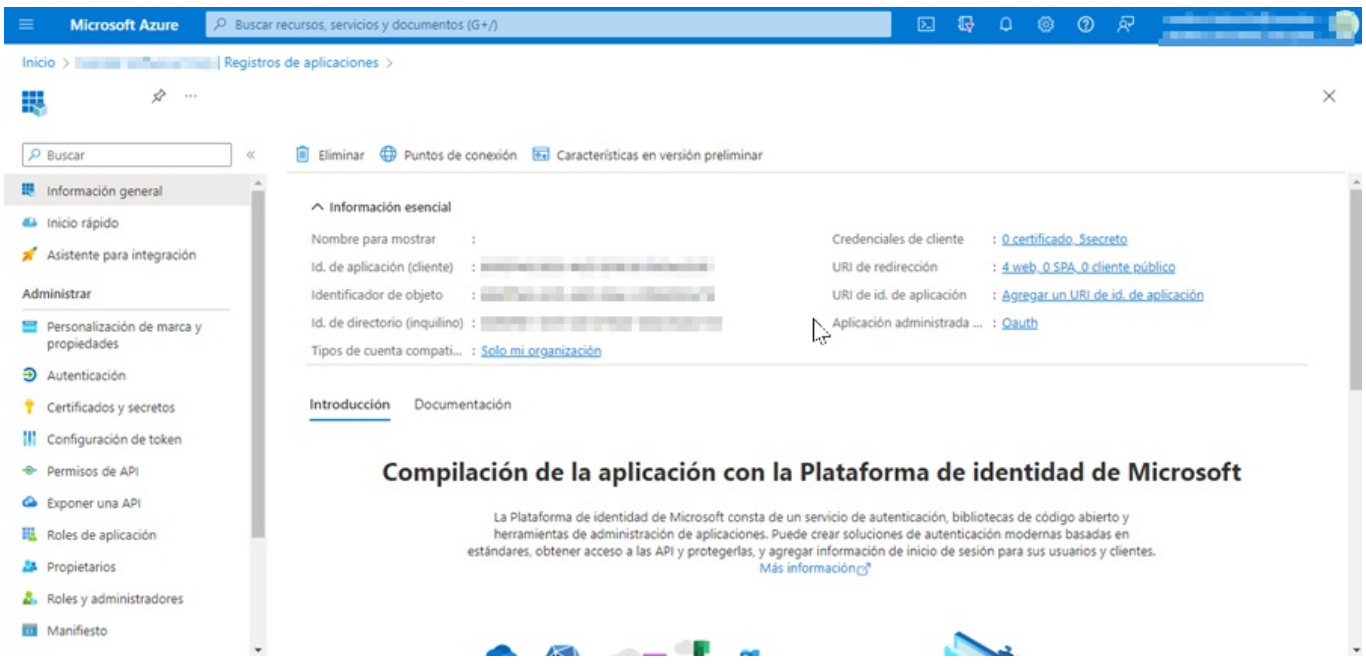


4.Cuando se tenga registrada la aplicación, guarde los siguientes datos que se requieren para la configuración en la sincronizacion de LDAP con Microsoft Entra ID.

- Id. de directorio (inquilino) = URL

  ⚐ Nota: La URL debe configurarse de la siguiente manera: (https://login.microsoftonline.com/ + Id. de directorio inquilino/)

- Id. de aplicación (cliente) = Cliente id



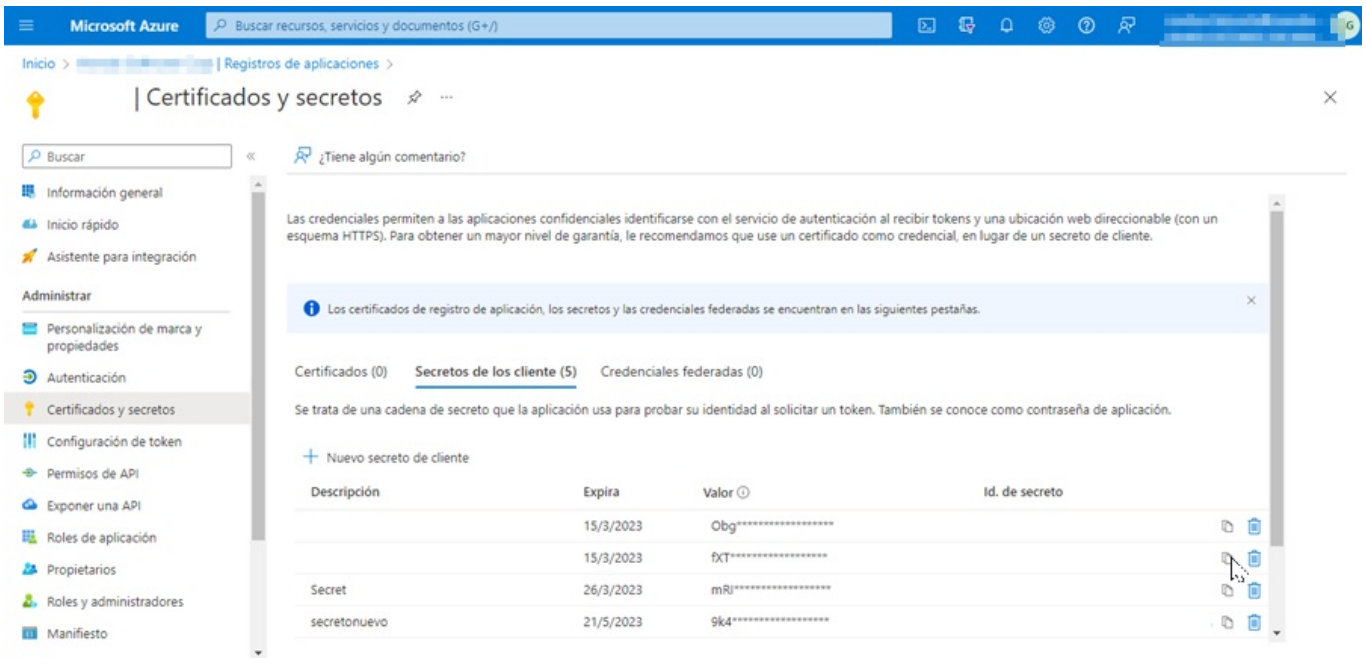
Configurar Aplicación Azure

Cuando se tenga la aplicación creada y los datos guardados, podrá configurar la aplicación de la siguiente manera:

Creación del Secreto

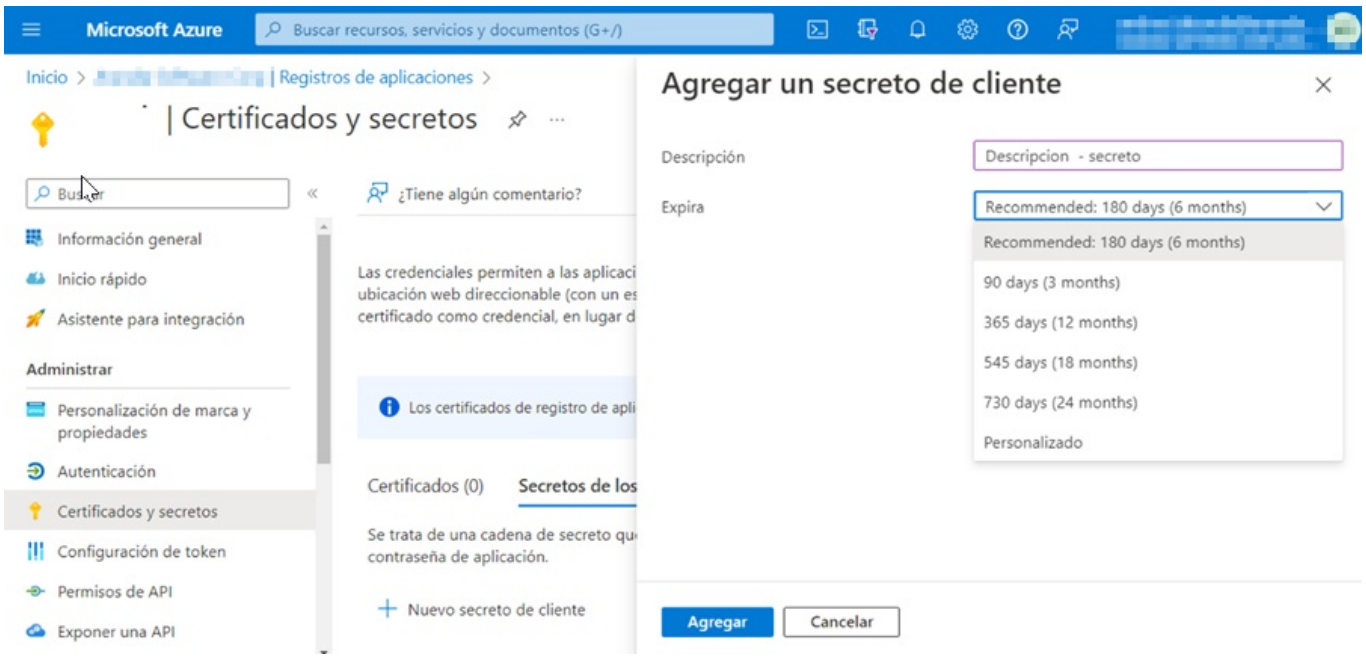
1. Para crear el secreto ingrese al portal de Azure > Menú > Microsoft Entra ID > Registros de aplicaciones > seleccione la aplicación creada del listado disponible.

2. En la sección Administrar seleccione la opción Certificados y secretos > y en la vista de información haga clic en la pestaña Nuevo secreto de cliente.



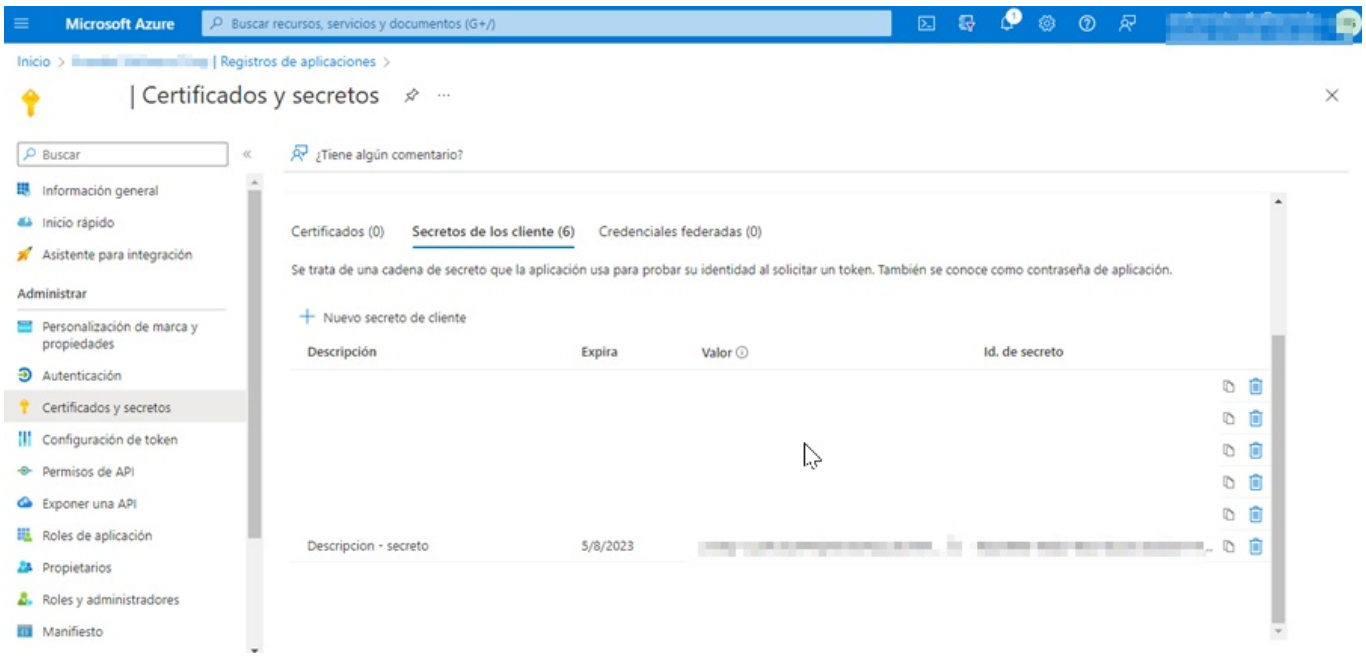
3. En la ventana Agregar un secreto de cliente diligencie el campo Descripción, defina la duración del secreto en el campo Expira y haga clic en el botón Agregar.

⚐ Nota: Se recomienda no olvidar el tiempo de duración configurado. En caso de vencimiento, de no actualizarse, fallará la autenticación



4. El valor del secreto sólo es visible cuando se crea; se debe guardar para usarlo más adelante o consultarlo durante las configuraciones que se requieran en los productos de Aranda.

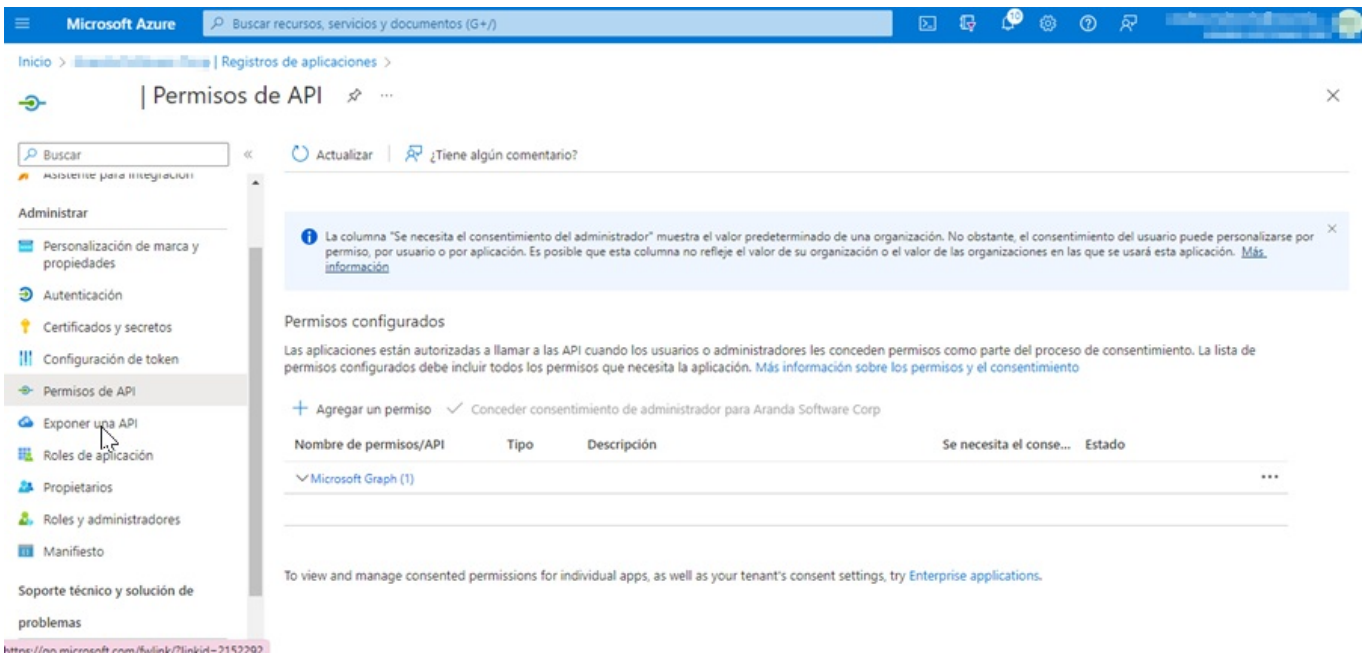
- Valor secreto de cliente = Cliente secreto.



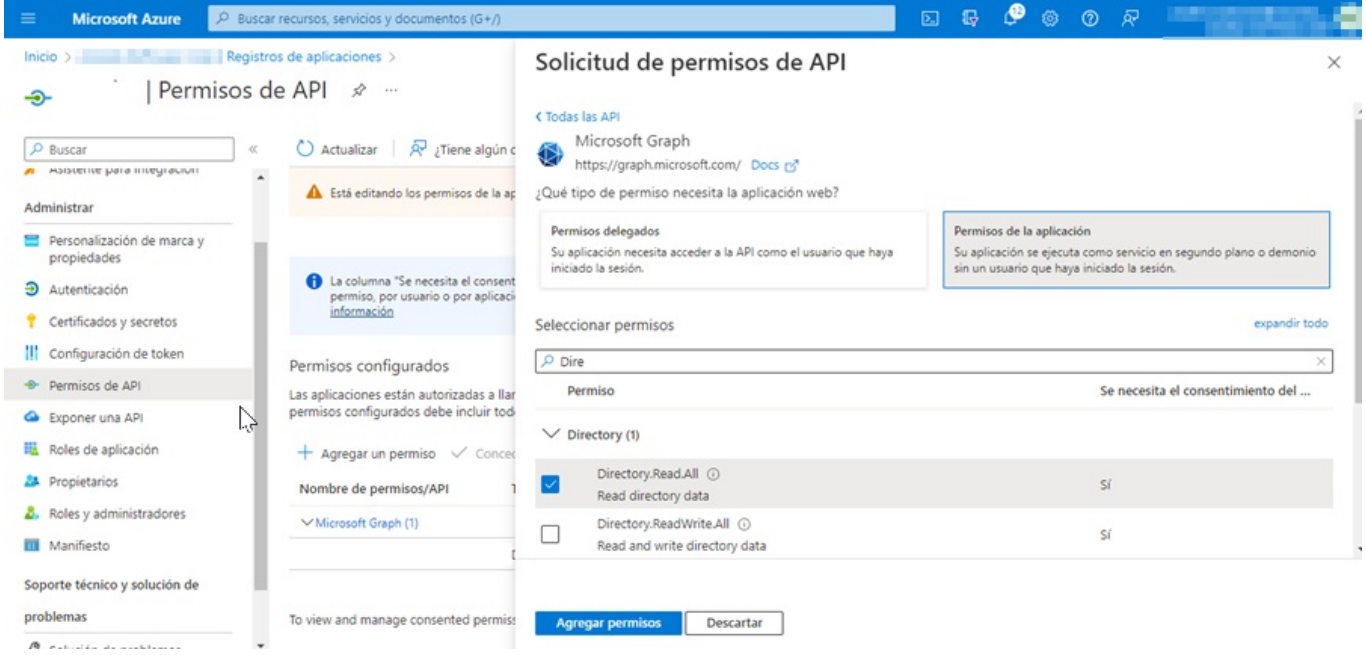
Configurar permisos de API

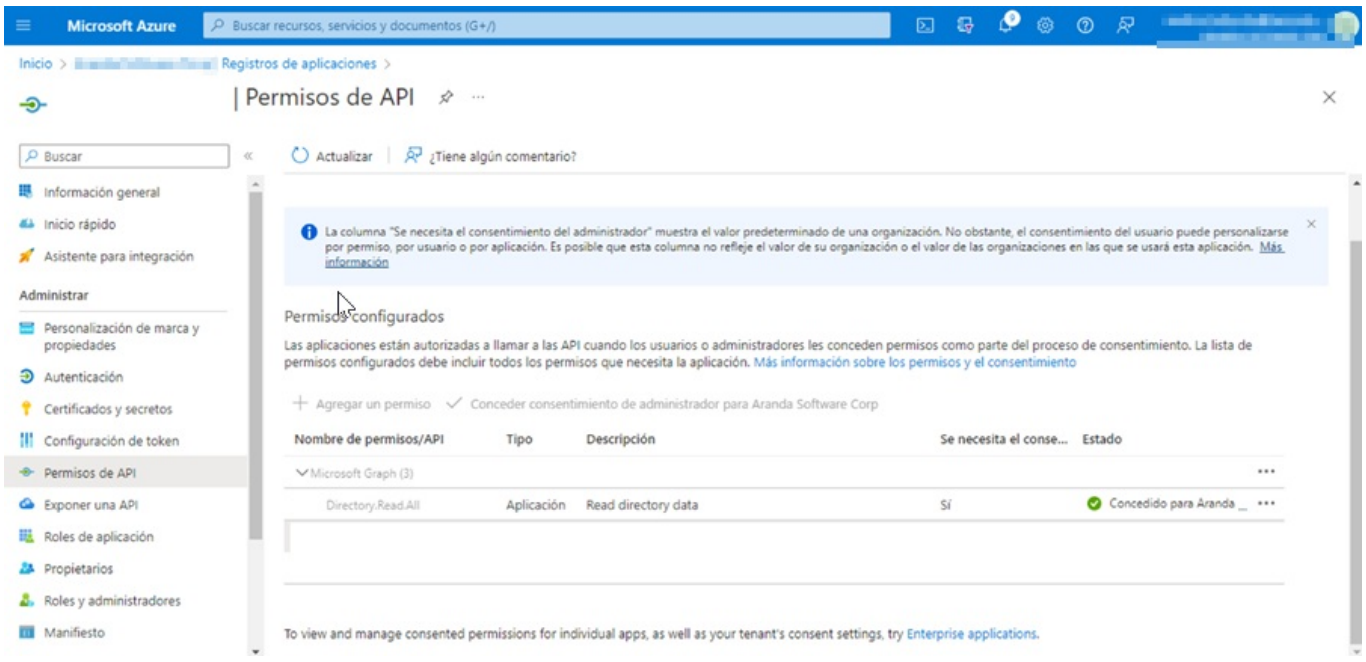
1. Para configurar los permisos de API se ingresa al portal de Azure > Menú > Microsoft Entra ID > Registros de aplicaciones > seleccione la aplicación creada del listado disponible.

2. En la sección Administrar del menú principal, seleccione la opción Permisos de API > y en la vista de información, en la sección Permisos Configurados, haga clic en Agregar un permiso.



3. En la ventana Solicitud de permisos de API, seleccione la opción Microsoft Graph > y luego Permisos de Aplicación, active los permisos de acuerdo a sus requerimientos: Directory.Read.All (Leer datos de directorio). Haga clic en Agregar permiso.





Una vez realizado este proceso, podrá finalizar la sincronización con Azure AD.

Sincronización Ldap/ Microsoft Entra ID

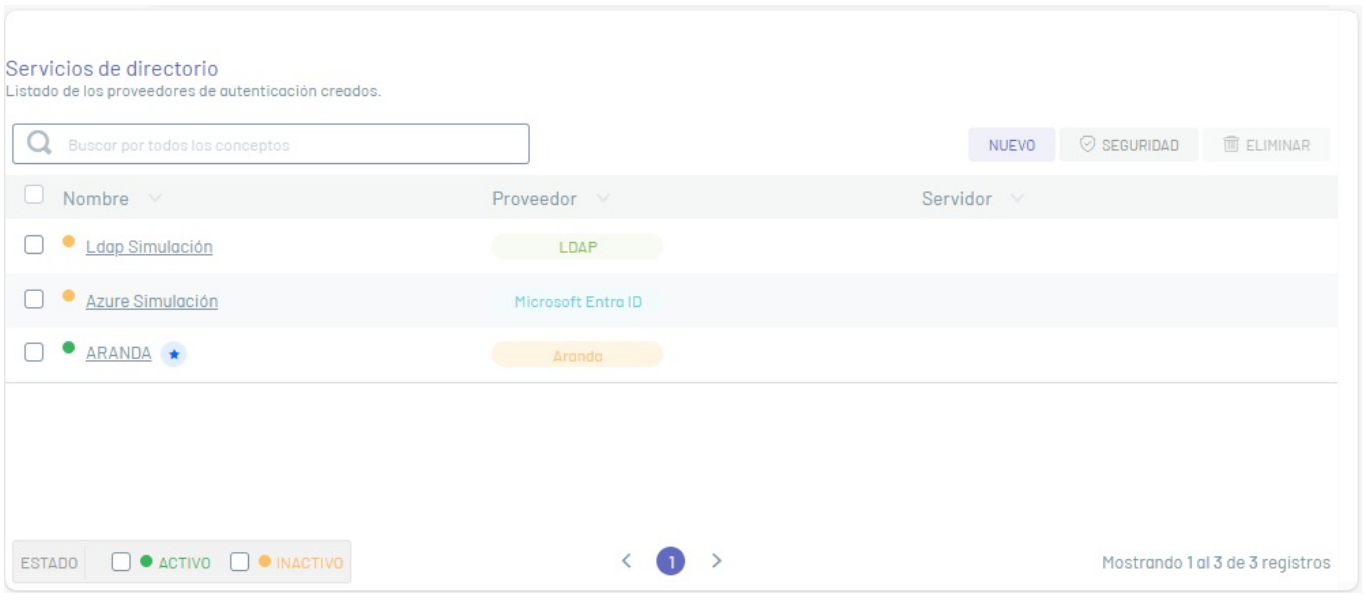
Para realizar la configuración de Ldap con Microsoft Entra ID en las aplicaciones Aranda, verifique el siguiente enlace:

- Ver Sincronización y configuracion Aranda Service Management ASMS

Gestión servicios de directorios

Visualizar Servicio de Directorios

1. En la vista de información de Servicio de directorios podrá visualizar el listado de proveedores de autenticación, agrupados por datos como:



Campo	Tipo Campo	Descripción
Nombre	Texto	Nombre con el cual se identifica el servicio de directorio.
Proveedor	Texto	Tipo de servicio de directorio.
Servidor	Texto	Nombre y/o la IP en donde se encuentra el dominio.

⚐ Nota: La columna Proveedor indica el tipo de proveedor del servicio de directorio; el cual puede ser Aranda, LDAP y Microsoft Entra ID

⚐ Nota: A través del proveedor interno Aranda, podrá Configurar las especificaciones para las políticas de contraseña para el acceso de Aranda.

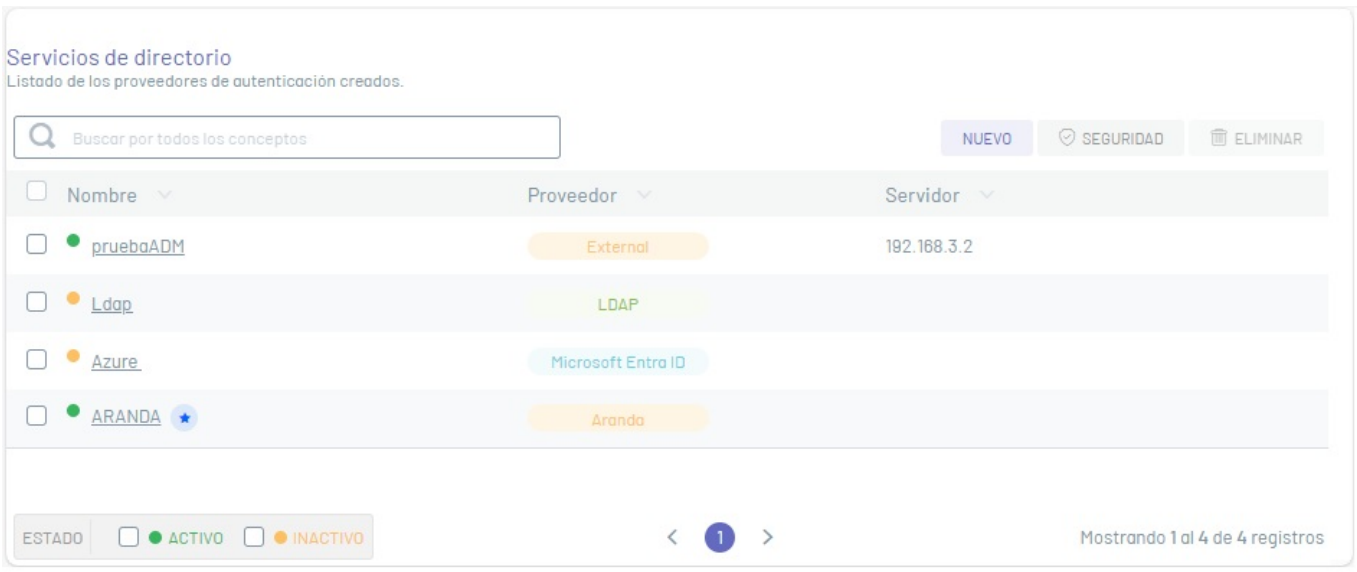
2. En la vista de información de servicios de directorio, tendrá habilitadas acciones de gestión y organización de la información.Vista de Información en Entorno Commons

Enlaces Relacionados:

- Crear Servicio de Directorios
- Editar Servicio de Directorios
- Eliminar Servicio de Directorios

Crear Servicios de directorio

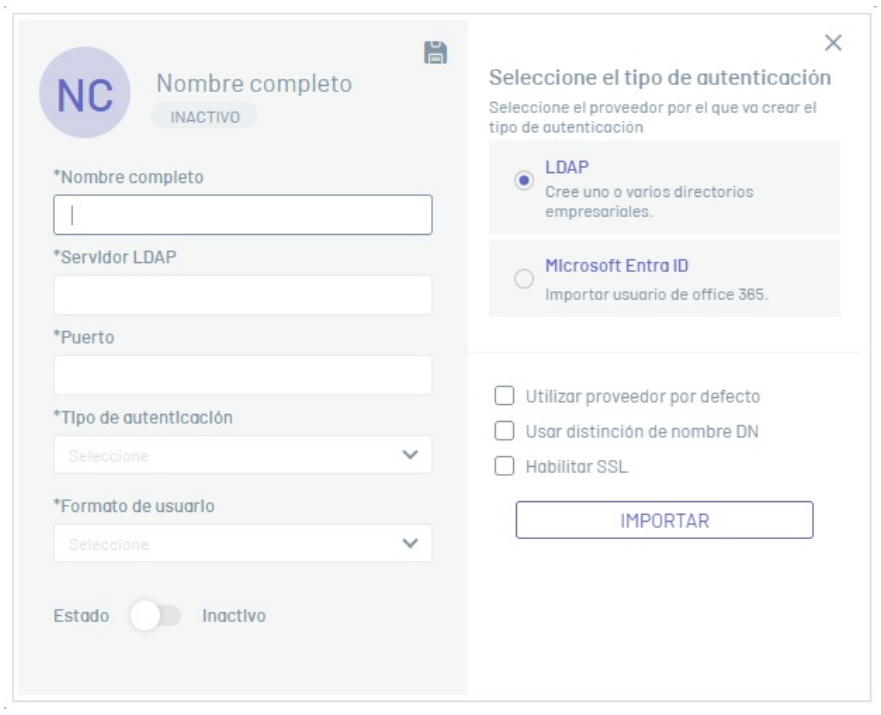
1. En la vista de información de servidores de directorios, seleccione el botón Nuevo.



Datos Básicos

2. En la ventana que se habilita podra completar la información básica requerida para establecer la conexión con su servidor de directorio como nombre, servidor, puerto, tipo de autenticación, proveedores, entre otros.

Cada uno de los campos de servicios de directorio deben tener en cuenta las especificaciones para campos Common



Tipo de Autenticación

4. En la sección Tipo de Autenticación, podrá estabalecer el tipo de proveedor para la autenticación:

- LDAP: Es un protocolo de aplicación estándar para consultas, que puede almacenar, gestionar, proteger y autenticar la información de los usuarios.
- Microsoft EntraID: Servicio de administración de identidades basado en el cloud de Microsof, desde el cual se pueden importar los usuarios de Office 365

Proveedor LDAP

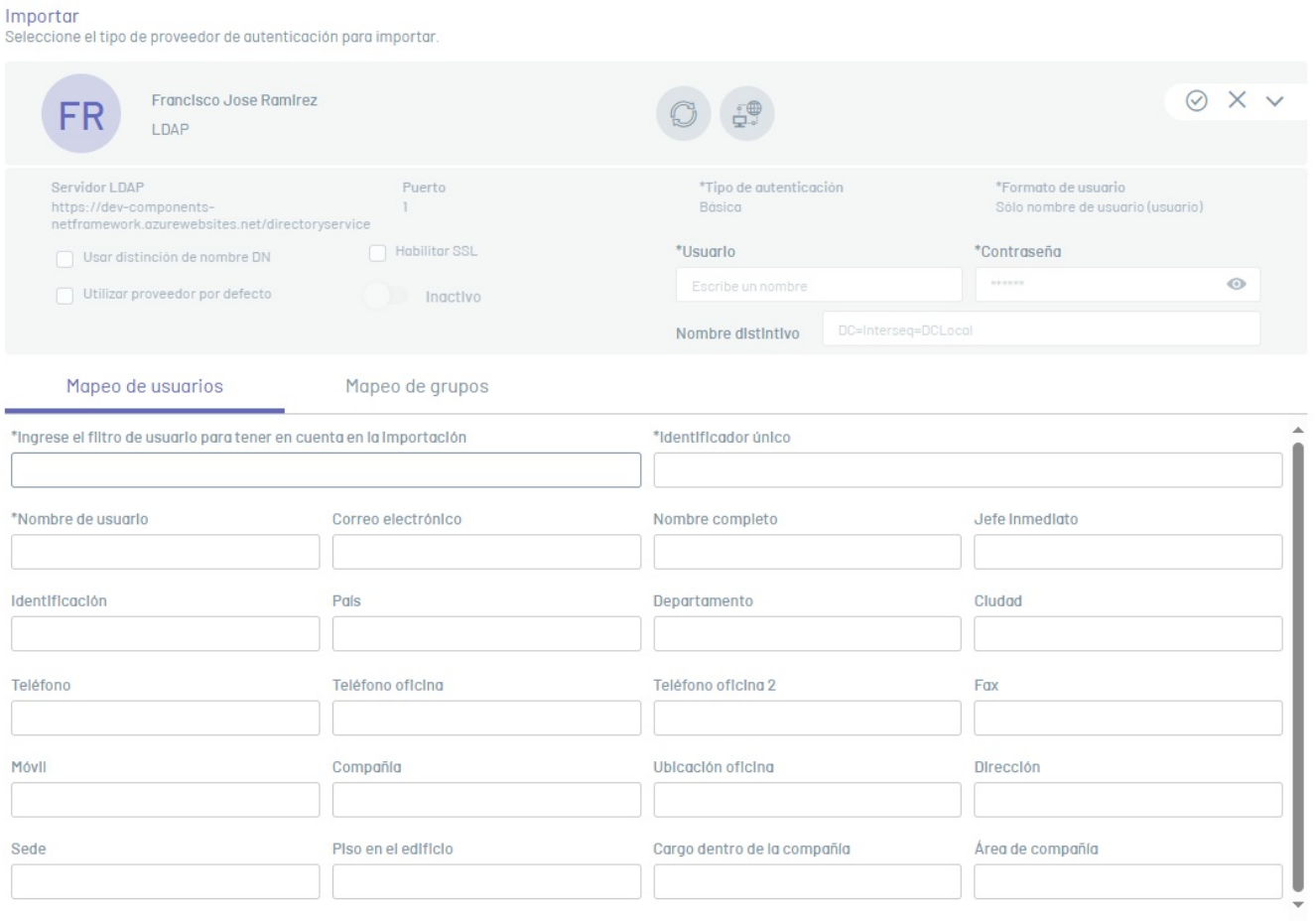
5. En la vista detalle del proveedor, haga clic en el botón IMPORTAR; se habilita la ventana Importar donde podrá ingresar los datos necesarios para la sincronización. En la información básica del directorio empresarial LDAP, ingrese los datos usuario y contraseña.

⚐ Nota:

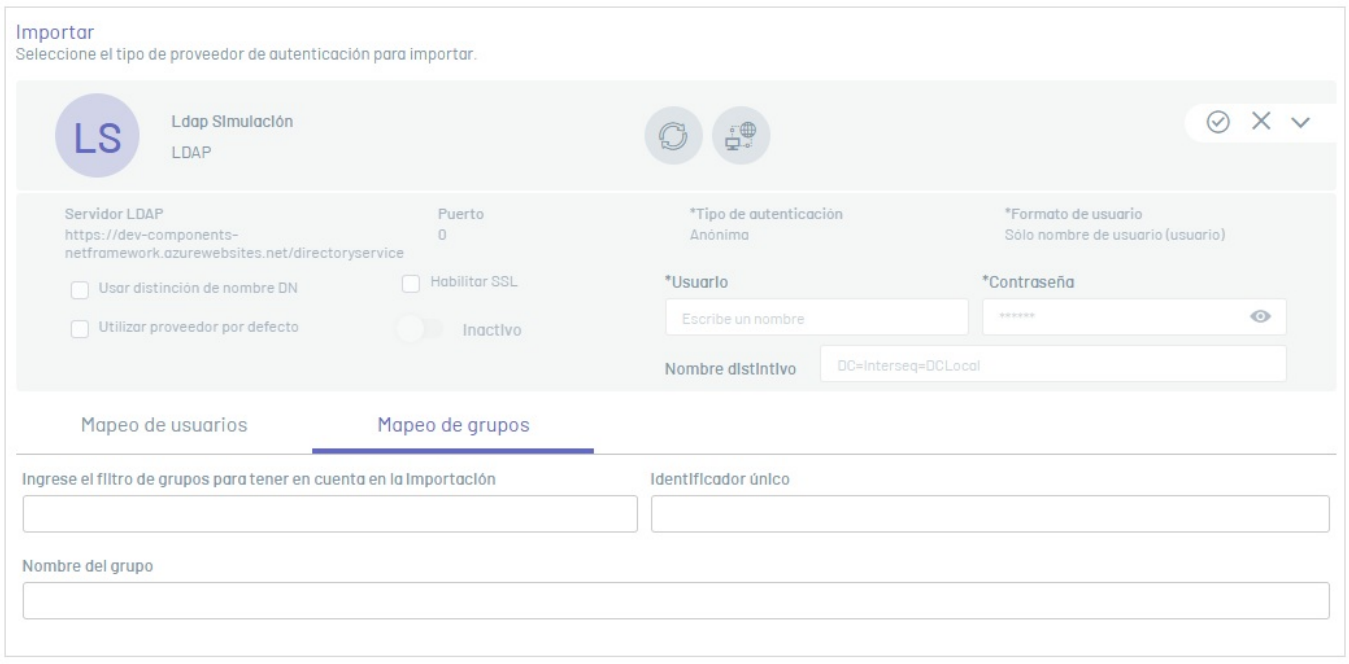
- Para los directorios activos configurados con OpenLDAP, diligencie el campo Nombre distintivo.
- Puede consultar algunos filtros de ejemplo para LDAP

En las pestañas de Mapeos podrá especificar los atributos de nomenclatura correspondientes para cada campo y los filtros deben cumplir con la sintaxis de LDAP para sincronizar la información.

En la pestaña Mapeo de Usuarios los campos obligatorios a registrar son: Filtro de usuario para tener en cuenta en la importación, identificador único y nombre de usuario.



En la pestaña Mapeo de Grupos (grupos de usuarios) si digita algún valor en el campo “Ingrese el filtro de grupos para tener en cuenta en la importación”, los campos “Identificador único” y “nombre del grupo” se vuelven obligatorios.



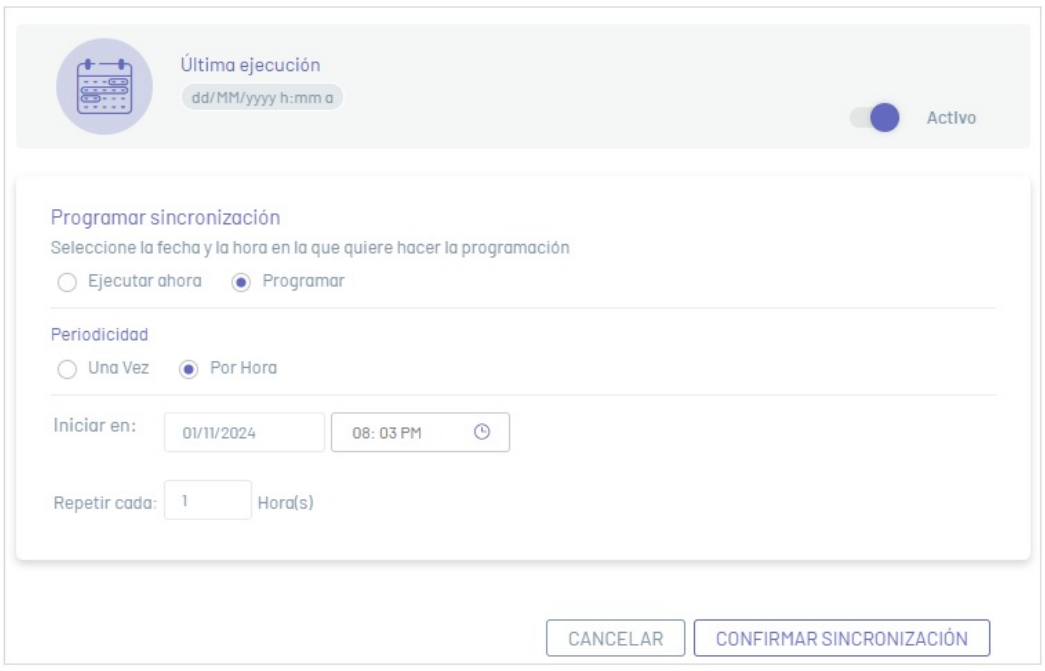
6. Al registrar los campos haga clic en el botón Probar conexión

. Si la conexión fue exitosa podrá visualizar el mensaje: La información quedó completa ya puedes finalizar la importación y se autoriza la continuación del proceso.

7. Al terminar de registrar la información, haga clic en el botón de sicronizar

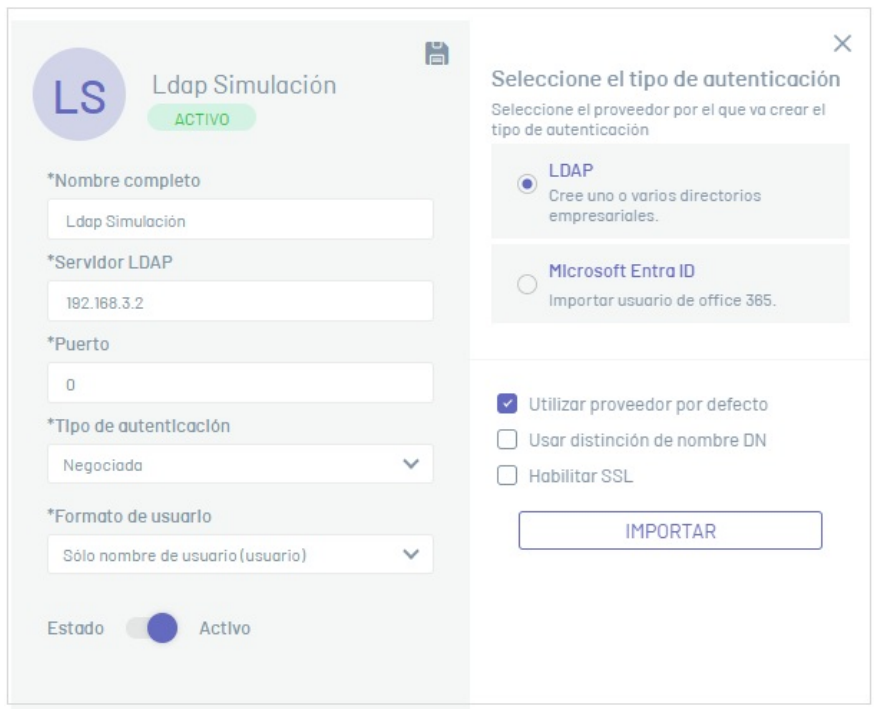
y en la ventana que se habilita active la sicronización.

8. La sincronización puede ser manual (de inmediato) o se puede programar automáticamente una única vez o cada cierto número de horas para actualizar los nuevos usuarios. Después de seleccionar el tipo de sincronización y realizar la configuración, haga clic en el botón CONFIRMAR SINCRONIZACIÓN.



9. Al terminar la configuración del directorio LDAP, en la ventana Importar, haga clic en el botón de confirmación

y en la ventana de configuración básica de LDAP haga clic en Guardar

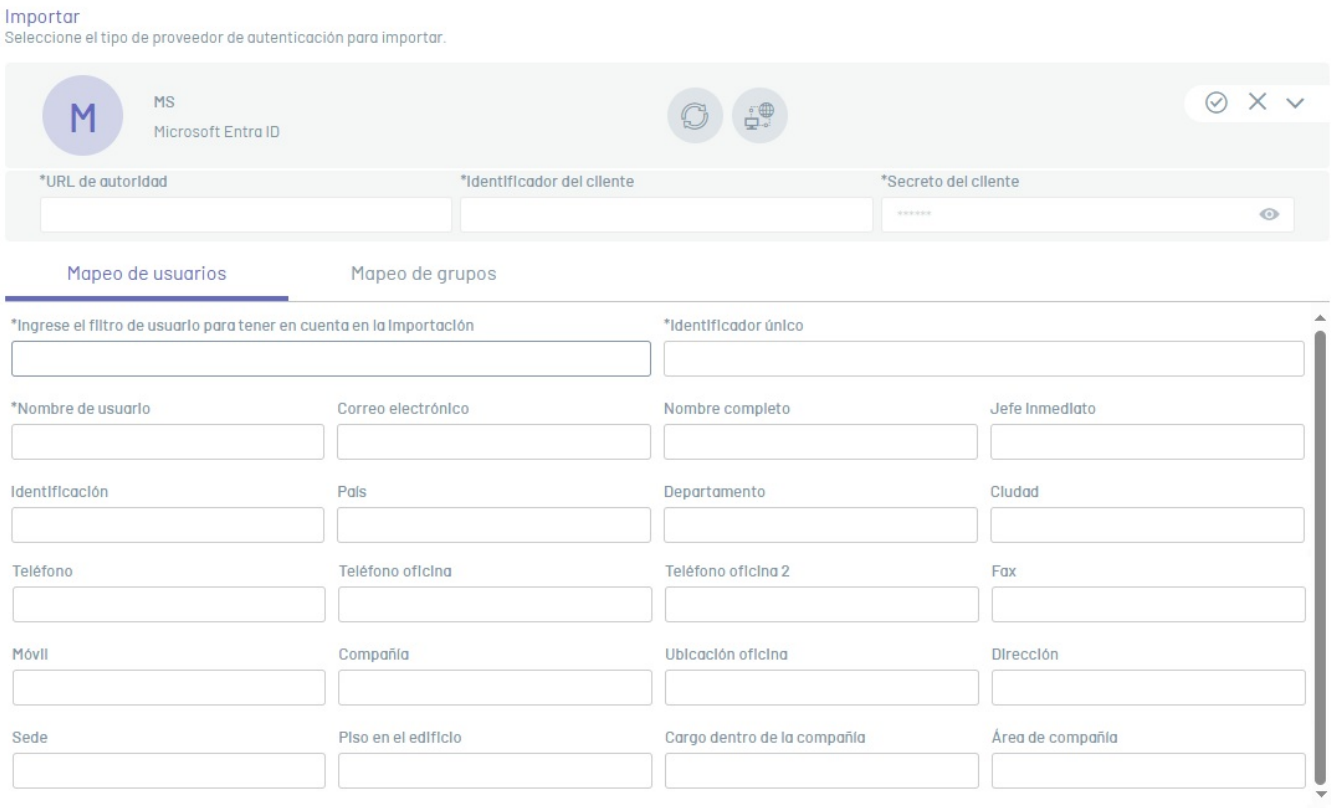


10. Terminada la sincronización, el administrador podrá asignar los roles respectivos a los usuarios sincronizados.

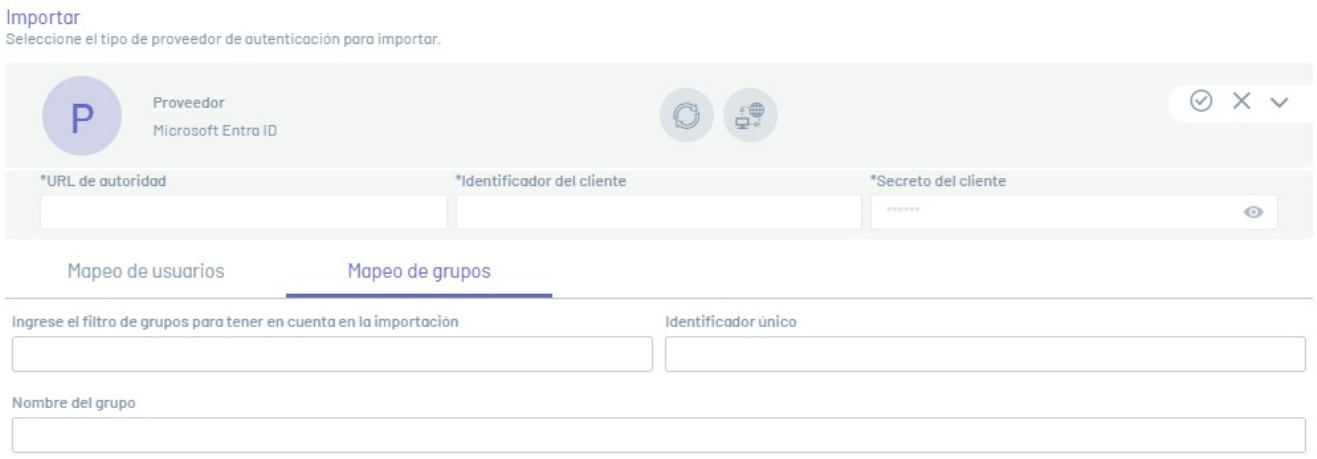
Proveedor Microsoft EntraID

1. En la vista detalle del proveedor, ingrese el nombre completo del directorio que desea sincronizar y haga clic en el botón IMPORTAR; se habilita la ventana Importar donde podrá ingresar los datos necesarios para la sincronización. En la información básica del directorio, ingrese los datos URL de autoridad, el identificador del cliente y el secreto del cliente suministrado por Microsoft EntraID.

En la pestaña Mapeo de Usuarios los campos obligatorios a registrar son:Filtro de usuario para la importación, identificador único y Nombre de usuario.



En la pestaña Mapeo de Grupos (grupos de usuarios) si digita algún valor en el campo “Ingrese el filtro de grupos para tener en cuenta en la importación“, los campos “Identificador único” y “nombre del grupo” se vuelven obligatorios.



Si desea conocer información acerca de los filtros de usuario y atributos para el mapeo de campos, puede consultar la documentación de Microsoft en los siguientes enlaces:

Filtro de usuarios y grupos
Campos de usuarios
Campos de grupos

⚐ Nota: : Puede consultar algunos filtros y mapeo de campos de ejemplo Microsoft EntraID

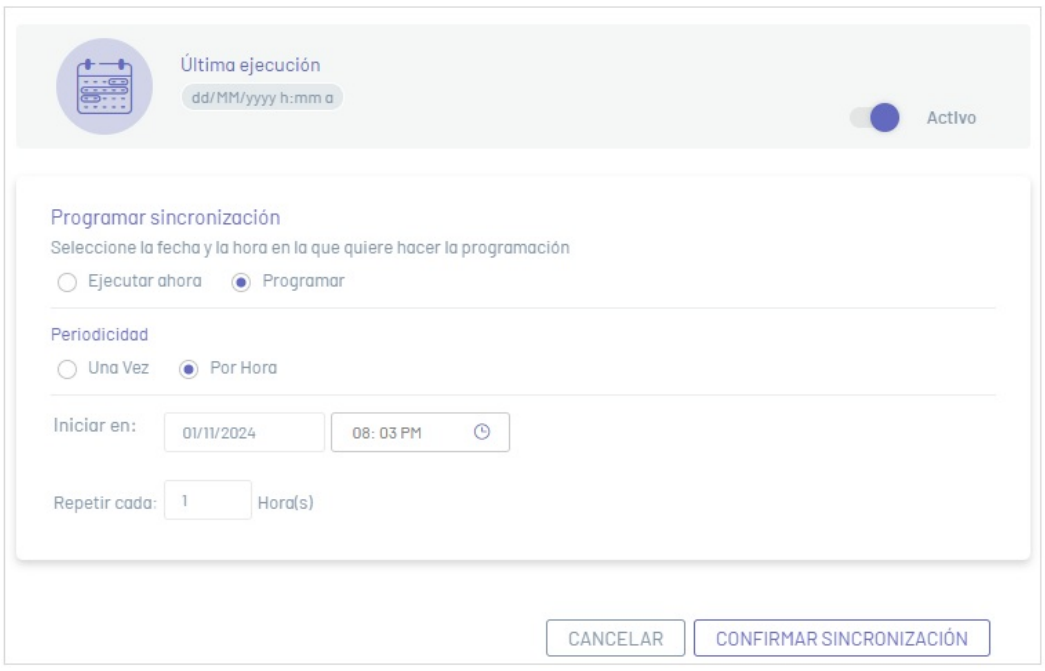
6. Al registrar los campos haga clic en el botón Probar conexión

. Si la conexión fue exitosa podrá visualizar el mensaje: La información quedó completa ya puedes finalizar la importación y se autoriza la continuación del proceso.

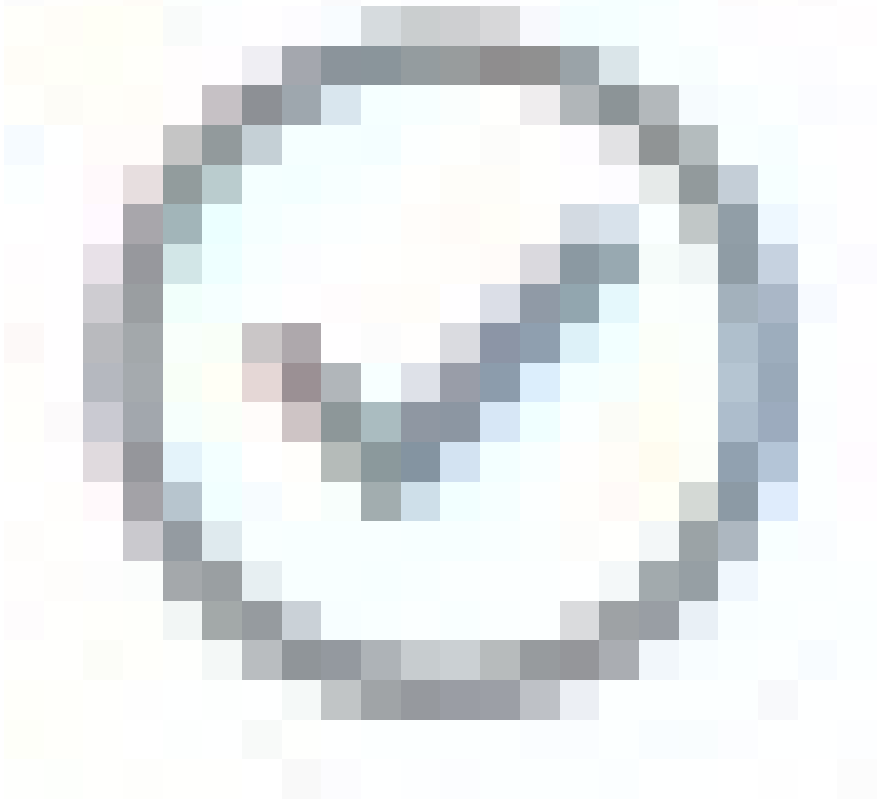
7. Al terminar de registrar la información, haga clic en el botón de sicronizar

y en la ventana que se habilita active la sicronización.

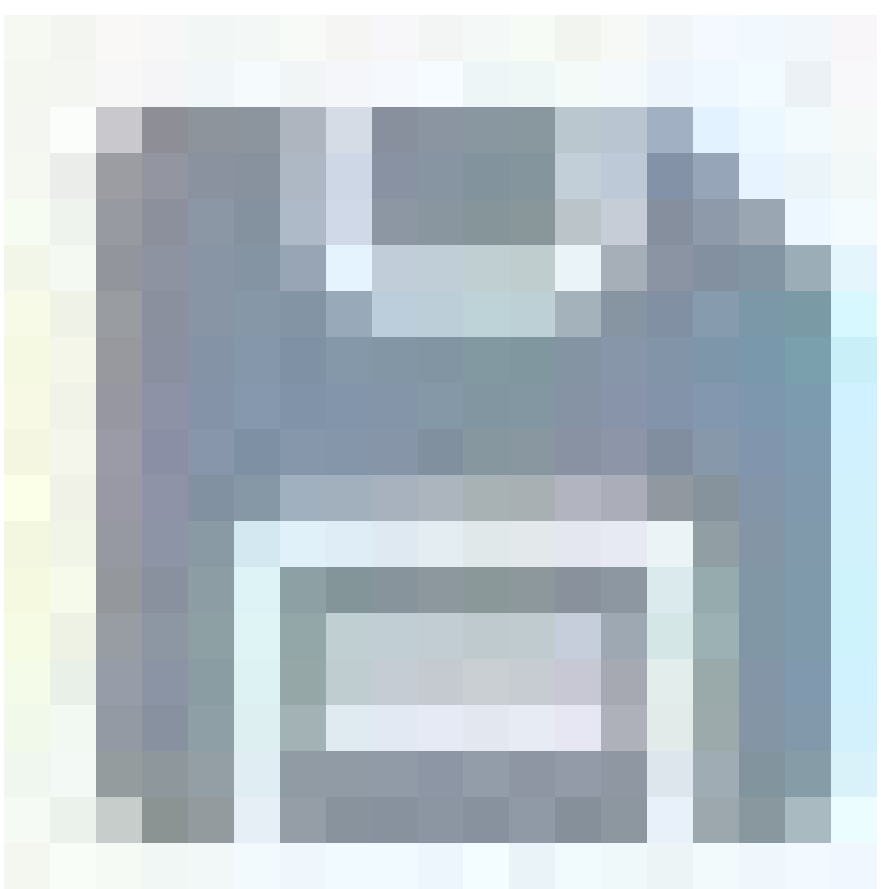
8. La sincronización puede ser manual (de inmediato) o se puede programar automáticamente una única vez o cada cierto número de horas. Después de seleccionar el tipo de sincronización y realizar la configuración, haga clic en el botón COFIRMAR SINCRONIZACIÓN.



9. Al terminar la configuración del directorio de Microsofrt Entra ID en la ventana Importar, haga clic en el botón de confirmación



y en la ventana de configuración básica del proveedor haga clic en Guardar

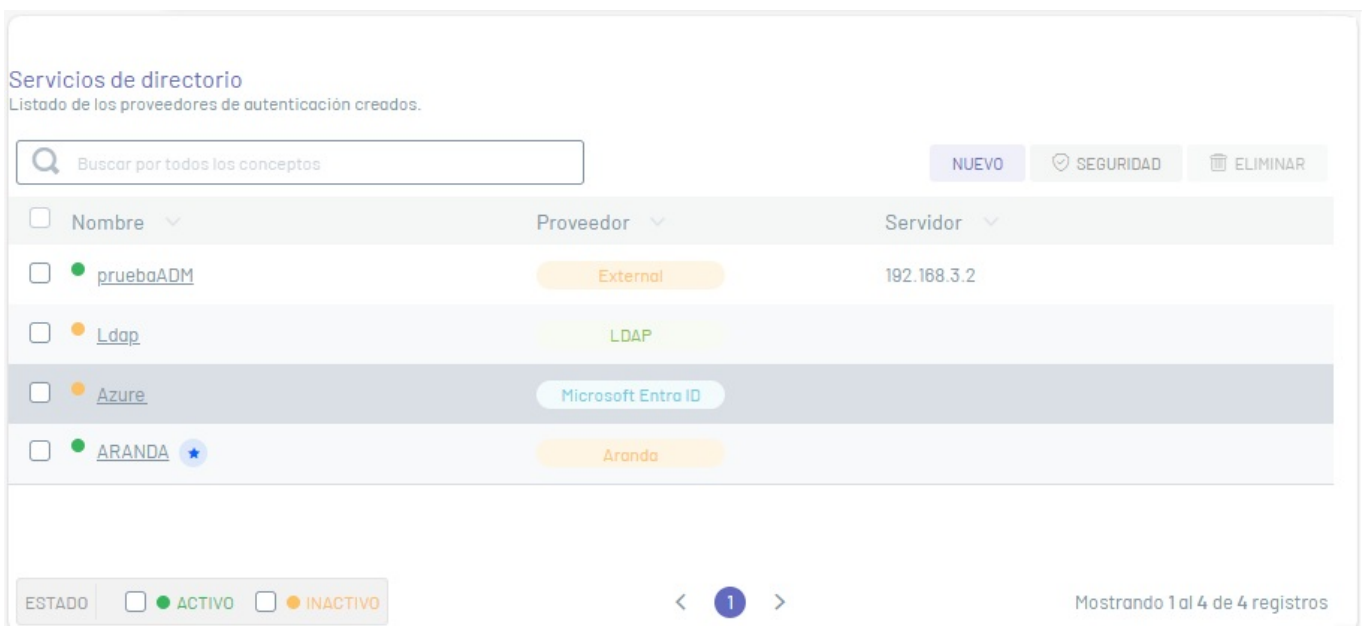


.

⚠ Importante: El proveedor Microsoft Entra ID sólo permite las sincronización de usuarios y grupos de usuarios, no aplica para ser utilizado como proveedor de autenticación, por lo que siempre queda en estado Inactivo. Para Acceder al sitio web de producto Aranda utilizando los usuarios de este tipo de directorio se debe configurar la autentica externa (SAML).

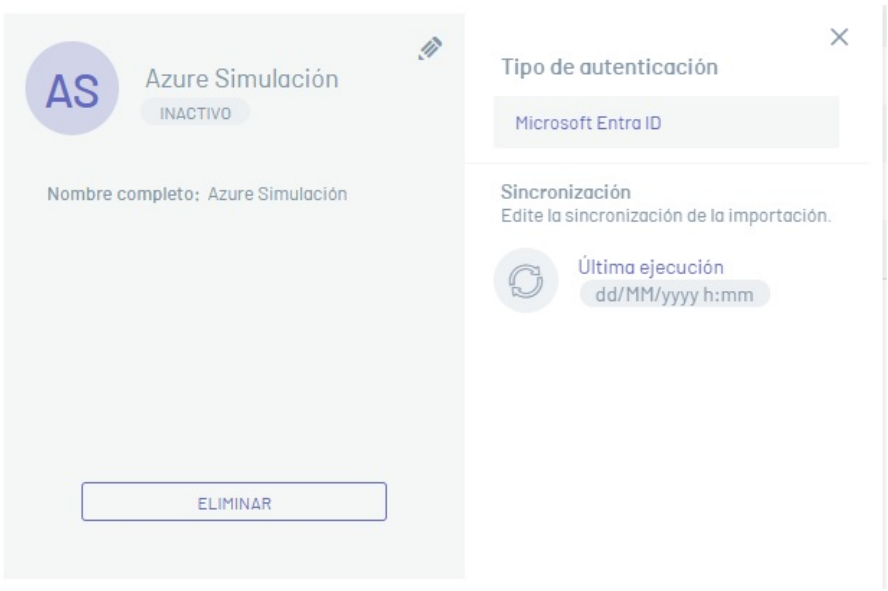
Editar Servicios de Directorio

1. Para editar un directorio o proveedor de autenticación, en la vista de información de servicios de directorios , seleccione un registro del listado de proveedores existentes.



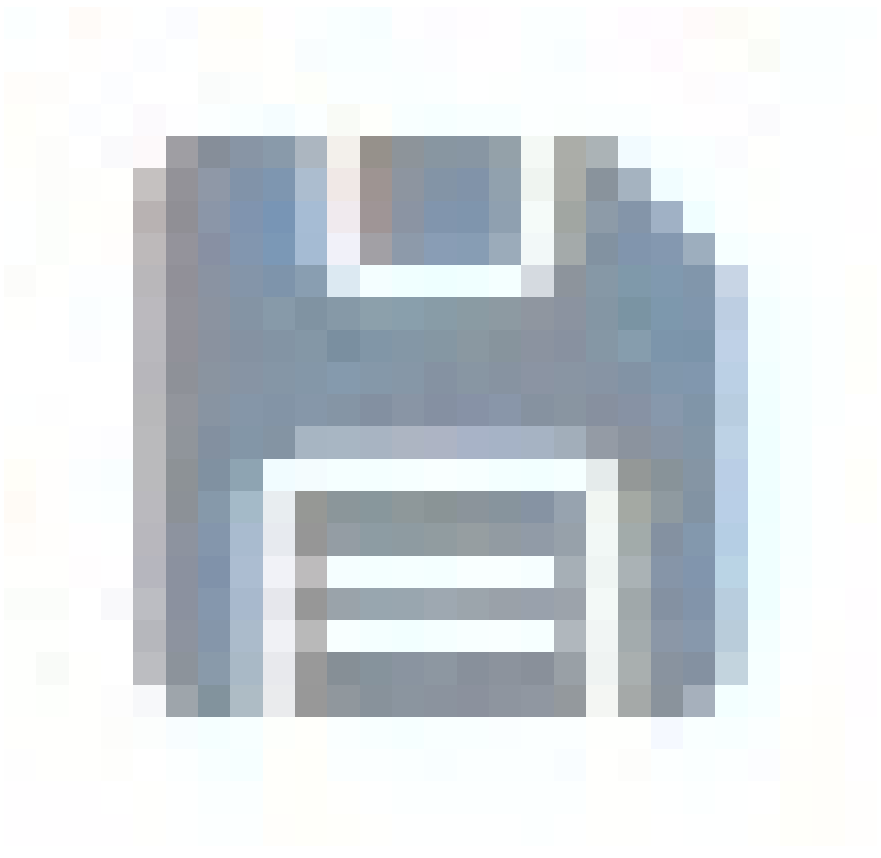
2. En la vista detalle haga clic en el ícono de editar

para modificar la información requerida.



3. En la ventana Edición de directorio podrá actualizar la información básica y la información importada del proveedor.

4. Al terminar de editar el usuario, haga clic en el ícono Guardar



para confirmar los cambios realizados.

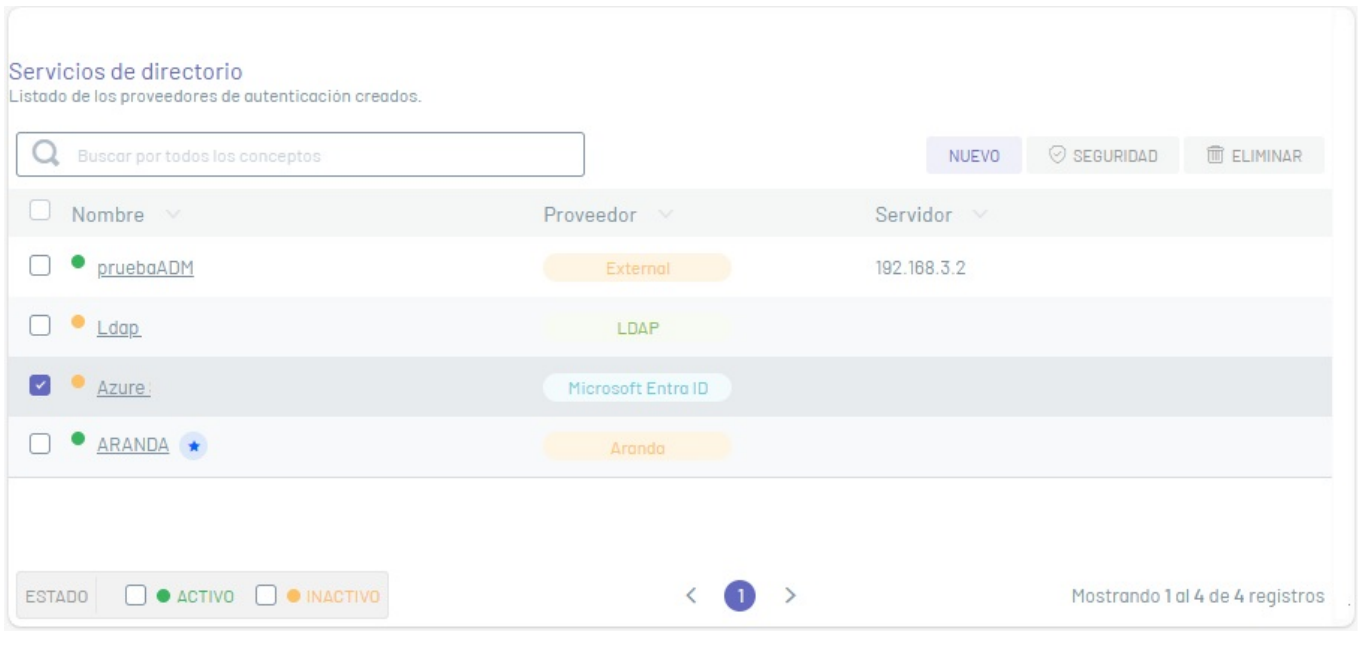
Eliminar Servicios de directorio

La eliminación de los registros de servicios de directorios se puede realizar de dos formas:

1. En la vista de información de servicios de directorios seleccione un registro del listado de servicios de directorios o proveedores de autenticación que desea eliminar y

haga clic en el botón

.



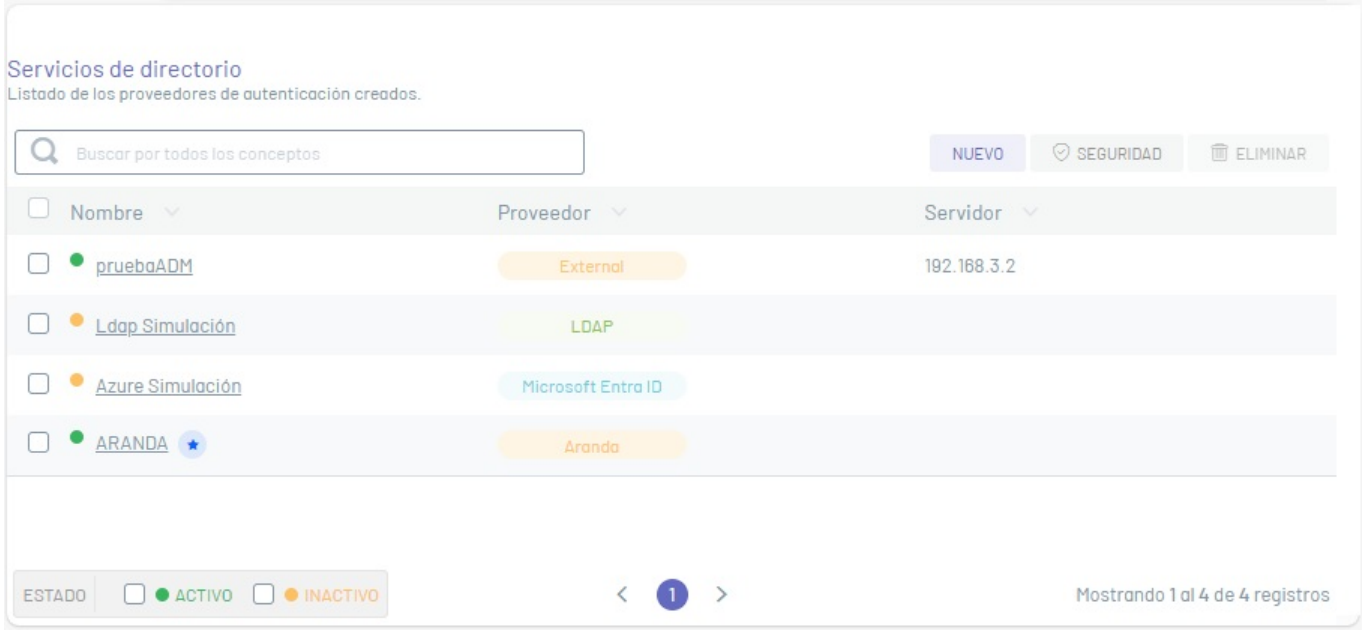
2. En la vista de detalle de un servicio de directorio o proveedor seleccionado que desea eliminar, haga clic en el botón ELIMINAR

3. En ambos casos podrá visualizar un mensaje de confirmación para validar la acción de borrado.

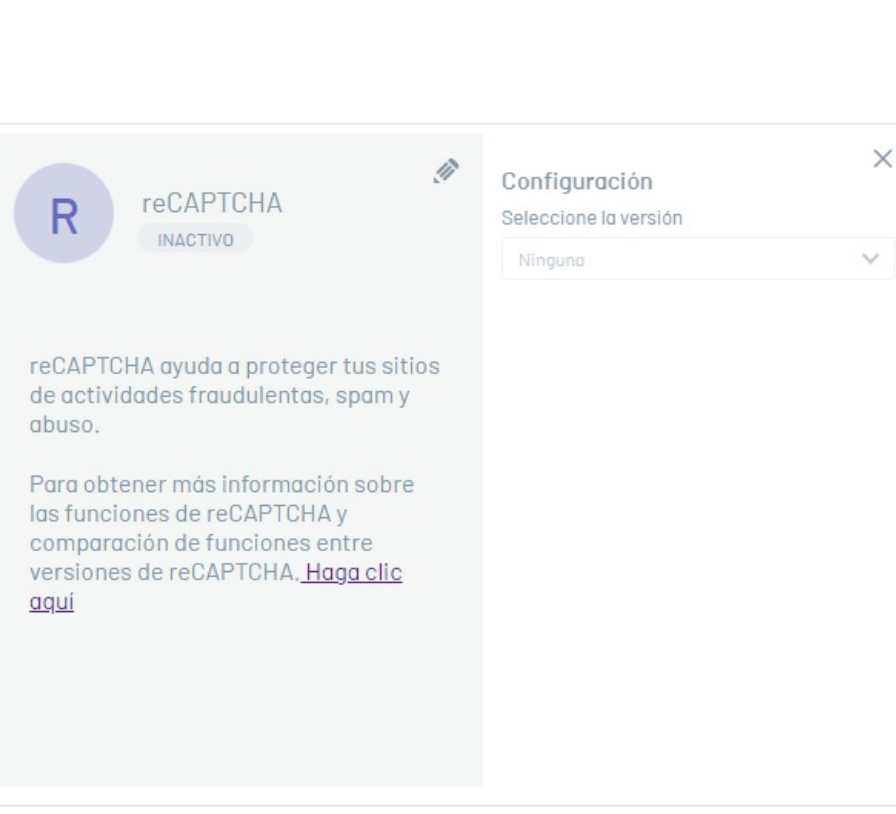
Configuración Seguridad reCAPTCHA

⚠ Importante: La configuración de reCAPTCHA es un componente Opcional que lo podrá implementar en la gestión de proveedores de servicios de directorio, si requiere esta condición de autenticación.

1. Para realizar la configuración de reCAPTCHA, en la vista de información de servidores de directorios, seleccione el botón



2. Se habilita la ventana reCAPTCHA donde podrá configurar este componente. Haga clic en el botón Editar



2. Seleccione la versión requerida, de acuerdo al tipo de clave configurado en Google y complete la información solicitada:

Campo	Tipo Campo	Descripción
Versión	Selector	Versión configurada en Google.
Clave de sitio	Texto	Clave pública obtenida de la configuración realizada en Google.
Clave secreta	Texto	Clave secreta obtenida de la configuración realizada en Google.
Puntuación	Texto	Si elige versión V3, defina la puntuación para la calificación del usuario

⚐ Nota: Al cambiar la versión de reCAPTCHA, será necesario volver a diligenciar los campos solicitados o cancelar la operación.

Configuración para reCAPTCHA V2 y V3

Precondiciones

Crear claves de reCAPTCHA para sitios web

- Registrarse en Google.
- Prepara tu entorno para reCAPTCHA Enterprise.
- Asegúrese de tener el rol de Identity and Access Management: Administrador de reCAPTCHA Enterprise (roles/recaptchaenterprise.admin)
- Define el tipo de clave que mejor se adapte a al caso de uso.

Configurar tokens para recaptcha de google

Información necesaria para configuración

⚐ Nota: Se requiere tener una cuenta google previamente creada y un entorno para reCAPTCHA Enterprise: Para crear consola Google Cloud y Google Cloud project: Ir a Google Cloud

Habilita la API de reCAPTCHA Enterprise

1. En la consola de Google Cloud, ingrese a la página del API de reCAPTCHA Enterprise
2. Verifique que el nombre del proyecto aparezca en el selector de proyectos en la parte superior de la página. Si no visualiza el nombre del proyecto, haga clic en el selector de proyectos y seleccione el proyecto requerido.
3. Haga clic en Habilitar.

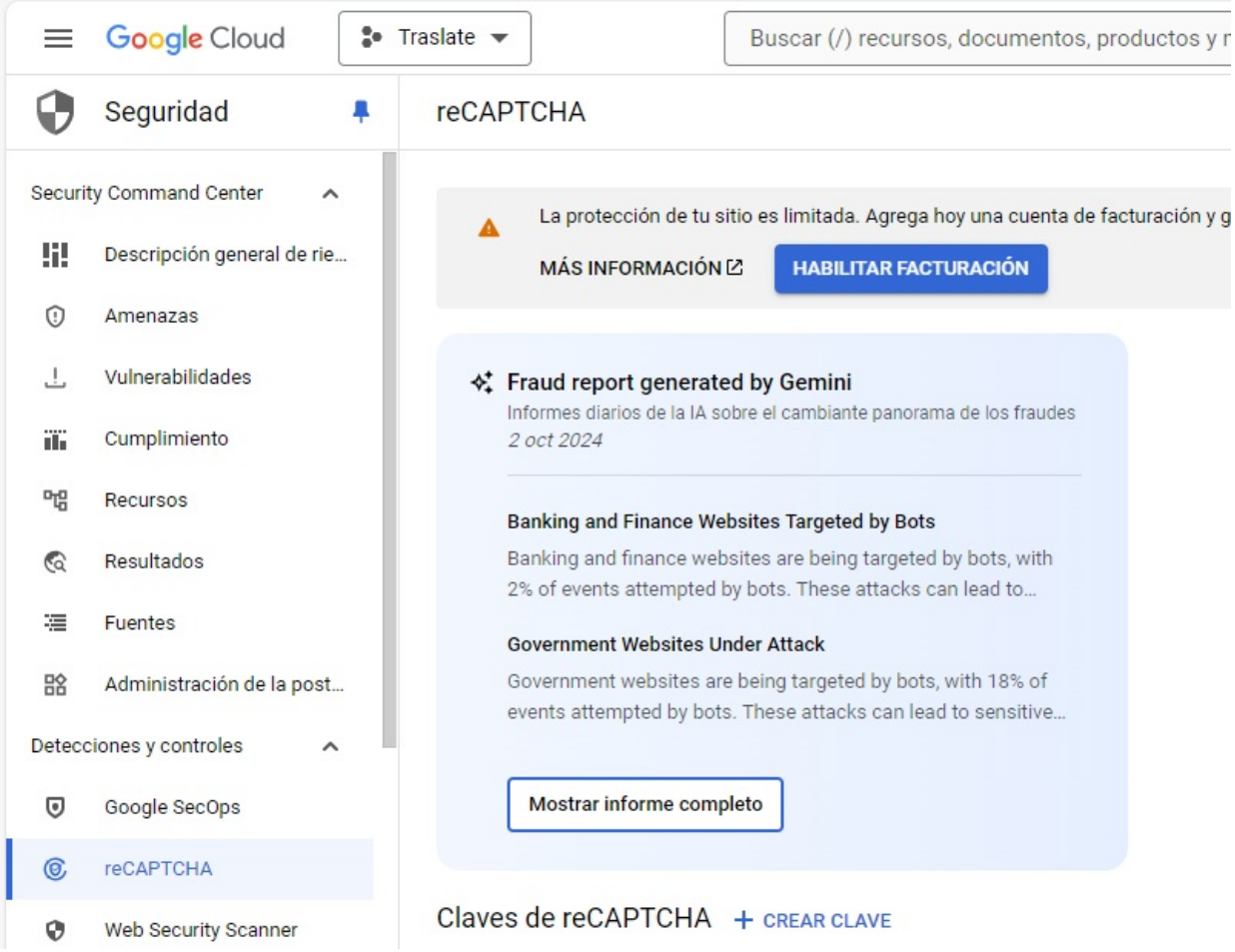
⚐ Nota: Se realiza redireccionamiento en la página, donde se permitirá la creación de las credenciales.

Crear claves de reCAPTCHA

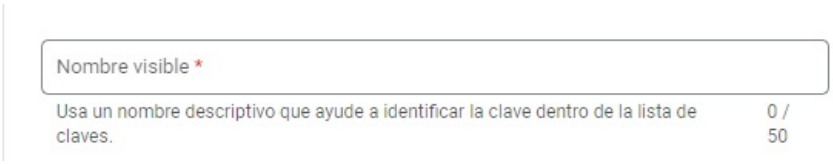
1. En la consola de Google Cloud, ingrese a la página de reCAPTCHA Enterprise.
2. Verifique que el nombre del proyecto aparezca en el selector de recursos en la parte superior de la página.

⚐ Nota: En caso de no visualizar el nombre del proyecto, haga clic en el selector de recursos y seleccione el proyecto requerido.

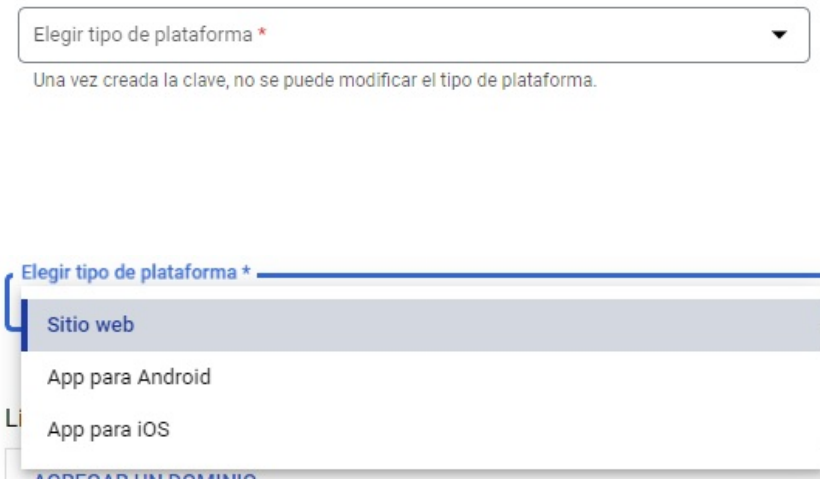
3. Haga clic en Crear clave.



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



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



⚐ Nota: Aparecerá la sección Lista de dominios.

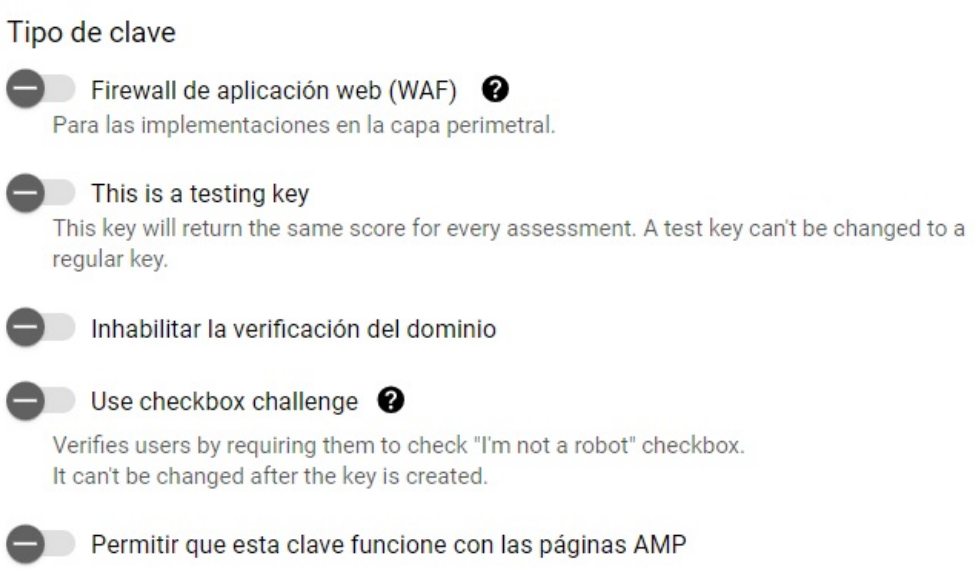
6. Ingrese el nombre de dominio del sitio web:

- 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: Crear una clave basada en puntuaciones es la opción predeterminada en la consola de Google Cloud".

- reCAPTCHA basada en puntuaciones:

- Con el objetivo de proteger la clave de reCAPTCHA para dominio y subdominios, valide que la opción Inhabilitar la verificación del dominio esté desactivada.
  Si requiere que la clave basada en puntuaciones funcione con Accelerated Mobile Pages (AMP), active el botón **Inhabilitar la verificación del dominio es un riesgo de seguridad porque no hay restricciones en el sitio, en consecuencia cualquier persona podrá acceder a la clave de reCAPTCHA y usarla.



- 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.
<img src="/common/assets/images/configurar_recaptcha/img9.png" >
- Haga clic en **Crear clave**.
<img src="/common/assets/images/configurar_recaptcha/img10.png" >

⚐ Nota: La nueva clave aparecerá en la página de claves de reCAPTCHA.

⚐ Nota: No se recomienda utilizar claves de casilla de verificación, ya que aumentan la fricción del usuario y no mejoran la exactitud.

- reCAPTCHA con casillas de verificación:
- Expande la sección Firewall de aplicación web (WAF), verificación del dominio, páginas de AMP y desafío.

<img src="/common/assets/images/configurar_recaptcha/img7.png" >

- Con el objetivo fin de proteger la clave de reCAPTCHA para dominio y subdominios, confirme que la opción Inhabilitar la verificación del dominio esté desactivada. Inhabilitar la verificación del dominio es un riesgo de seguridad porque no hay restricciones en el sitio, por lo que cualquier persona puede acceder a la clave de reCAPTCHA y usarla.

<img src="/common/assets/images/configurar_recaptcha/img8.png" >

- Habilite el botón de activación Usar el desafío de la casilla de verificación.

<img src="/common/assets/images/configurar_recaptcha/img12.png" >

- Seleccione la opción Seguridad del desafío adecuada.
- Para un entorno que no es de producción, si requiere especificar una puntuación que muestre la clave cuando se generen las evaluaciones para ella, ten en cuenta lo siguiente::

- Haga clic en el botón de activación **Esta es una clave de prueba.**.
- En el cuadro **Score**, especifica una puntuación entre 0 y 1.0.
- Seleccione la opción **Tipo de desafío** adecuada.

- En algunas ocasiones, el desafío aparece como **automático**.
- **Ningún CAPTCHA** no muestra un desafío.
- Un **desafío sin resolver** muestra las imágenes, pero el desafío no se aprueba.

<img src="/common/assets/images/configurar_recaptcha/img13.png" > - Haga clic en **Crear clave**.

<img src="/common/assets/images/configurar_recaptcha/img10.png" >

⚐ Nota: La nueva clave aparecerá en la página de claves de reCAPTCHA.

⚐ Nota:

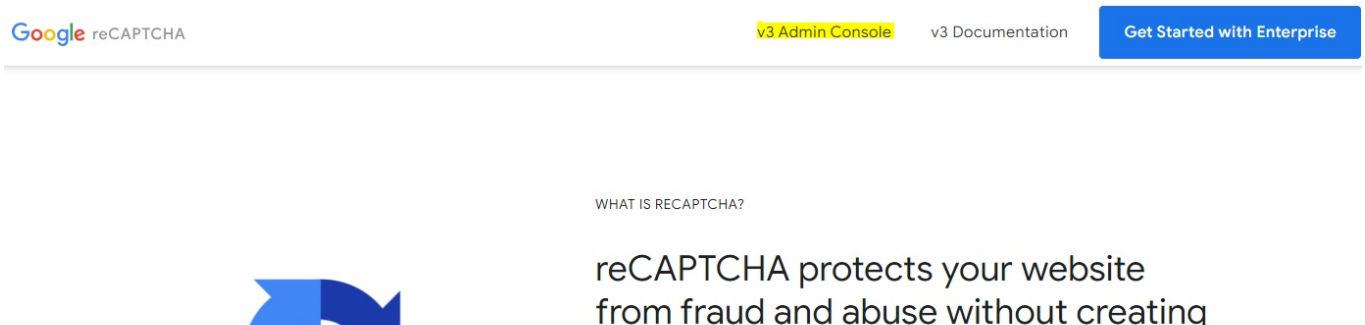
- La opción de seguridad del desafío controla la probabilidad de solicitar a un usuario un desafío secundario para seleccionar imágenes según una categoría identificada (por ejemplo, seleccione las imágenes con una motocicleta o escaleras).
- Para asegurar una mejor protección antifraude, selecciona (más seguro contra bots)**.
- En caso de seleccionar la opción Dificultad del desafío más simple, es menos probable que se les solicite a los usuarios el desafío visual.

⚐ Nota: Nota: Después de crear las claves de reCAPTCHA, podrá editarlas o borrarlas. No podrá recuperar las claves borradas.

Configurar reCAPTCHA V2

reCAPTCHA Versión 2

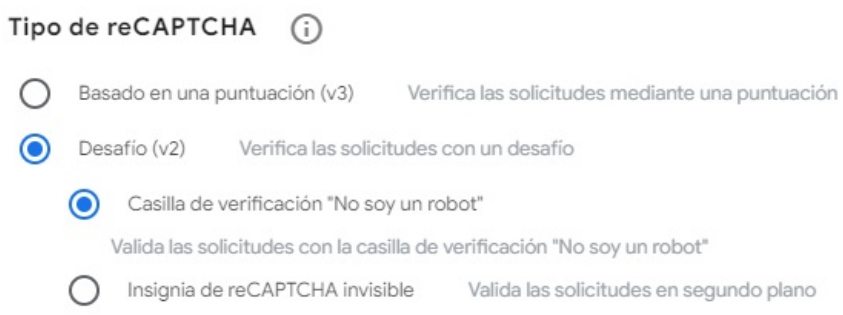
1. Estando registrado en google ingrese a la administración de reCAPTCHA



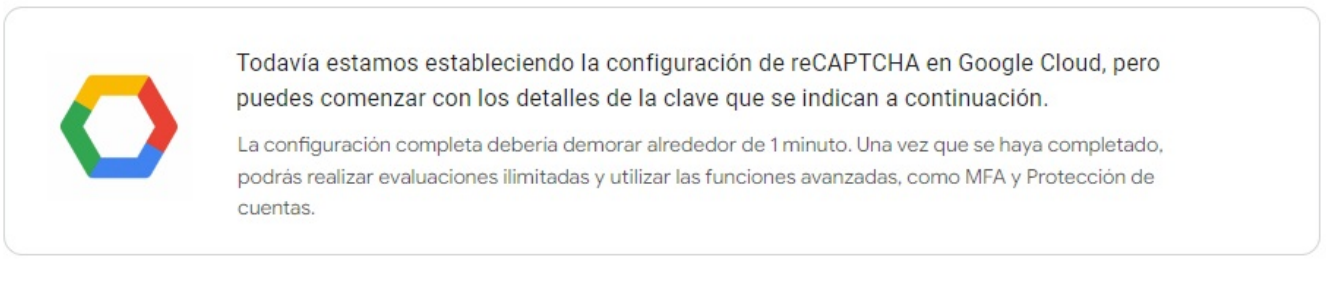
2. Agregue el valor del campo Etiqueta

3. En la pantalla que se habilita seleccione **Desafío (v2)** y según la configuración deseada:

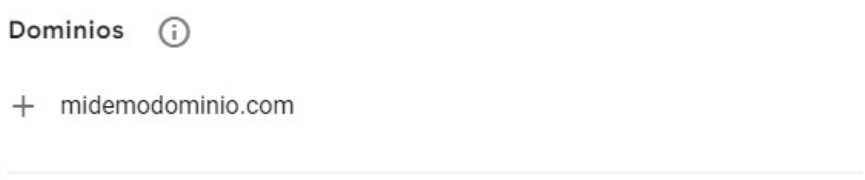
- Marque la opción "Casilla de verificación "No soy un robot""
- Marque la opción "Insignia de reCAPTCHA invisible"



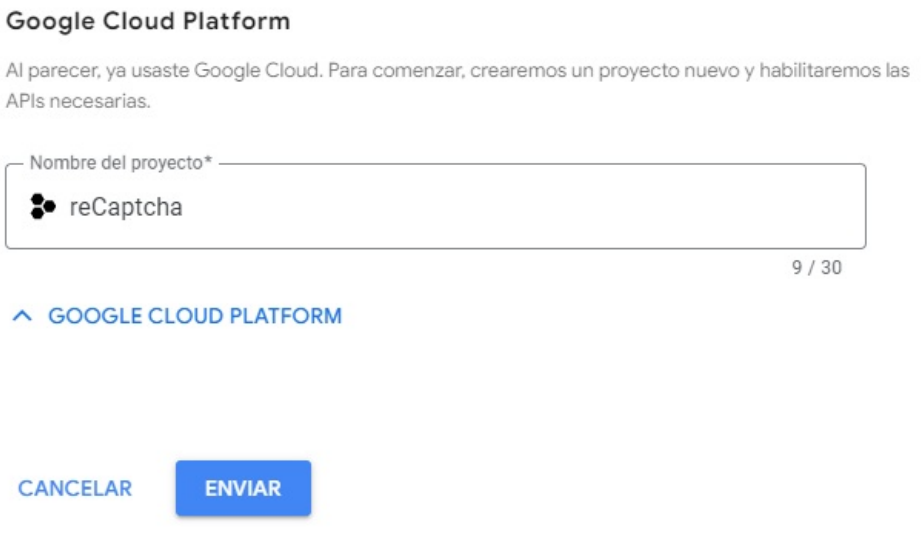
⚐ Nota: Podrá visualizar una notificación de configuración del sitio; espere a que se habiliten las opciones para continuar:



4. Agregue el valor del campo Dominios.



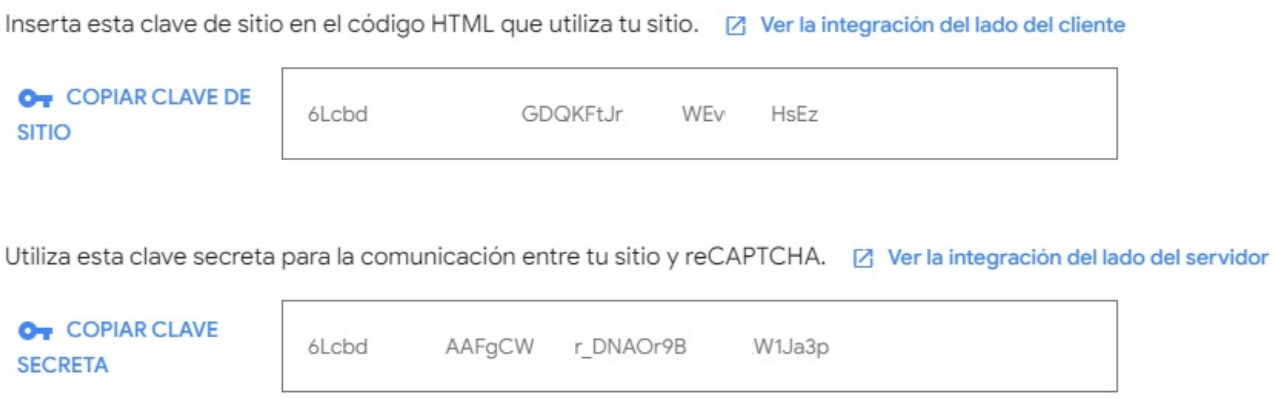
5. Seleccione el nombre del proyecto y haga clic en Enviar.



⚐ Nota: La página mostrará automáticamente las claves del sitio, para realizar posteriormente la configuración en el componente de DirectoryServices

6. Copie la información que se visualiza en los campos:

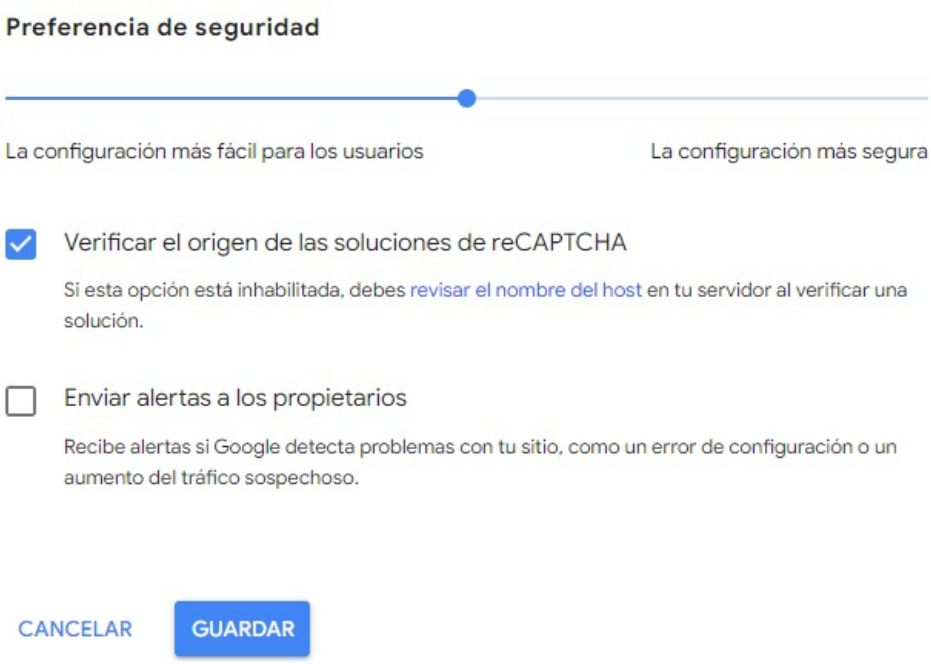
- Clave del sitio.
- Clave secreta.



7. Después de guardar o configurar las claves, haga clic en el botón "IR A CONFIGURACIÓN"

⚐ Nota: Verifique en la página que se habilita que la información presentada, corresponde con los valores diligenciados previamente.

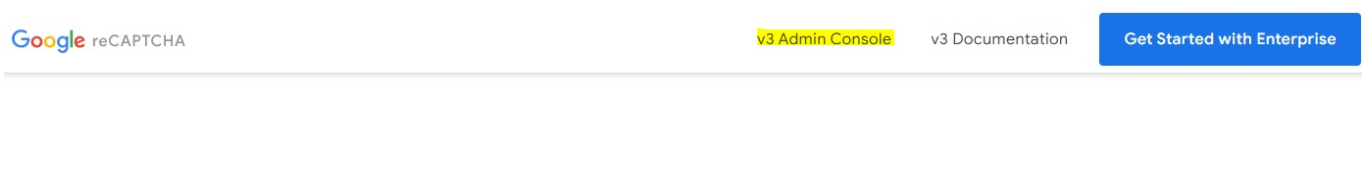
8. Valide y configure la Preferencia de seguridad según lo requiera y haga clic en el botón Guardar



Configurar reCAPTCHA V3

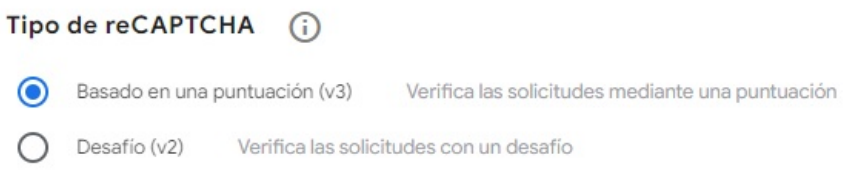
reCAPTCHA Versión 3

1. Estando en registrado en google ingrese a la administración de reCAPTCHA

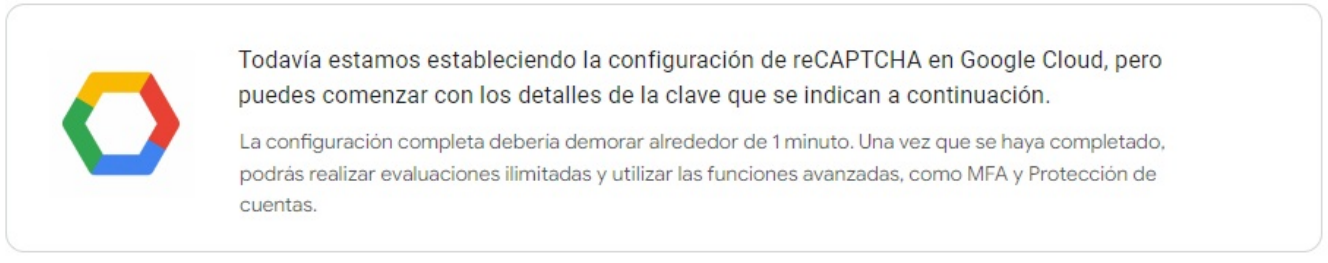


2. Agregue el valor del campo Etiqueta

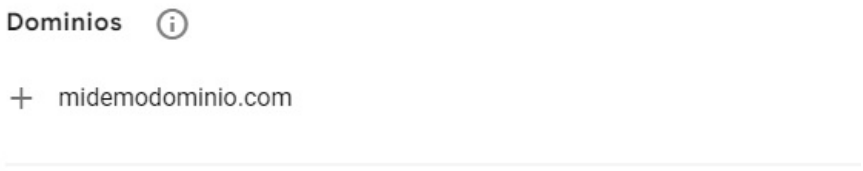
3. En la pantalla que se habilita seleccione Basado en una puntuación (v3) y según la configuración deseada:



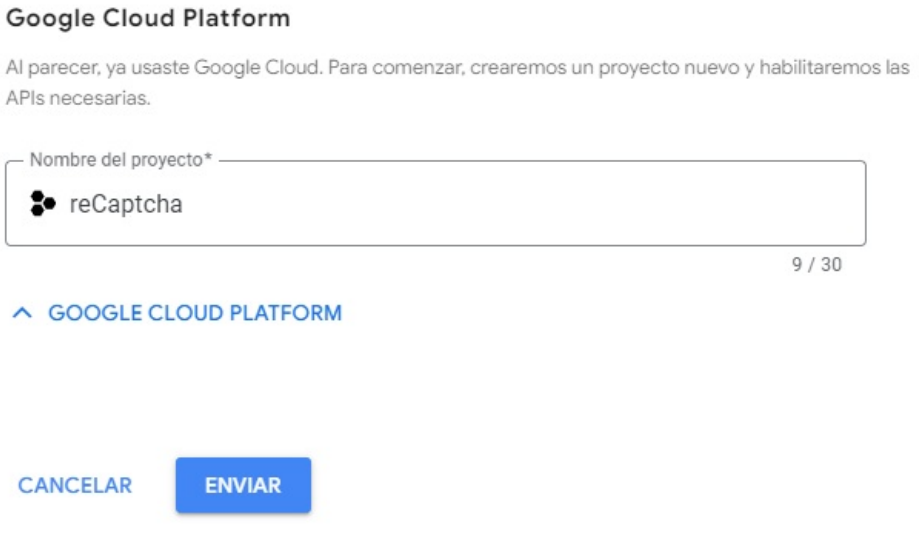
⚐ Nota: Al visualizar la notificación de configuración del sitio, espere que se habiliten las opciones para continuar:



4. Agregue el valor del campo Dominios.



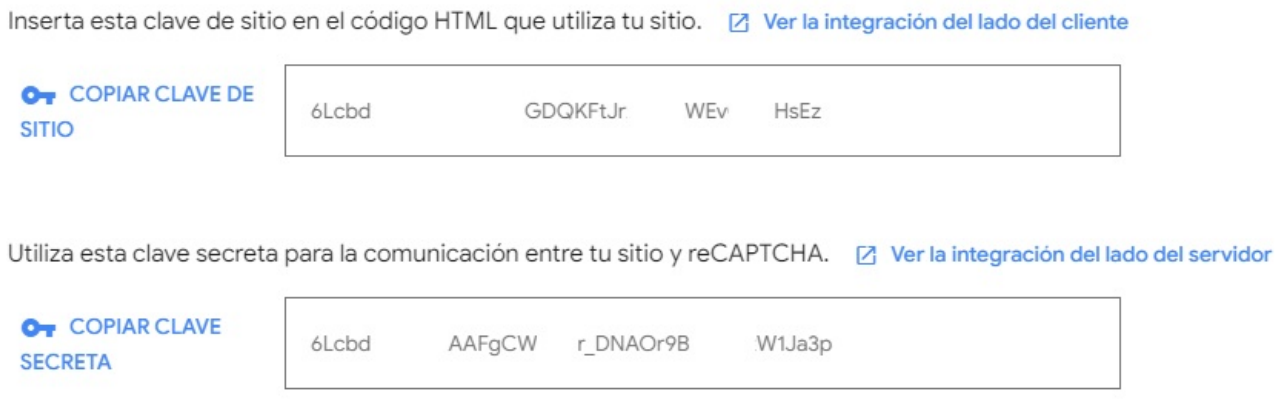
5. Seleccione el nombre del proyecto y haga clic en Enviar.



⚐ Nota: La página mostrará automáticamente las claves del sitio, para realizar posteriormente la configuración en el componente de DirectoryServices

6. Copie la información que se visualiza en los campos:

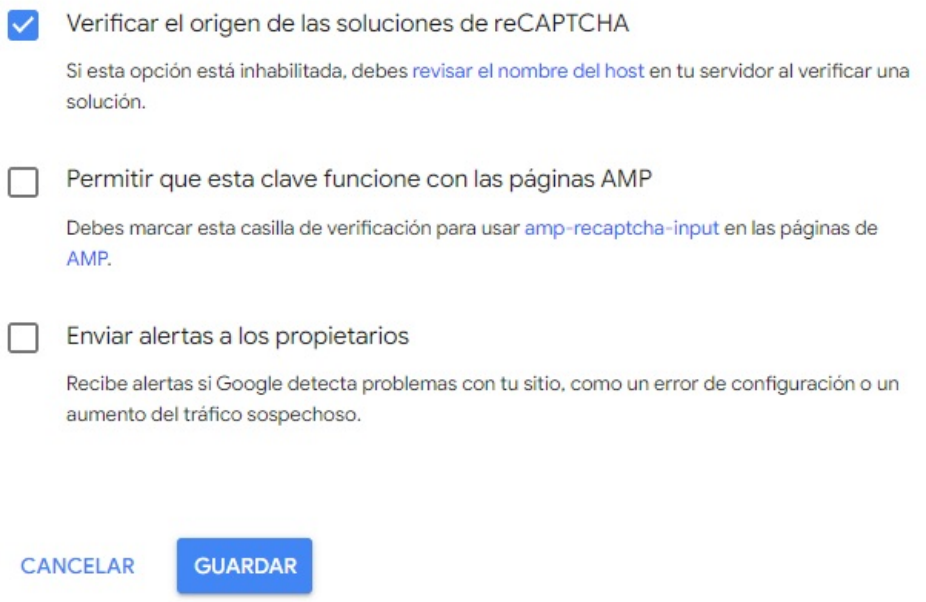
- Clave del sitio.
- Clave secreta.



7. Después de guardar o configurar las claves haga clic en el botón "IR A CONFIGURACIÓN"

⚐ Nota: Verifique en la página que se habilita que la información presentada, corresponde con los valores diligenciados previamente.

8. Valide y configure la Preferencia de seguridad según lo requiera y haga clic en el botón Guardar

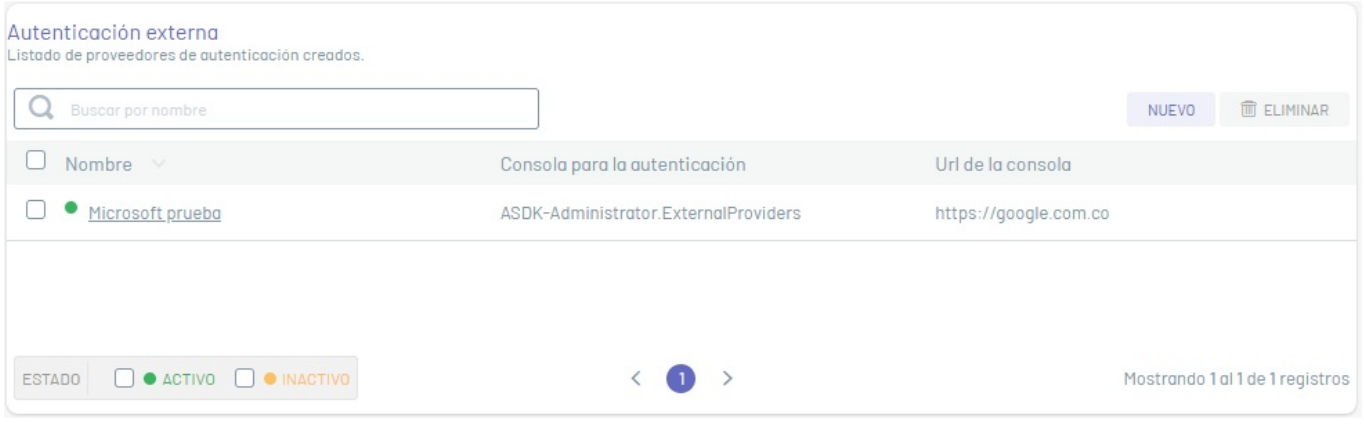


Módulo Autenticación Externa

Gestión de Proveedores Externos

Visualizar proveedores externos

1. En la vista de información de proveedores externos podrá visualizar el listado de proveedores registrados, agrupados por datos como:



Campo	Tipo Campo	Descripción
Nombre	Texto	Nombre con el cual se identifica el proveedor.
Consola para la autenticación	Texto	Indica el tipo de consola que se desea integrar.
Url de la consola	Texto	Es la url pública de la consola, este valor se debe proporcionar al proveedor de autenticación como identificador (Id de entidad).

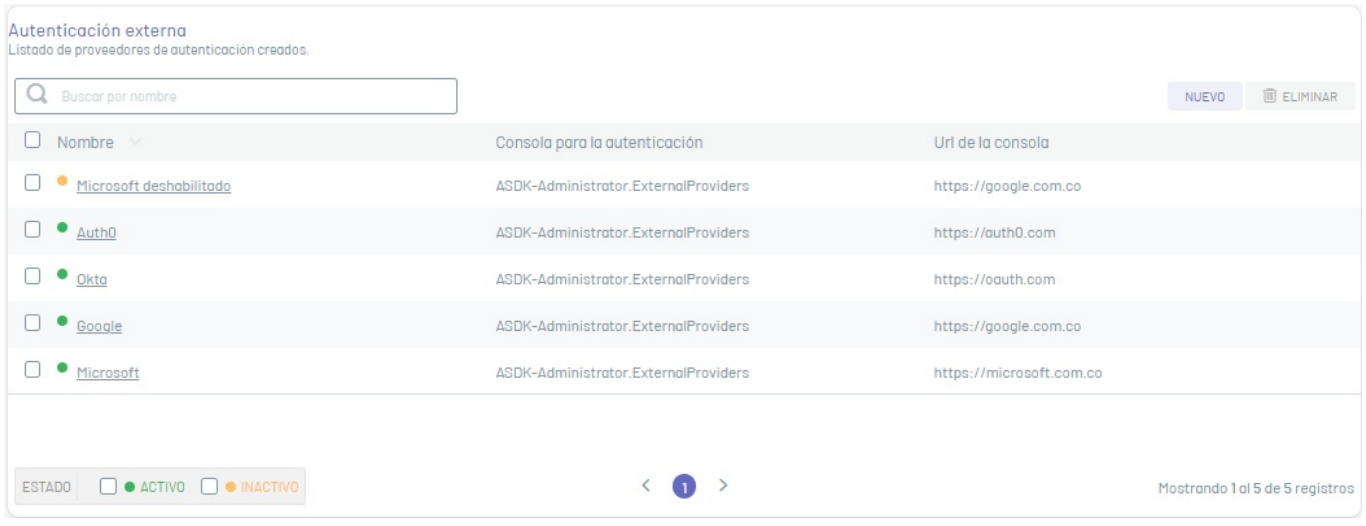
2. En la vista de información de proveedores externos, tendrá habilitadas acciones de gestión y organización de la información.Vista de Información en Entorno Commons

Enlaces Relacionados:

- Crear proveedor externo
- Editar proveedor externo
- Eliminar proveedor externo

Crear Proveedor Externo

1. Para crear un nuevo proveedor externo, en la vista de información de proveedores, haga clic en el botón Nuevo.



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

Datos Básicos

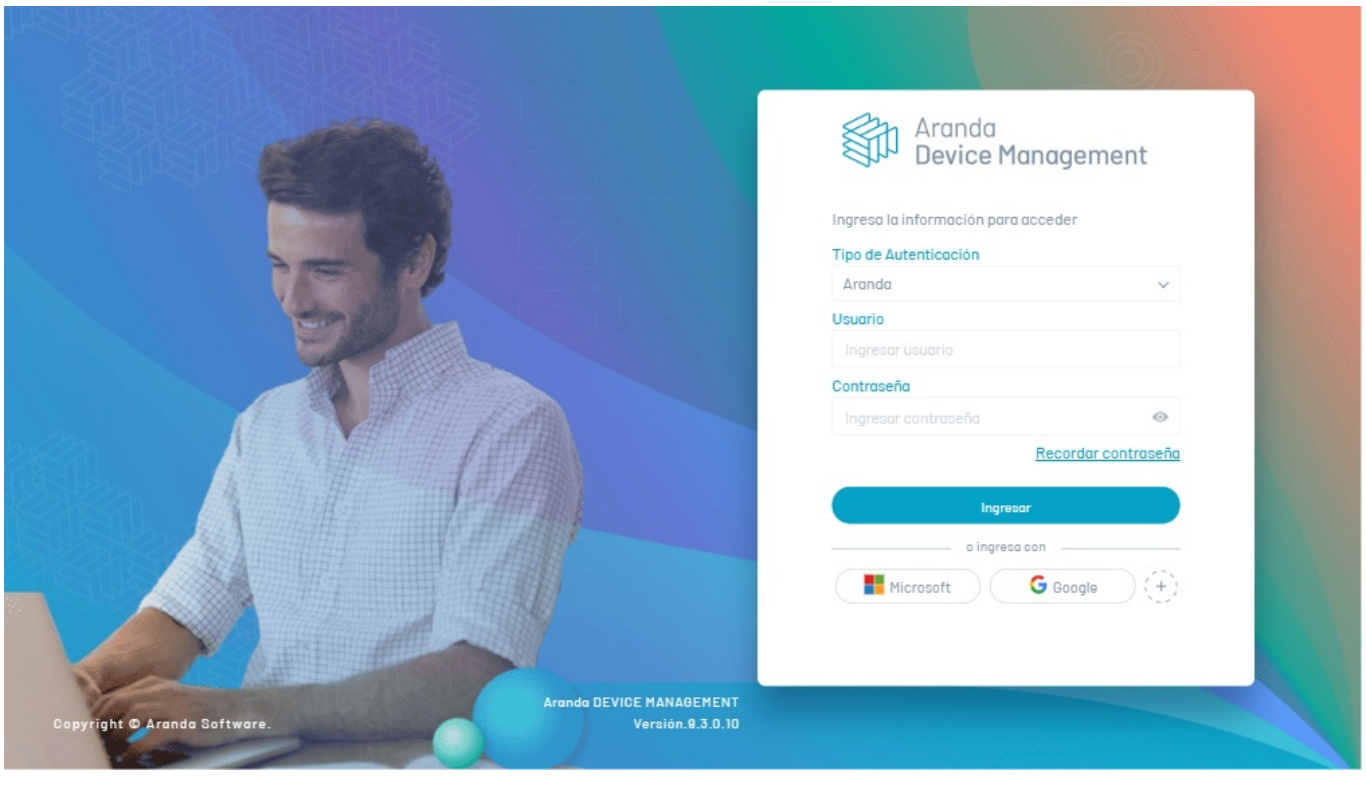
2. En la ventana que se habilita podrá completar los datos básicos del proveedor externo como nombre de proveedor, URL de la consola, URL inicio de sesión, URL cerrar sesión, estado, ícono y texto del proveedor, entre otros.
Cada uno de los campos de proveedor externo deben tener en cuenta las especificaciones para campos

⚐ Nota: Los campos URL inicio de sesión y URL cerrar sesión cuentan con funcionalidad de autocompletado y se basa en la información que se suministra en el campo URL de la consola.

4. Al terminar de configurar la autenticación de proveedores, haga clic en el botón de Guardar.

⚐ Notas:

- Si la configuración es exitosa, en la vista de proveedores externos podrá visualizar los registros de los últimos proveedores creados.
- En la pantalla de inicio y acceso a la aplicación requerida, podrá visualizar el ícono con el nombre dado al proveedor externo.

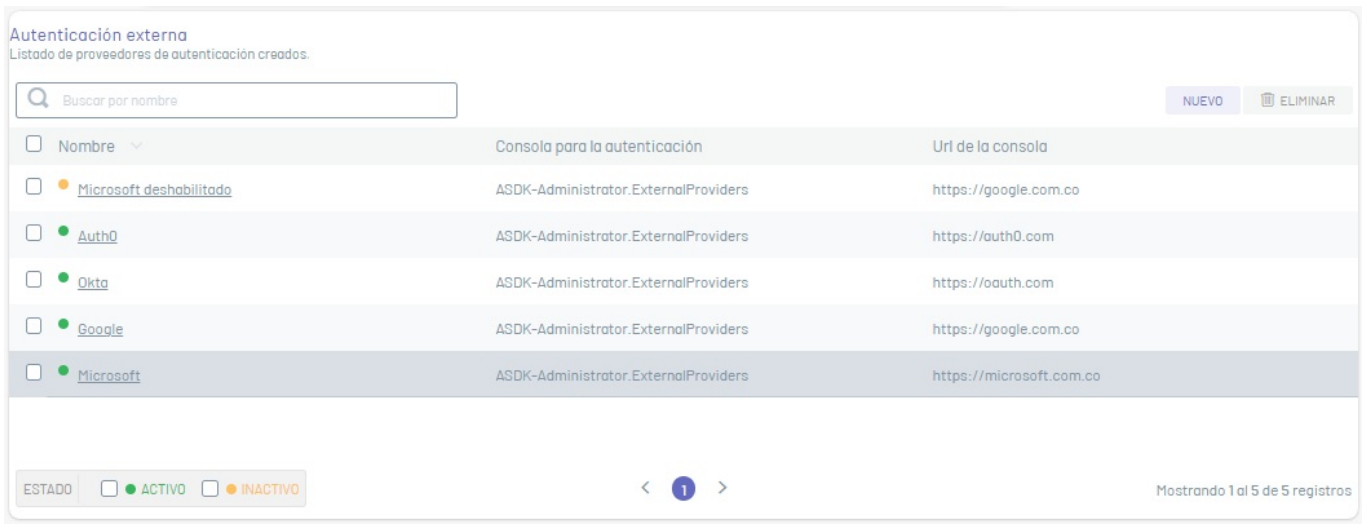


⚐ Notas:

- El correo con el que se realiza la autenticación desde el proveedor externo es utilizado como la identificación del usuario y debe estar registrado en la aplicación respectiva.
- Para que el sitio web pueda autenticar al usuario, este debe ser importado o creado antes de realizar la configuración de autenticación externa.

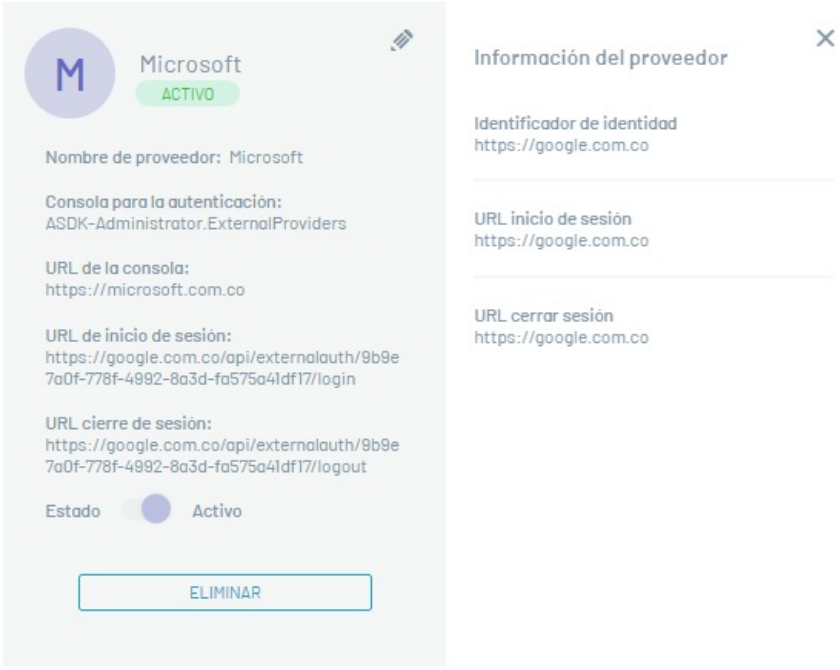
Editar Proveedor Externo

1. Para modificar un proveedor externo, en la vista de información de proveedores externos seleccione un registro del listado de proveedores existentes.

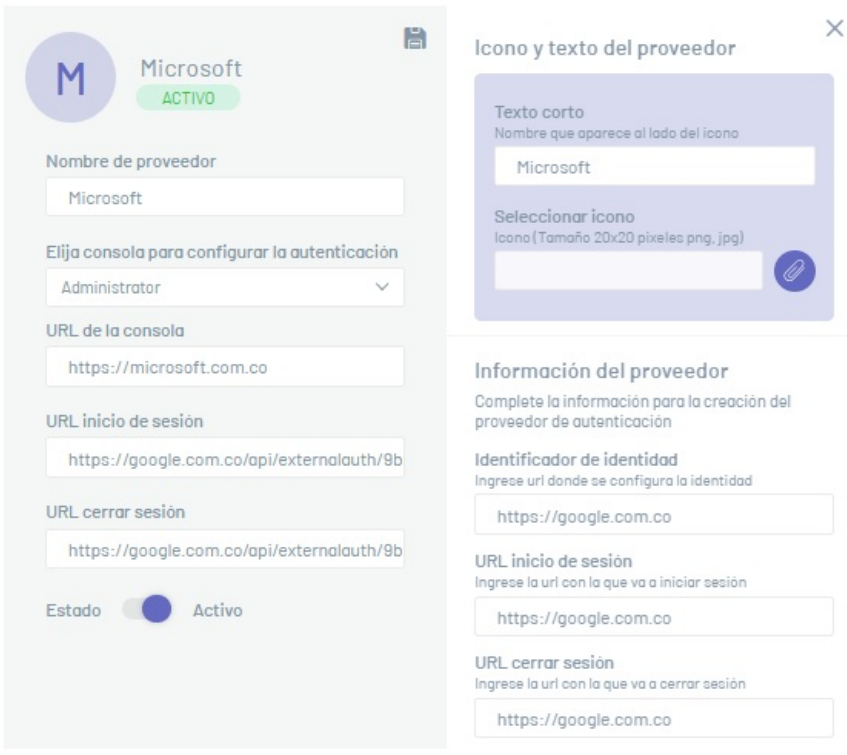


2. En la vista de detalle del proveedor, haga clic en el ícono Editar

y modifique la información requerida.



3. En la ventana Edición de proveedores externos podrá actualizar la información básica del proveedor.



⚐ Nota: El valor del campo Seleccionar ícono no se va a ser visible en vista de edición, sin embargo si no se realiza cambios a este campo la imagen que se haya guardado cuando se creo el proveedor se debe mantener.

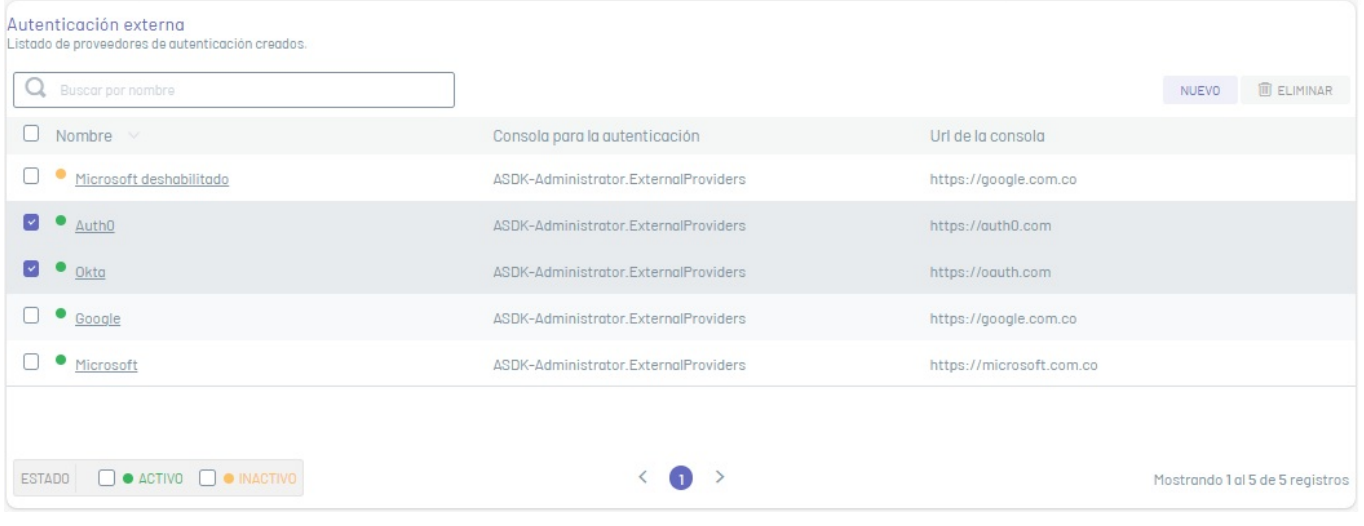
4. Al terminar de editar el proveedor externo, haga clic en el ícono Guardar

para confirmar los cambios realizados.

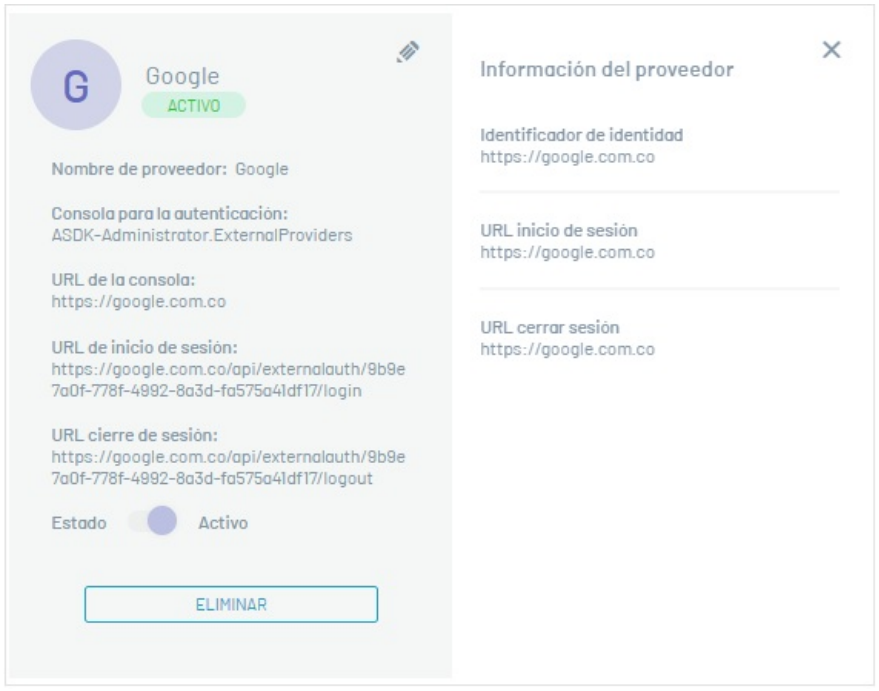
Eliminar Proveedor Externo

La eliminación de los registros de proveedores externos se puede realizar de dos formas:

1. En la vista de información de proveedores externos seleccione un registro del listado de proveedores que desea eliminar y haga clic en el botón



2. En la vista de detalle de un proveedor seleccionado que desea eliminar, haga clic en el botón ELIMINAR



3. En ambos casos podrá visualizar un mensaje de confirmación para validar la acción de borrado.

⚐ Nota:

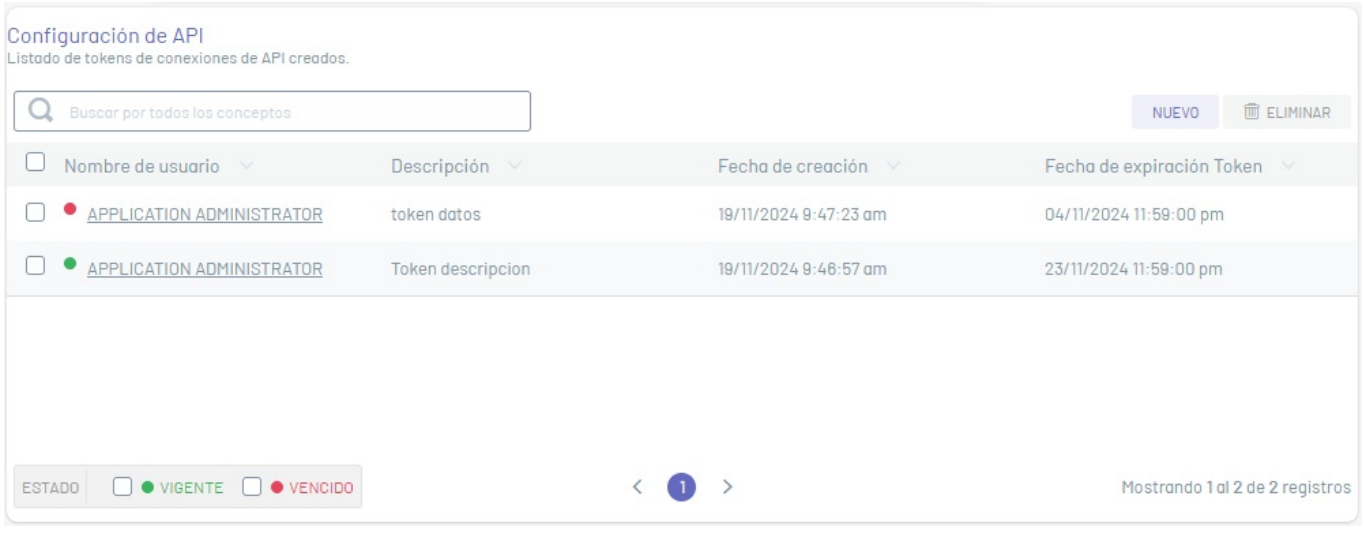
- Un proveedor eliminado no podrá ser restaurado.
- El proveedor no tiene restricción para su eliminación.

Módulo Token de Integración

Gestión de tokens

Visualizar Tokens

1. En la vista de información de Tokens podrá visualizar el listado de tokens creados, agrupados por datos como:



Campo	Tipo Campo	Descripción
Nombre de usuario	Texto	Nombre del usuario asociado al token.
Descripción	Texto	Descripción del token.
Fecha de creación	Texto	Fecha de creación.
Fecha de expiración de Token	Texto	Fecha que expira el token.

2. En la vista de información de los token, tendrá habilitadas acciones de gestión y organización de la información.Vista de Información en Entorno Commons

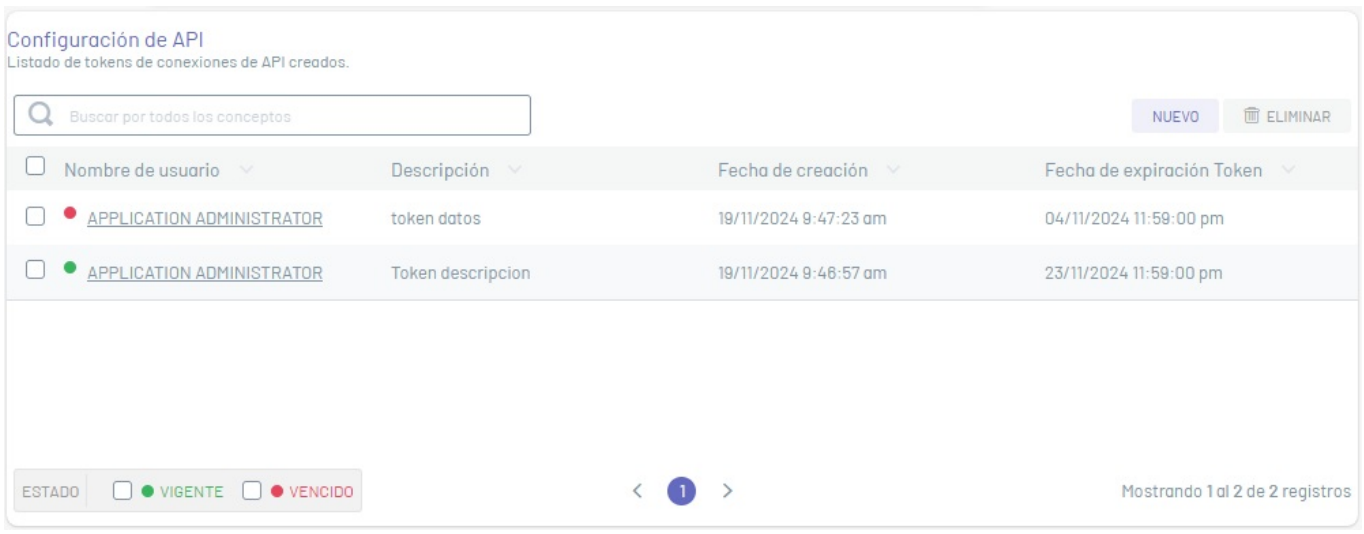
3. Para visualizar un token de integración, en la vista de información de tokens seleccione un registro del listado de tokens existentes. En la vista de detalle del token podrá visualizar la información con que fue creado el token, esta información no podrá ser editada.

Enlaces Relacionados:

- Crear Token Integración
- Eliminar Token Integración

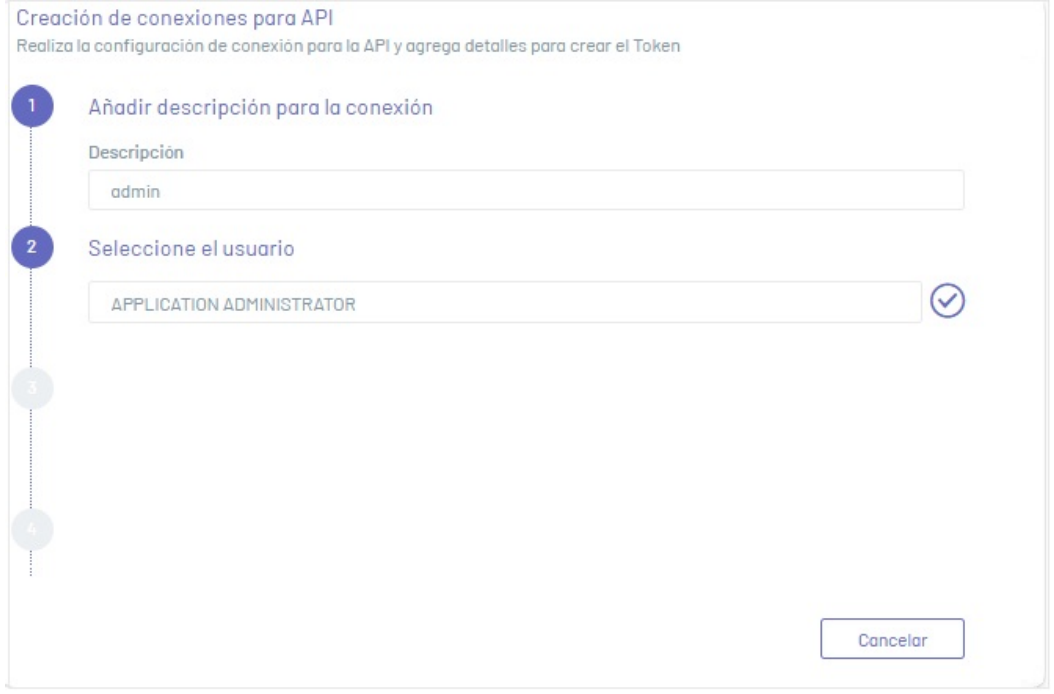
Crear tokens

1. Para crear un nuevo token de integración, en la vista de información de tokens, haga clic en el botón Nuevo.



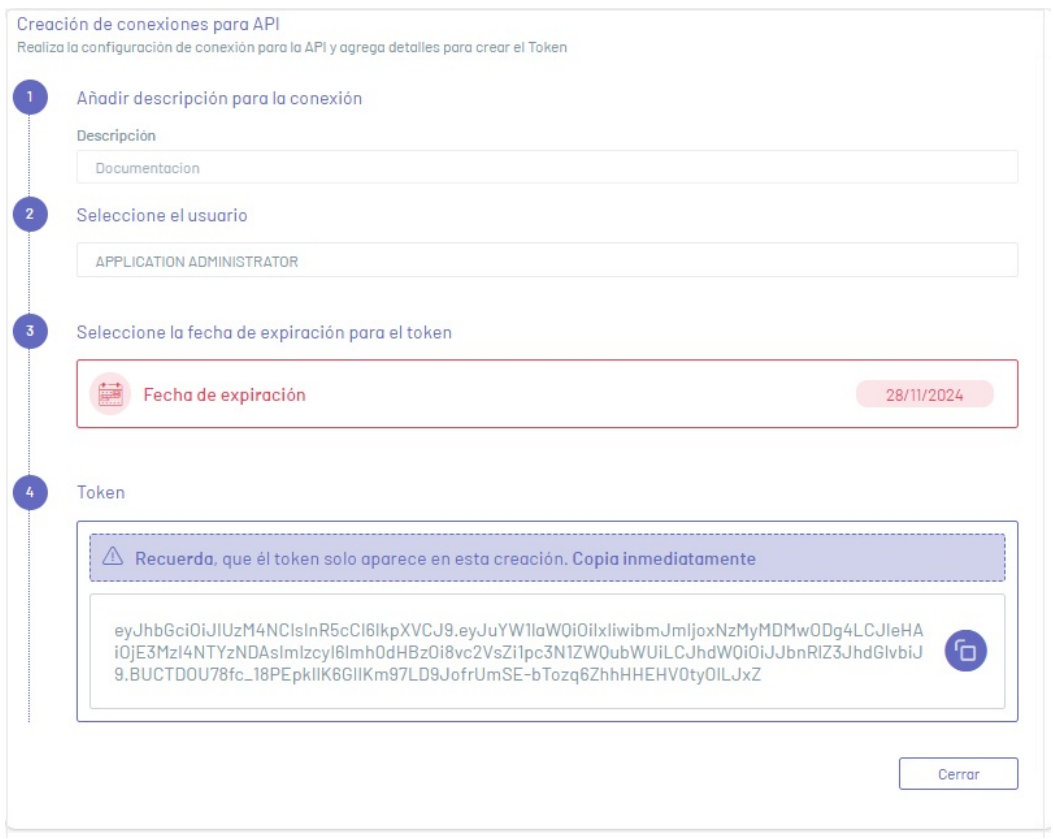
Datos Básicos

2. En la ventana que se habilita podrá completar los datos del token: Descripción, usuario y fecha de expiración. Cada uno de los campos del token deben tener en cuenta las especificaciones para campos Common



3. Al completar la configuración de cada campo, haga clic en el ícono

para confirmar los cambios generados.



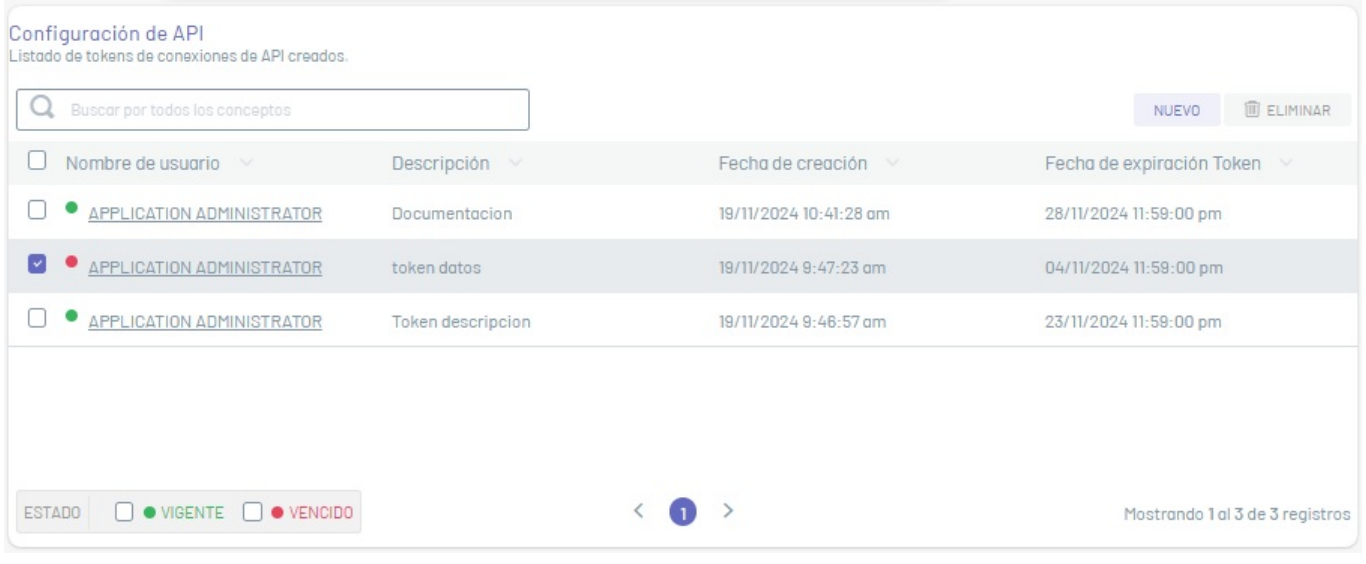
⚐ Nota: :

- Los tokens de integración no se pueden editar, por tal motivo los datos registrados deberán ser los correctos, o en caso contrario deberá crear otro token.
- El token generado se deberá copiar y guardar al momento de crearse, dado que no se volverá a mostrar.

Eliminar tokens

1. En la vista de información de tokens seleccione uno o varios registros del listado de tokens existentes y haga clic en el ícono

para borrar la información asociada.



2. Podrá visualizar un mensaje de confirmación para validar la acción de borrado.