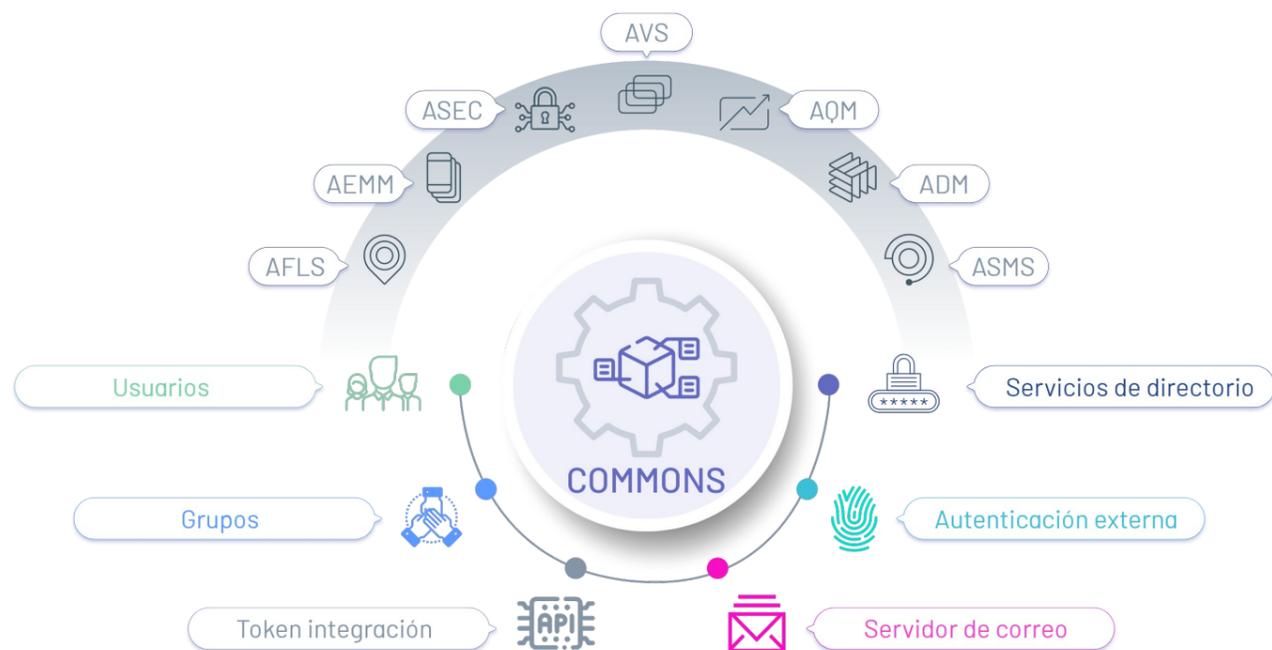




Configuración de Commons

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:

Módulos common

Implementados en:



¿Para Quién es este Manual?

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

¿Cuál es Nuestra Documentación?

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 diferentes 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

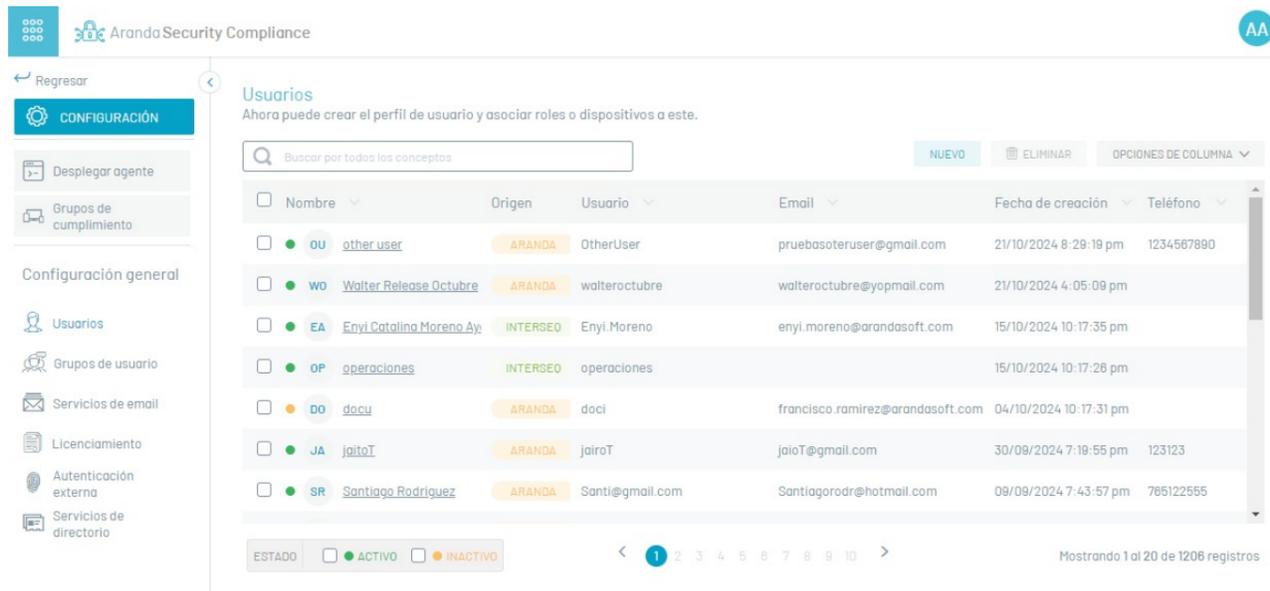
La gestión y configuración de los procesos de configuración para diferentes aplicaciones Aranda se realizan desde un entorno web con opciones y acciones compartidas.

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

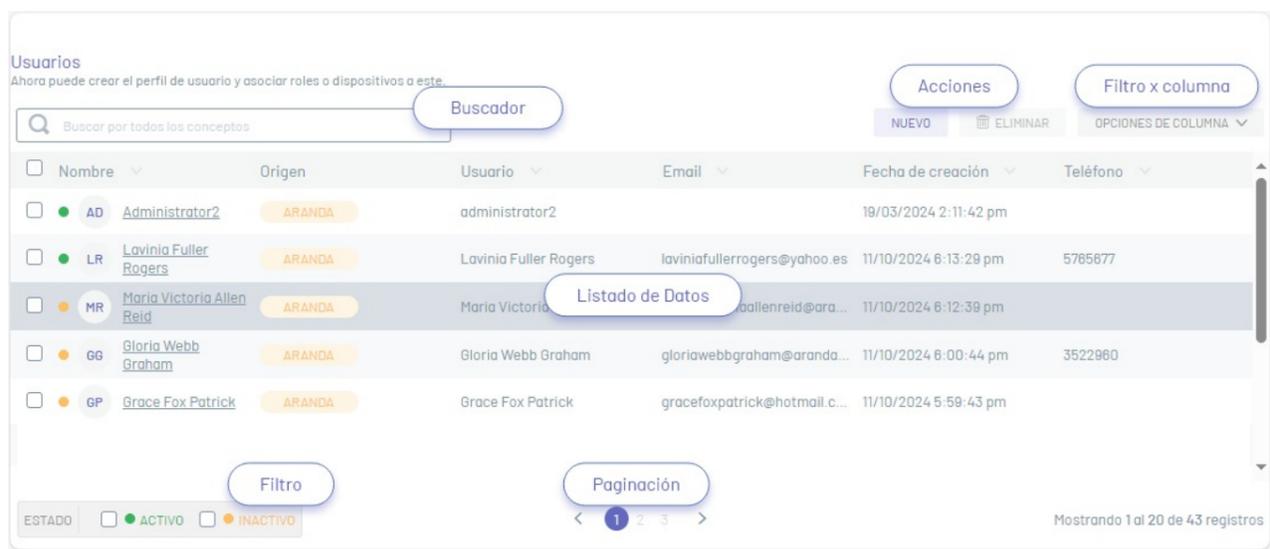
de directorio, tokens de integración) y al hacerlo se habilita la vista de información con los datos relacionados.

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.	    

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.

Nuevo



Este botón define la acción para eliminar un registro ya creado en los procesos de gestión.

Eliminar



Permite mostrar o ocultar opciones de la lista.

Filtro por de columna



Las opciones de columna del módulo de usuarios son: Nombre, origen, usuario, email, fecha de creación y teléfono.

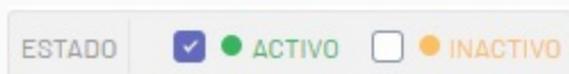
Permite navegar entre las páginas del listado de registros de usuario encontrados.

Paginación



Permite filtrar por el estado activo o inactivo de usuarios o proveedores de autenticación.

Filtro por estado



En el módulo Tokens de integración permite filtrar por el estado vigente o vencido de tokens de conexiones de API creados.



Este botón

Seguridad



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	<p>Este botón</p> 	
Filtrar	<p>Este botón</p> 	
Árbol de agrupación	<p>Esta sección despliega los grupos y subgrupos definidos.</p>	
Eliminar	<p>Este botón</p> 	
	<p>Este ícono</p> 	

Miga de pan



muestra la ubicación actual en el árbol de los grupos.

Este botón

Añadir
Usuarios

Añadir usuarios



define la acción para asociar usuarios a un grupo establecido.

Este botón

Gestionar
Roles

Gestionar roles



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:

Usuarios						
Ahora puede crear el perfil de usuario y asociar roles o dispositivos a este.						
<input type="text" value="Buscar por todos los conceptos"/>						
NUEVO ELIMINAR OPCIONES DE COLUMNA						
<input type="checkbox"/>	Nombre	Origen	Usuario	Email	Fecha de creación	Teléfono
<input type="checkbox"/>	AD Administrator2	ARANDA	administrator2		19/03/2024 7:11:42 pm	
<input type="checkbox"/>	LR Lavinia Fuller Rogers	ARANDA	Lavinia Fuller Rogers	laviniafullerrogers@yahoo.es	11/10/2024 11:13:29 pm	5765677
<input type="checkbox"/>	MR Maria Victoria Allen Reid	ARANDA	Maria Victoria Allen Reid	mariavictoriaallenreid@aran...	11/10/2024 11:12:39 pm	
<input type="checkbox"/>	GG Gloria Webb Graham	ARANDA	Gloria Webb Graham	gloriawebbgraham@arandas...	11/10/2024 11:00:44 pm	3522960

ESTADO ACTIVO INACTIVO < 1 2 3 > Mostrando 1 al 20 de 43 registros

Campo	Tipo 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](#)

Crear usuarios

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

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

Buscar por todos los conceptos

NUEVO ELIMINAR OPCIONES DE COLUMNA

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

ESTADO ACTIVO INACTIVO

Mostrando 1 al 20 de 43 registros

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](#)

Nuevo usuario
Complete la información para la creación del usuario.

*Nombre completo *Nombre de usuario

*Contraseña Confirmar contraseña Email Estado Inactivo

Información adicional Grupos Roles

Esta es información adicional para completar la información del usuario.

Celular Dirección Idioma Tipo de documento

Número de identificación Zona horaria Ubicación oficina Compañía

Área de compañía País Departamento Ciudad

Piso en el edificio Cargo Sede Teléfono

Información 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.

Nuevo usuario
Complete la información para la creación del usuario.

*Nombre completo *Nombre de usuario

*Contraseña Confirmar contraseña Email Estado Inactivo

Información adicional Grupos Roles

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

ad

Seleccionar todo

Administrators descripción del grupo

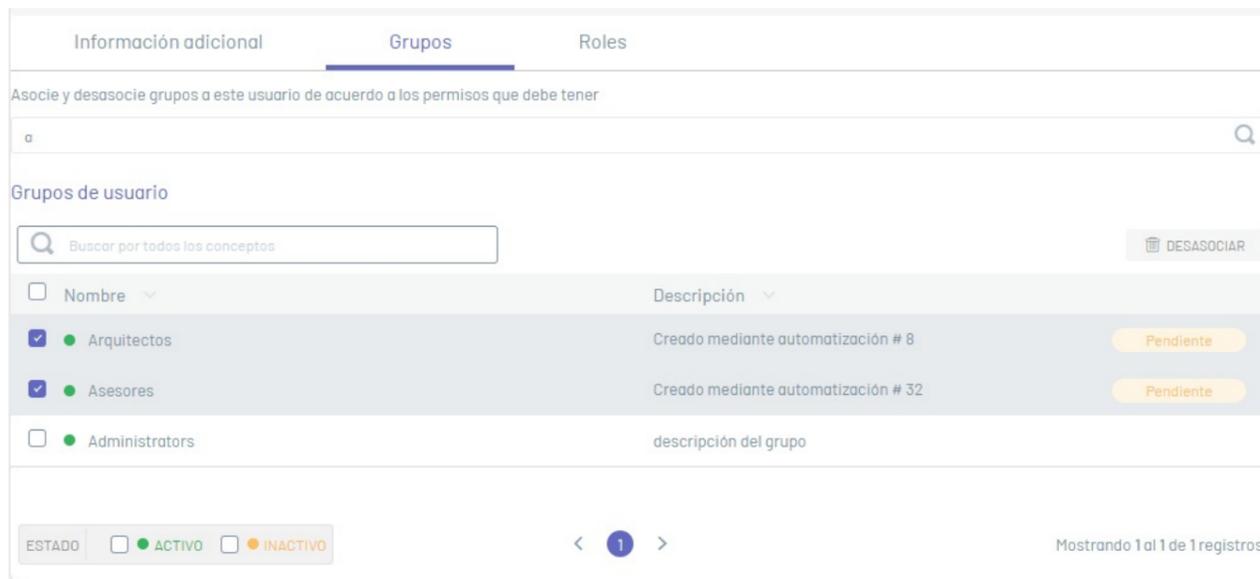
Comunicadores Creado mediante automatización # 28

Cancelar 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.



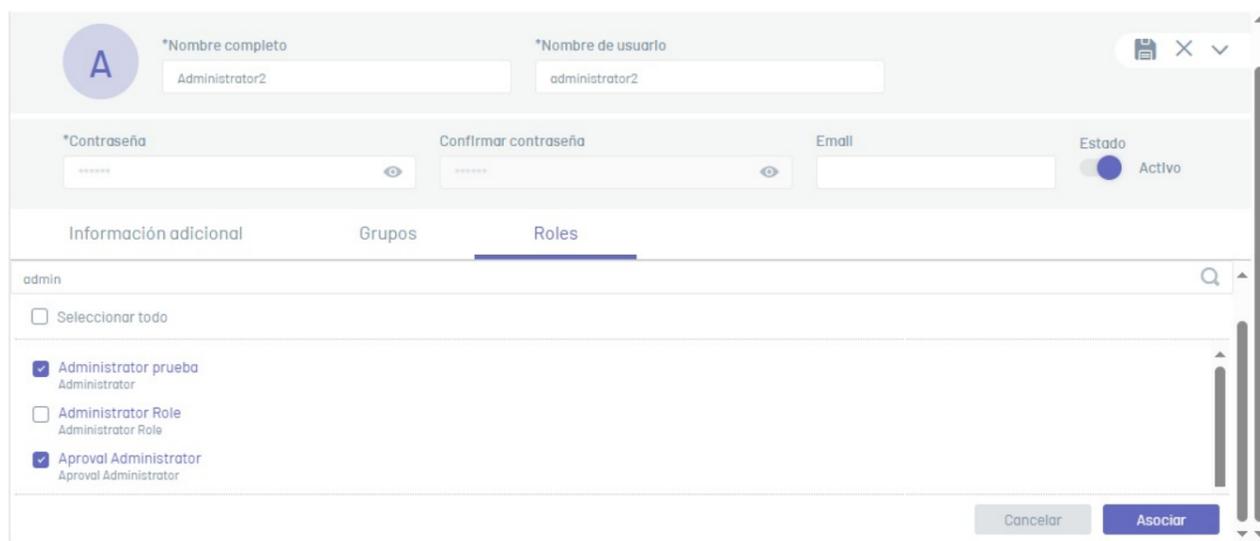
Nota:

- 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

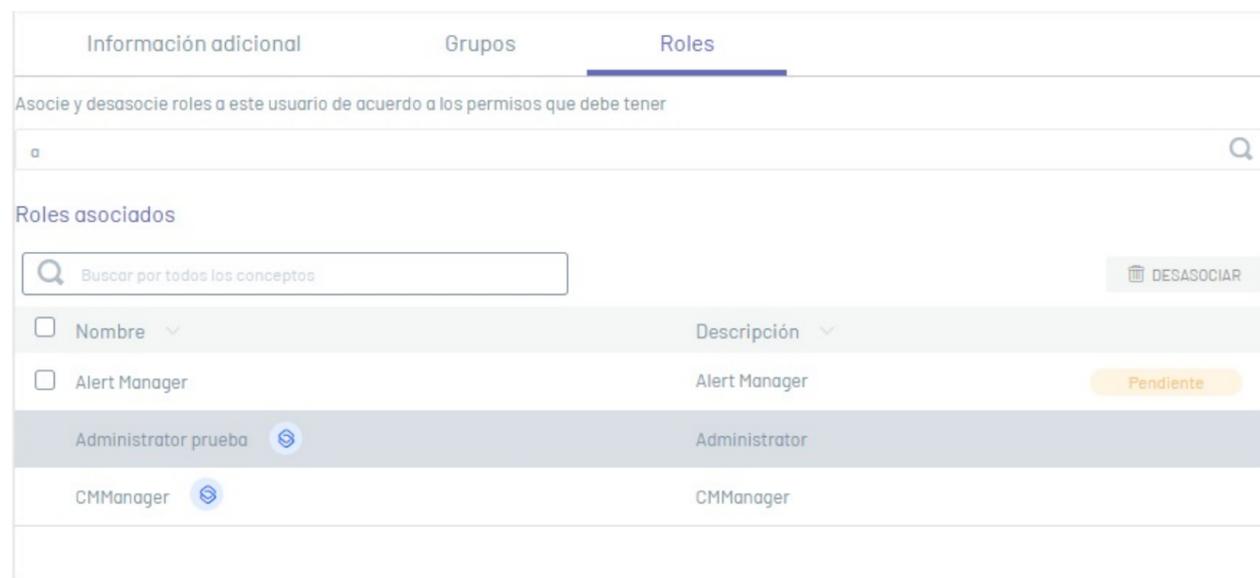
9. En la pestaña Roles, en el campo de búsqueda para asociar roles, podrá asociar los roles al usuario seleccionado, de acuerdo a los permisos establecidos.

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 icono 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.

Roles asociados

Buscar por todos los conceptos

DESASOCIAR

Nombre	Descripción
<input type="checkbox"/> Accounting Manager prueba	Accounting Manager
<input checked="" type="checkbox"/> Administrator prueba	Administrator
<input type="checkbox"/> Administrator Role	Administrator Role
<input type="checkbox"/> All Change Viewer	All Change Viewer

Editar usuarios

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

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

Buscar por todos los conceptos

NUEVO ELIMINAR OPCIONES DE COLUMNA

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

ESTADO ACTIVO INACTIVO

Mostrando 1 al 20 de 43 registros

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



y modifique la información requerida.

A Administrator2 ACTIVO

Usuario: administrator2
 Contraseña: *****
 Email:
 Teléfono:

Fecha de creación: Marzo 19, 2024 14:11

ELIMINAR

Información adicional
 Esta es información adicional para completar la información del usuario.

Roles
 Estos son los roles del usuario

AP CM

Grupos
 Este usuario está en estos grupos

AD

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.

Edición de usuario
 Complete la información para la edición del usuario.

A *Nombre completo: Administrator2 *Nombre de usuario: administrator2

*Contraseña: ***** Confirmar contraseña: ***** Email: Estado: Activo

Información adicional Grupos Roles

Esta es información adicional para completar la información del usuario.

Celular	Dirección	Idioma	Tipo de documento
		Seleccione	Escriba el nombre y seleccione
Número de identificación	Zona horaria	Ubicación oficina	Compañía
	(UTC-01:00) Azores	Escriba el nombre y seleccione	Escriba el nombre y seleccione
Área de compañía	País	Departamento	Ciudad
Escriba el nombre y seleccione			
Piso en el edificio	Cargo	Sede	Teléfono
Escriba el nombre y seleccione	Escriba el nombre y seleccione	Escriba el nombre y seleccione	

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.

Adamaris Navarro
ACTIVO

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

Nombre completo: Adolfo Valdez

Usuario: pgomez

Contraseña: *****

E-mail: pgomez@hotmail.com

Origen: Aranda

ELIMINAR

Información adicional
Esta es información adicional para completar la información del usuario.

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

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

Usuario bloqueado por exceder los intentos permitidos de contraseña.
DESBLOQUEAR

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.

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

Buscar por todos los conceptos

NUEVO ELIMINAR OPCIONES DE COLUMNA

<input type="checkbox"/>	Nombre	Origen	Usuario	Email	Fecha de creación	Teléfono
<input checked="" type="checkbox"/>	EM Eileen Powell Moss191	Ldap Simulac...	Eileen Powell Moss191	eileenpowellmoss191@aranda...	09/01/2021 9:44:27 am	
<input checked="" type="checkbox"/>	GL Gloria Jennings Larson852	Ldap Simulac...	Gloria Jennings Larson852	glorijenningslarson852@ara...	15/03/2023 4:19:53 pm	6019368459
<input type="checkbox"/>	AA APPLICATION ADMINISTRATOR	ARANDA	administrator		19/03/2024 7:11:42 pm	

ESTADO ACTIVO INACTIVO

< 1 2 3 >

Mostrando 41 al 43 de 43 registros

2. 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

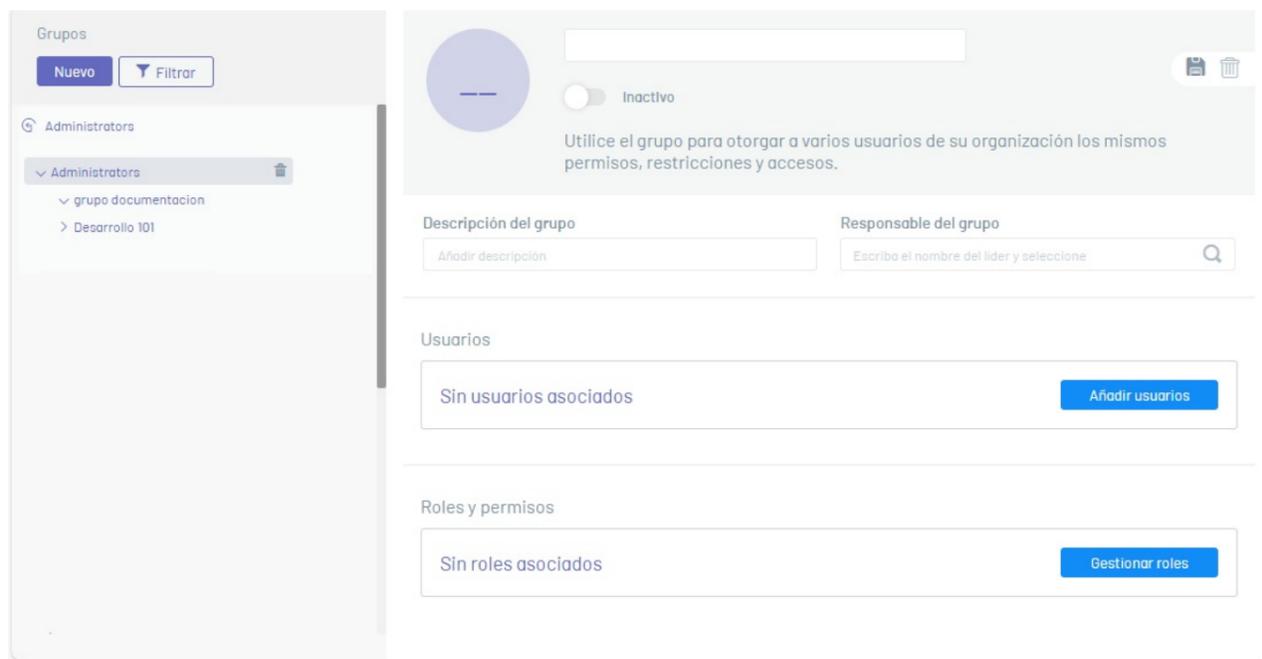
Gestión de grupos

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.



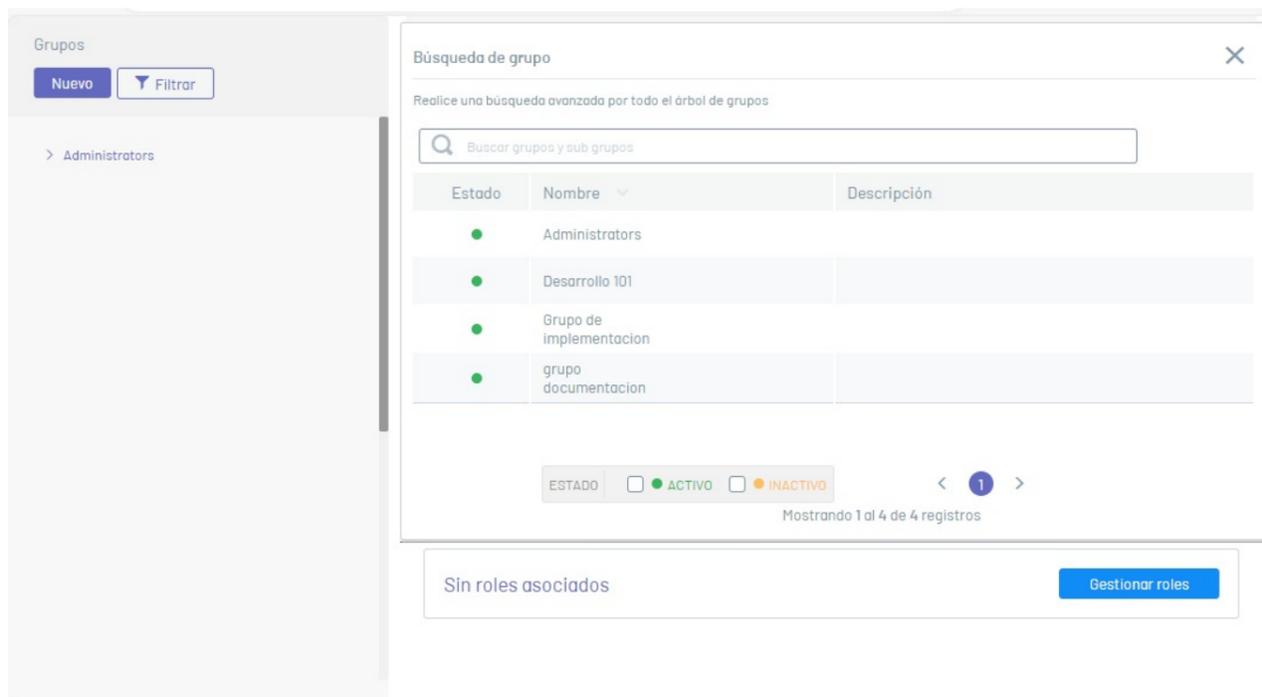
Nota: Aún si un grupo está deshabilitado se mostrará en el árbol.

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.

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

Descripción del grupo: Añadir descripción

Responsable del grupo: Escribo el nombre del líder y seleccione

Usuarios: Añadir usuarios

Roles y permisos: Sin roles asociados. Gestionar roles

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.

Asocie aquí usuarios para esta agrupación

ad

Seleccionar todo

Administrator2

APPLICATION ADMINISTRATOR

Cancelar Asociar

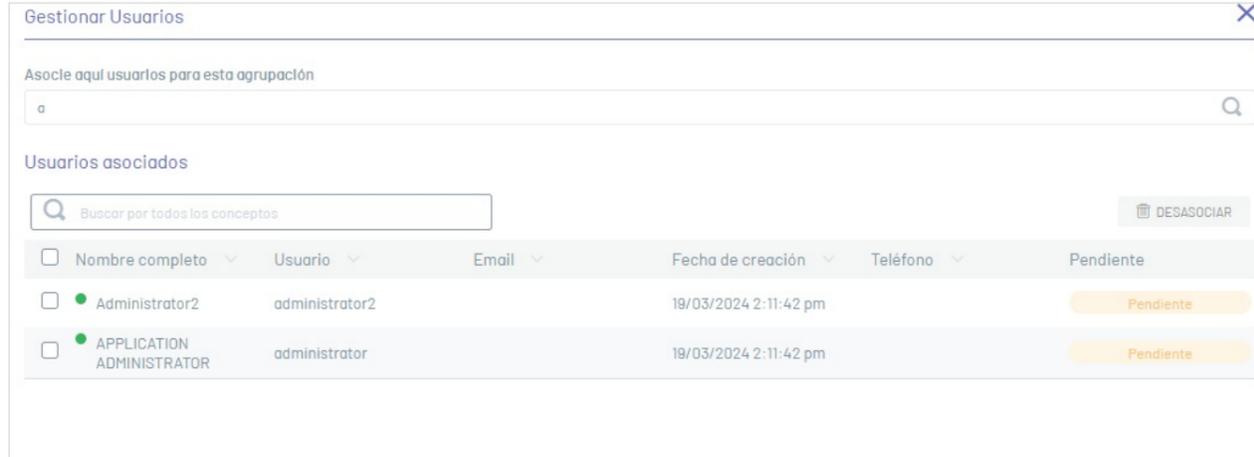
Usuarios asociados

Buscar por todos los conceptos

<input type="checkbox"/>	Nombre completo	Usuario	Email	Fecha de creación	Teléfono	Pendiente
No hay información.						

📌 Notas:

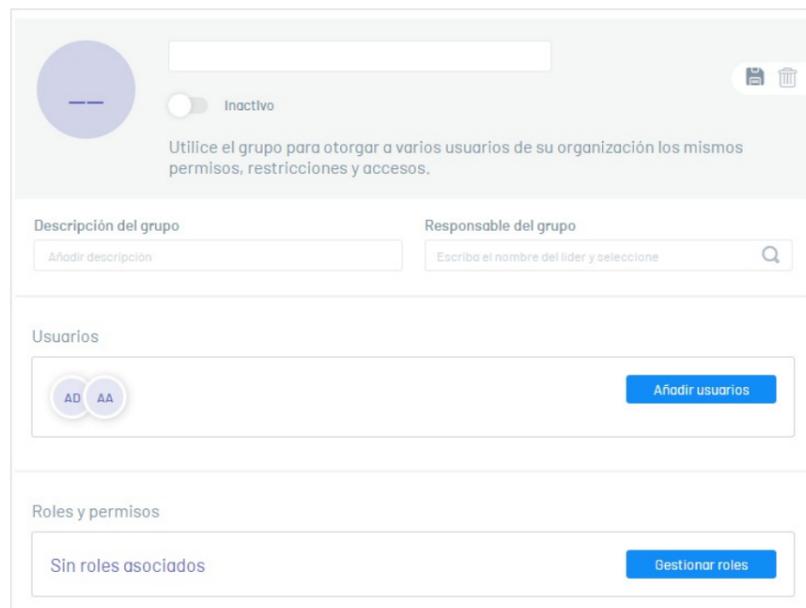
- Solo podrá listar usuarios activos. Los usuarios agregados quedarán con los roles del grupo.
- Una vez asociados los usuarios quedan en estado Pendiente hasta que se guarde el grupo



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

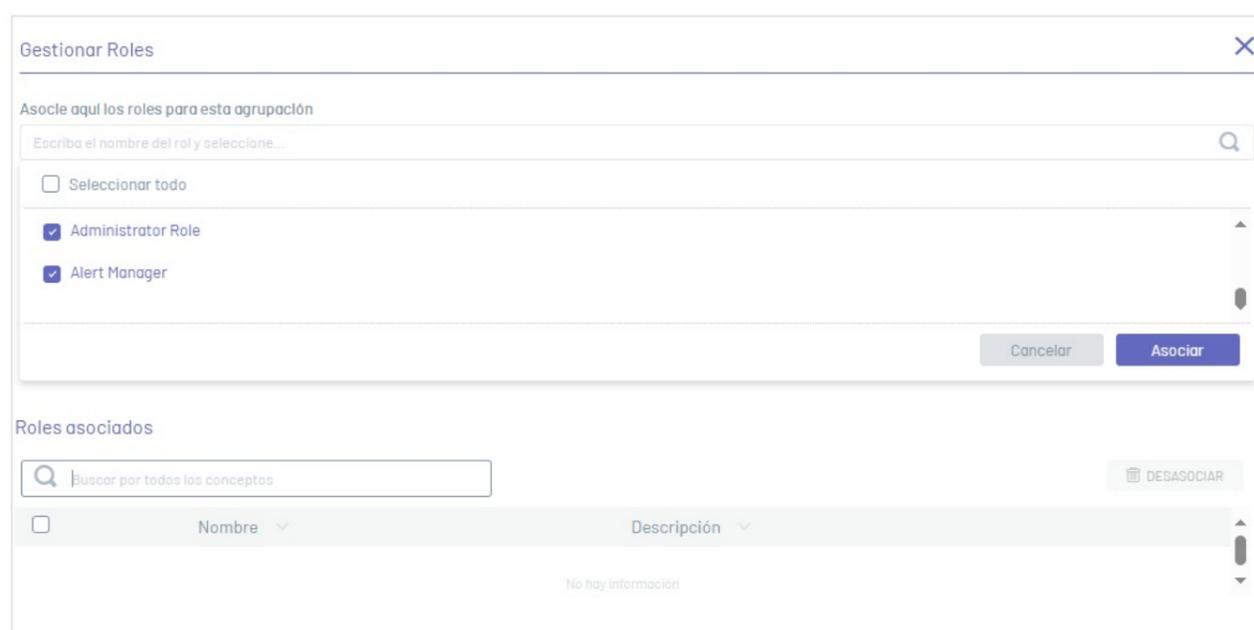
10. Para agregar roles, en la vista de información de un grupo de usuario, en la sección Roles y Permisos, seleccione el botón Gestionar Roles.



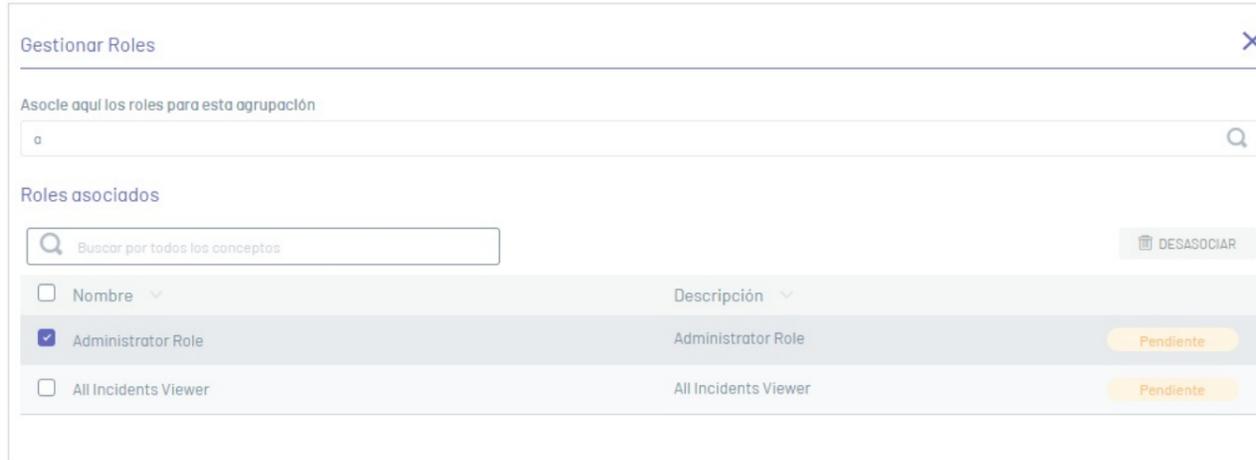
11. Se habilita la ventana Gestionar Roles, donde podrá consultar y agregar los roles requeridos para el grupo definido. En el campo de búsqueda ingrese el nombre del rol requerido y en la lista de resultados seleccione el rol a agregar.

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.

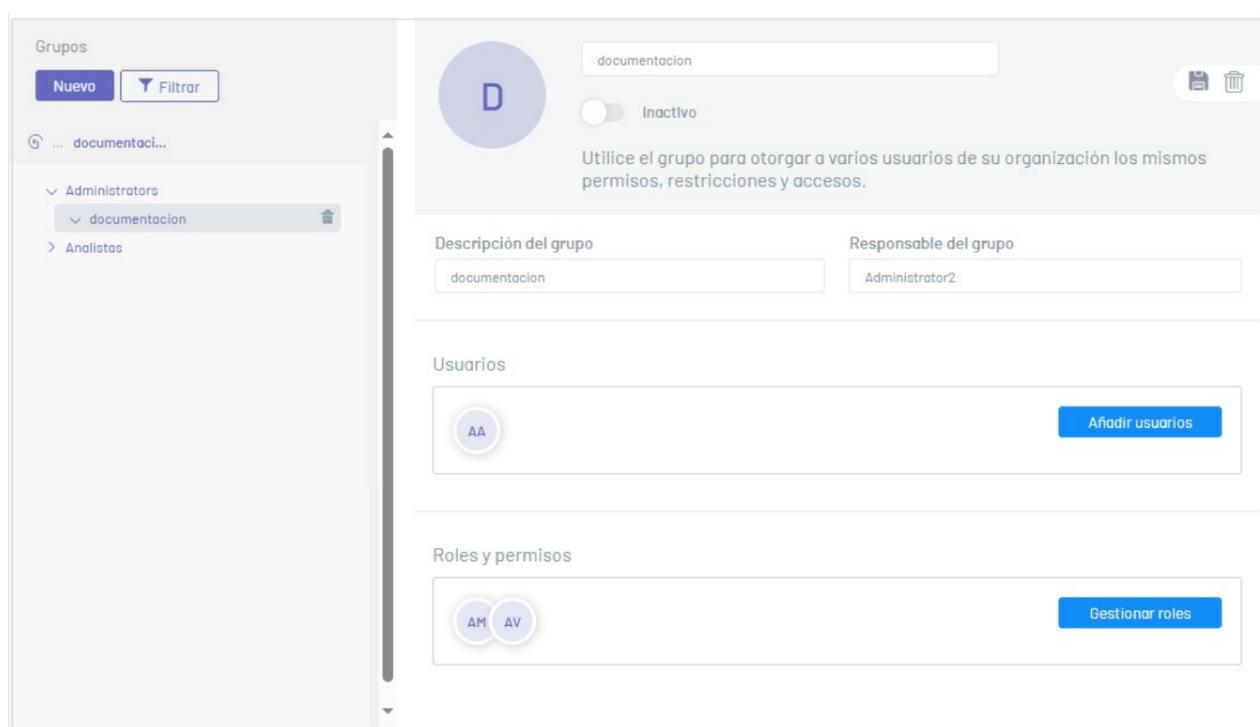
14. Al terminar de configurar el nuevo grupo, haga clic en el icono Guardar



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 icono Guardar



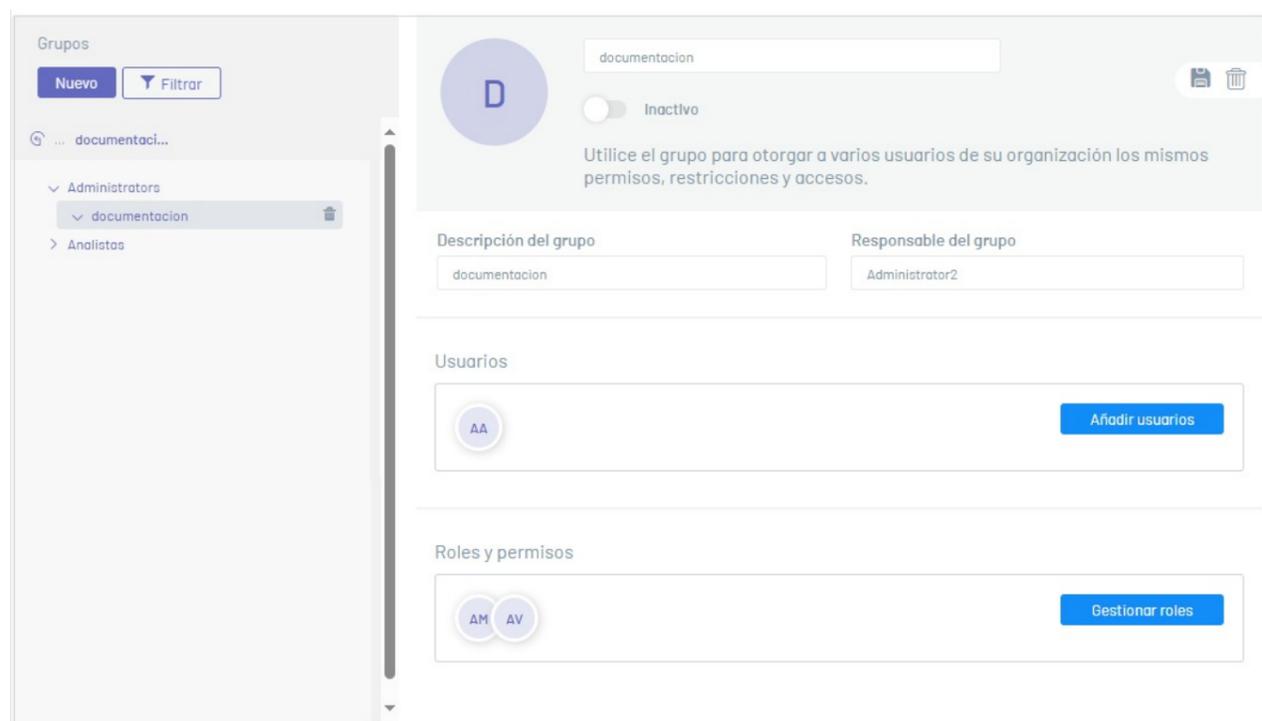
para confirmar los cambios realizados.

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 icono Eliminar



para borrar la información asociada.



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



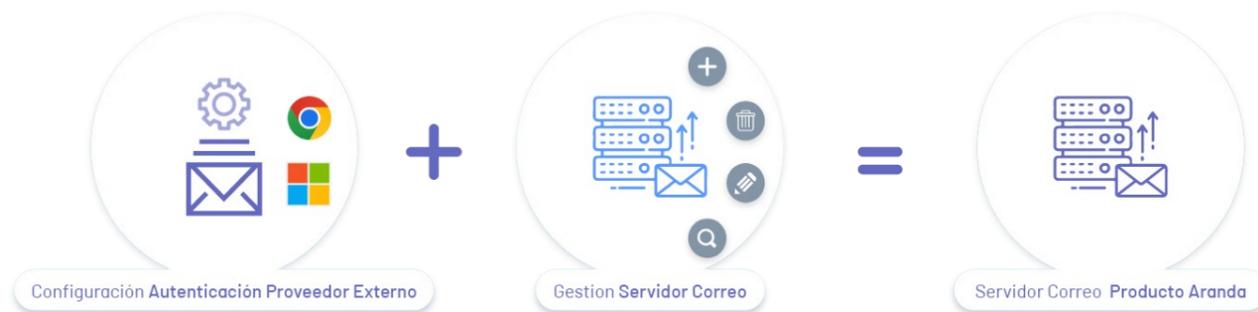
3. Podrá visualizar un mensaje de confirmación para validar la acción de borrado.

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.

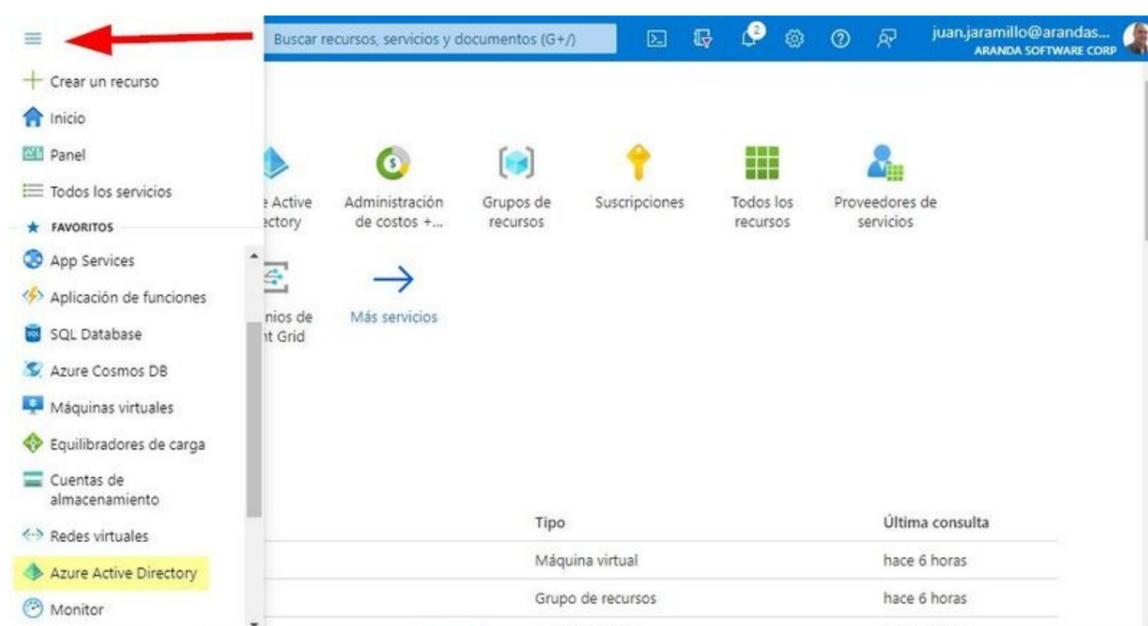
Para mayor información consulte la [Gestión Servidor de Correo](#).

Autenticación OAuth 2.0/Microsoft

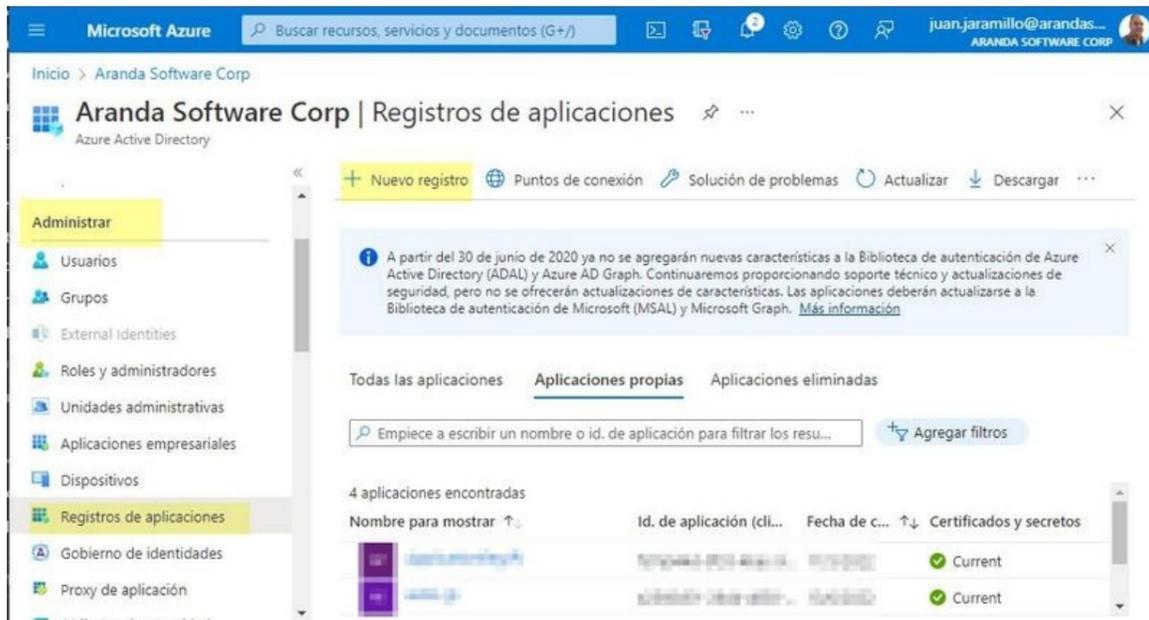
Creacion Aplicación en Azure

► Requisitos Autenticación Azure: ►

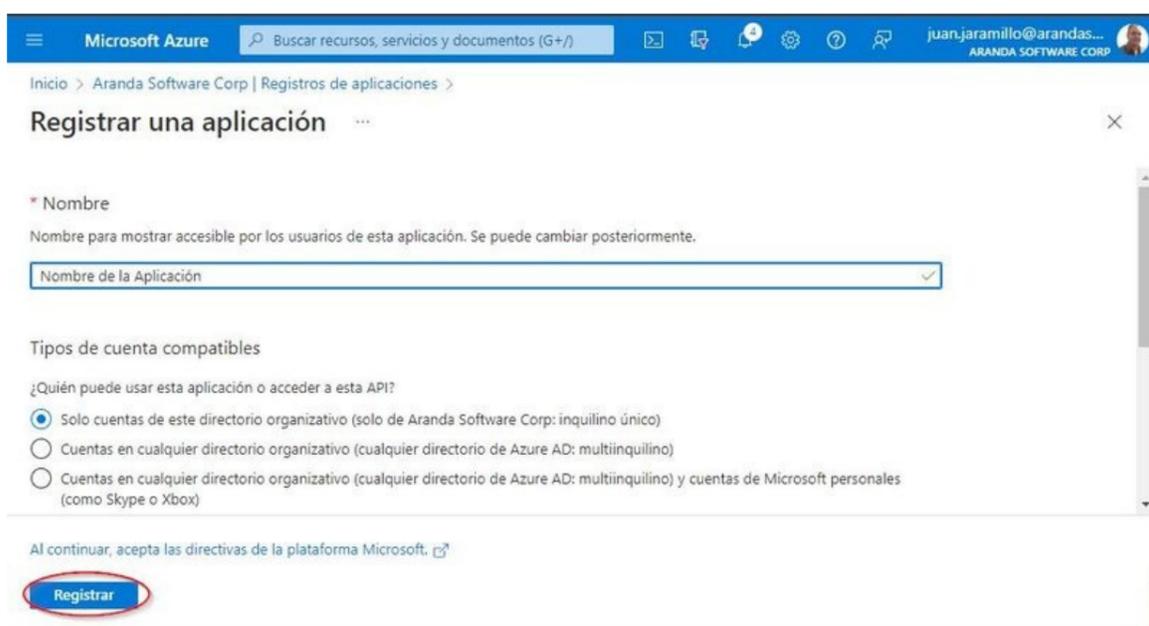
1. Se accede al portal de Azure [Ver Microsoft Azure](#), busque y seleccione Azure Active Directory.



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 cuenta compatibles), clic en Registrar.

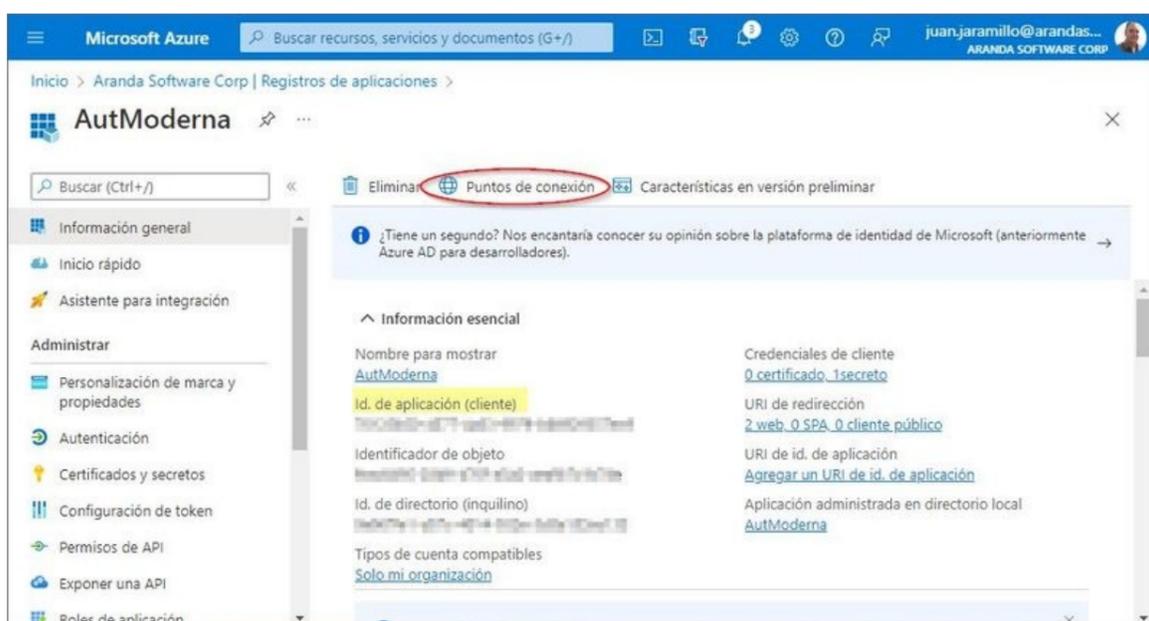


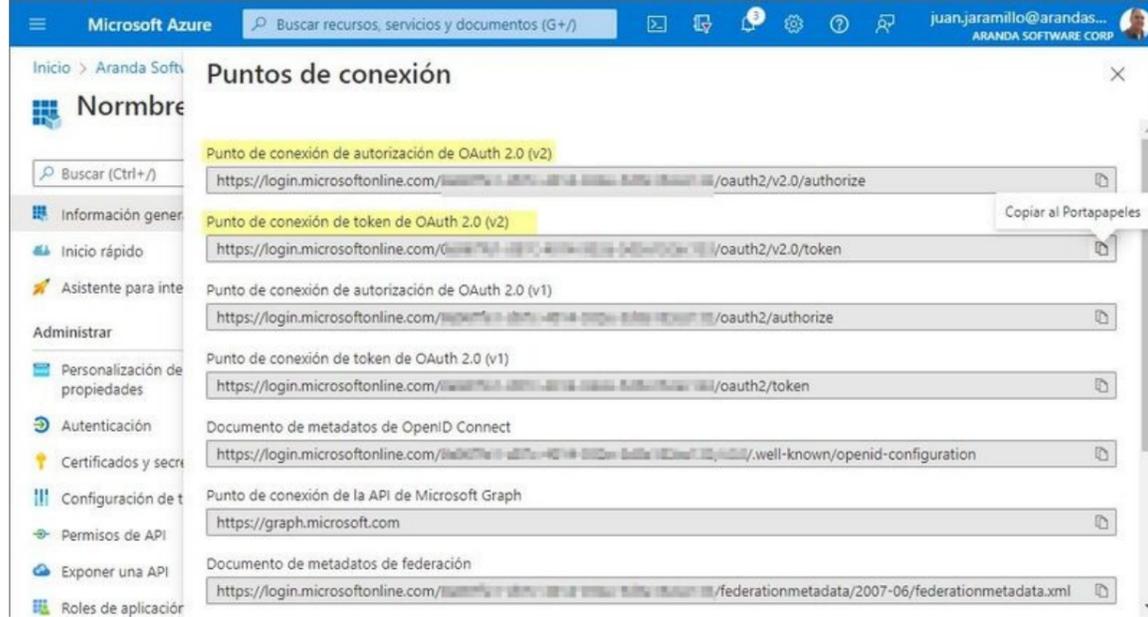
4. Cuando se tenga registrada la aplicación, guarde los siguientes datos que se requieren para la configuración en las aplicaciones de Aranda.

- 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.



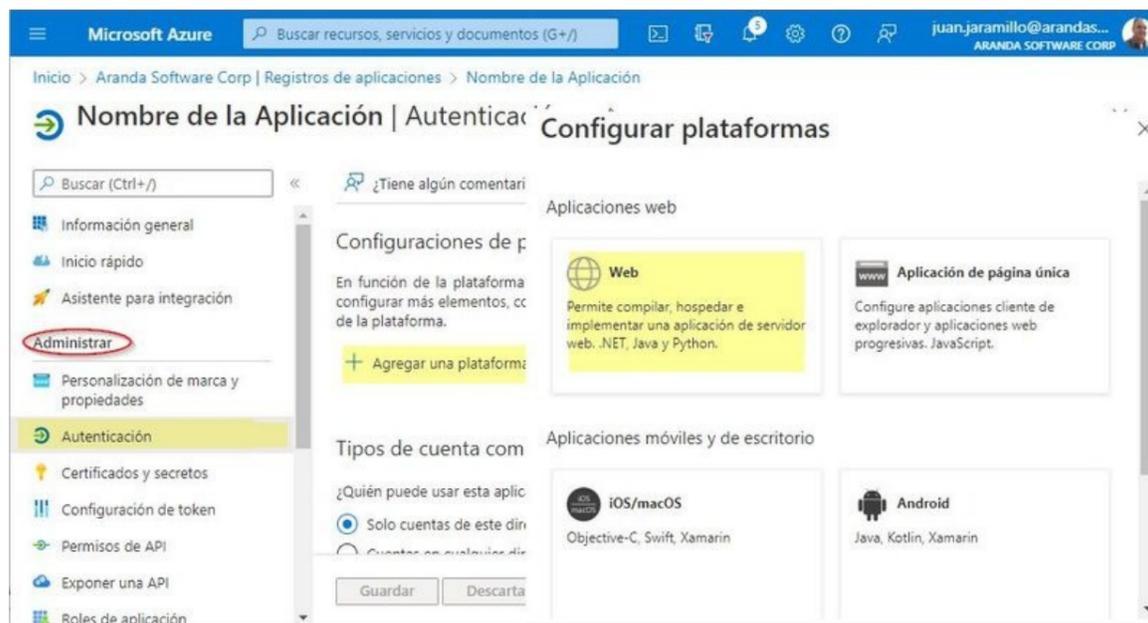


Configuración de la aplicación en el portal Azure

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:

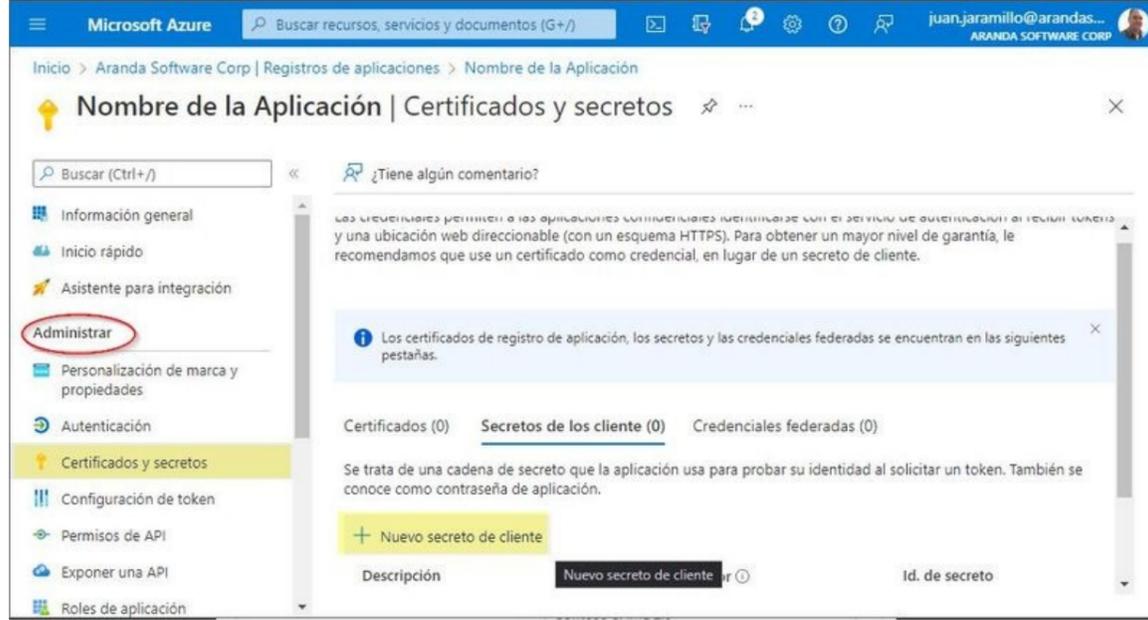
- Servidor de salida: `https://[dominio]/[SitioAdministracion]/Main/Pages/OauthToken.aspx`
- Servidor de entrada (Case creator): (`http://localhost`) y realice el [proceso manual de generacion del token](#) (Postman).

- Reemplace el `[dominio]` según corresponda, y luego seleccione Configurar.
- Reemplace `[SitioAdministracion]` con el nombre del directorio o aplicación del sitio de administración.
- Nota: Este nombre reconoce entre letras mayúsculas y minúsculas y se debe escribir como está configurado.

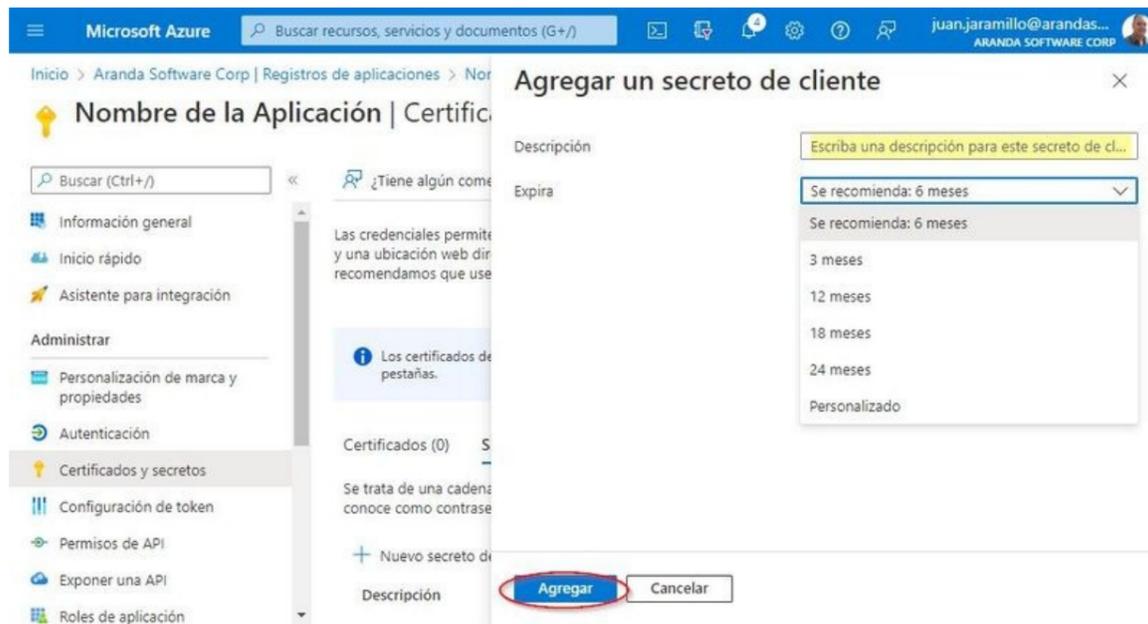
4. Para los demás productos Aranda, la URL de redirección es: (`https://localhost/sntp`) y debe realizar el [proceso manual de generacion del token](#) (Postman).

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.

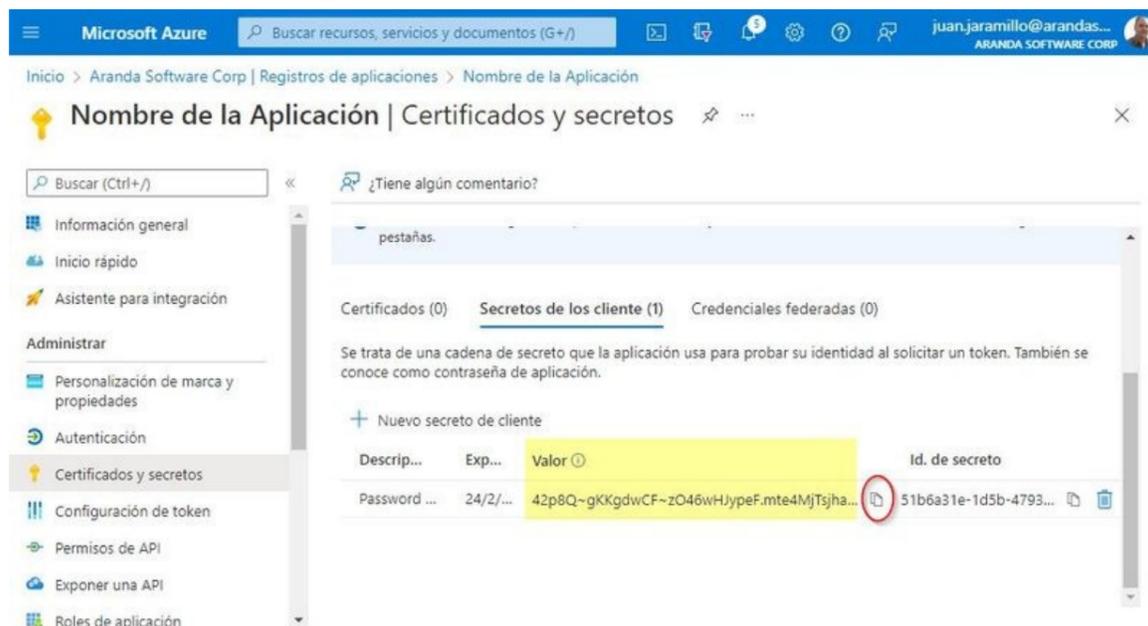


3. En la vista Agregar un secreto de cliente diligencie el campo Descripción, configure el campo Expira que corresponde a la duración del secreto. Luego selecciona Agregar (Es importante siempre tener presente esta duración dado que, a su vencimiento, si no se actualiza, fallará la autenticación).



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.

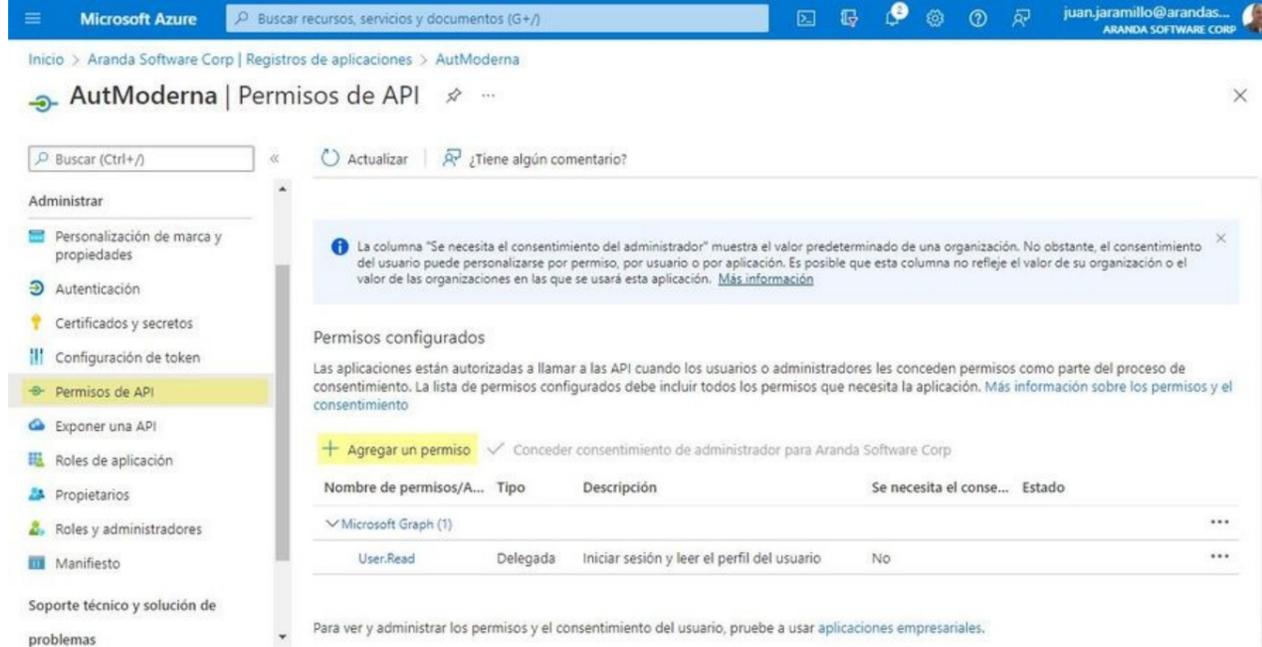
- Valor secreto de cliente -> Secreto cliente.



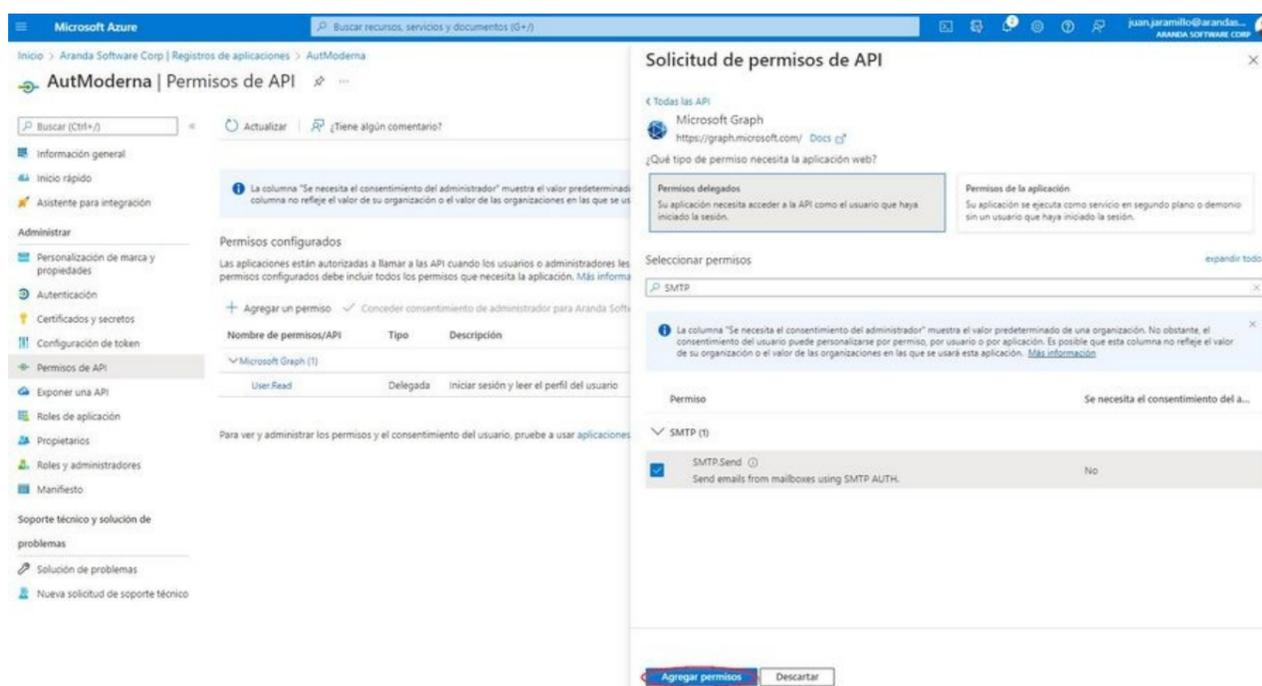
Configurar permisos de API

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.



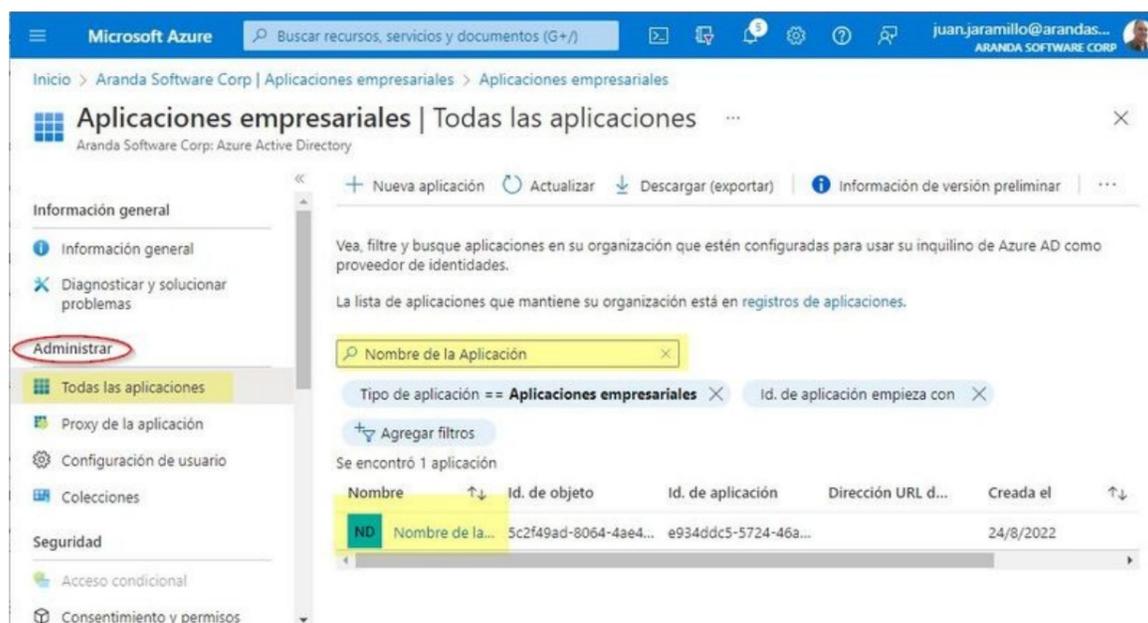
3. En la vista Solicitud de permisos de API, seleccionar Microsoft Graph > luego Permisos delegados, Seleccione los permisos de acuerdo a sus requerimientos: SMTP.Send (Envío de correos), IMAP y POP (Lectura de correos). Clic en Agregar permiso.



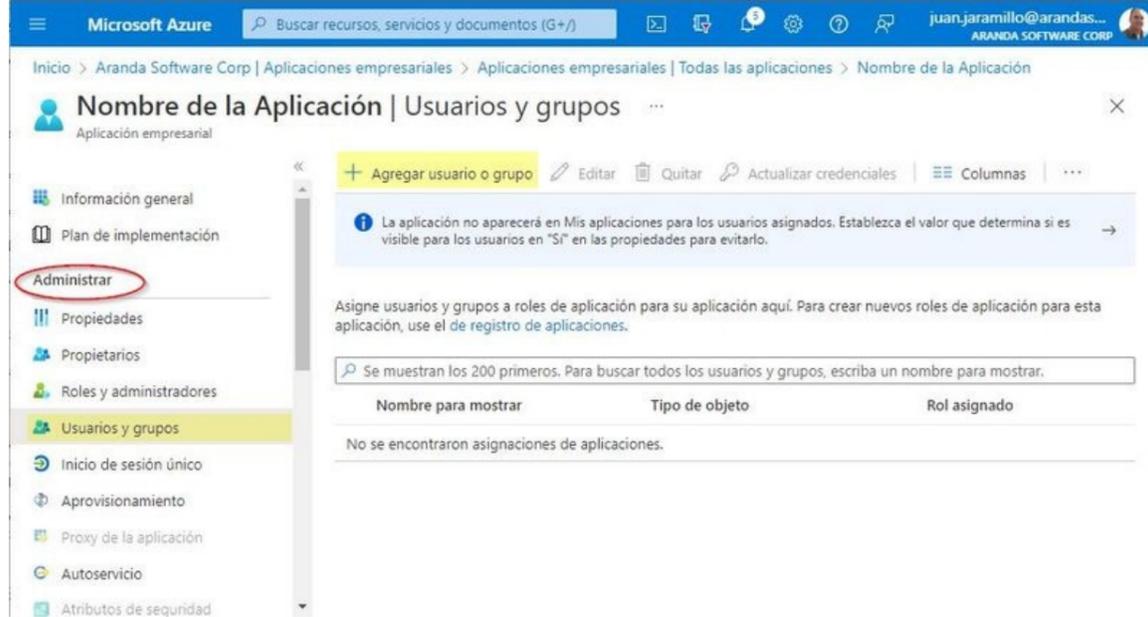
Configuración de usuarios y grupos

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

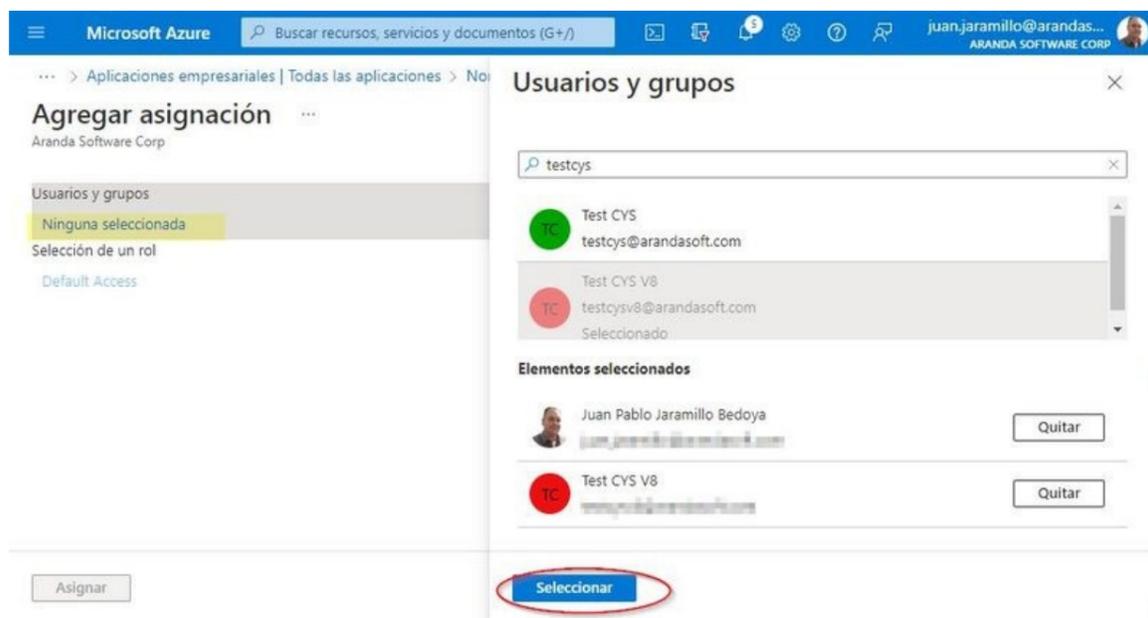
1. Se ingresa al portal de Azure > Menú > Azure Active Directory > Aplicaciones empresariales > seleccionar la aplicación creada del listado que aparece en la vista.



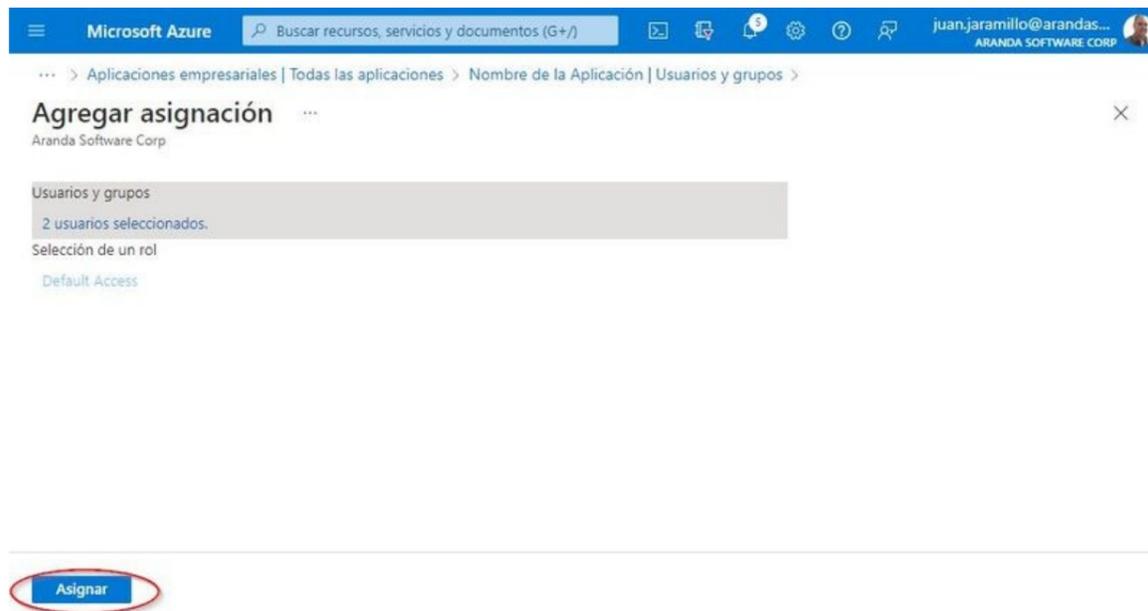
2. En la sección Administrar busque y seleccione Usuarios y grupos > y luego Agregar usuario o grupo.



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.



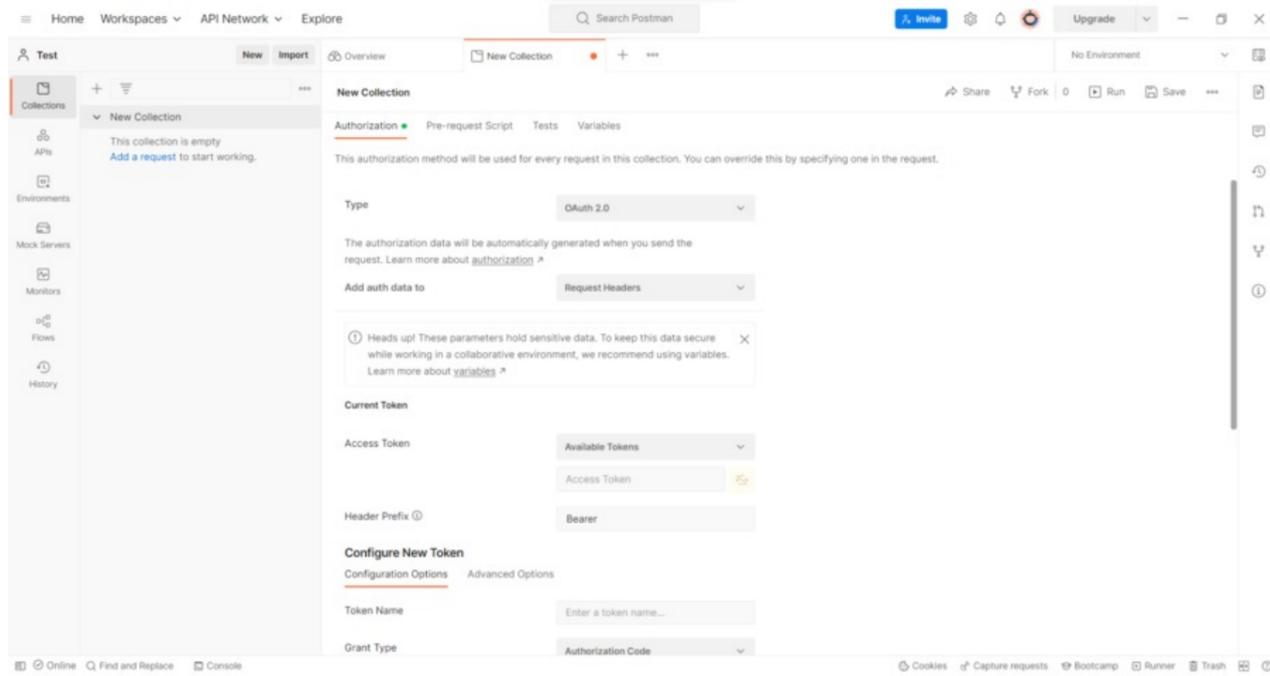
Creación Token Manual

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.

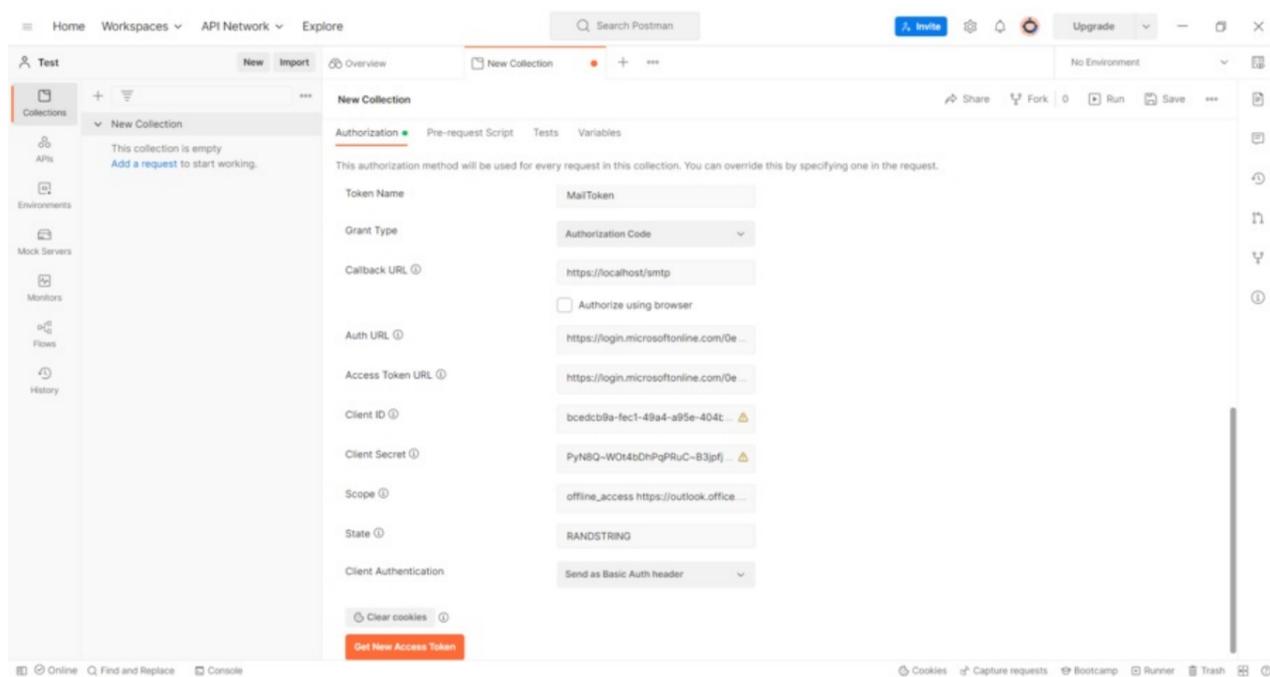
Configuración Token manual

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

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

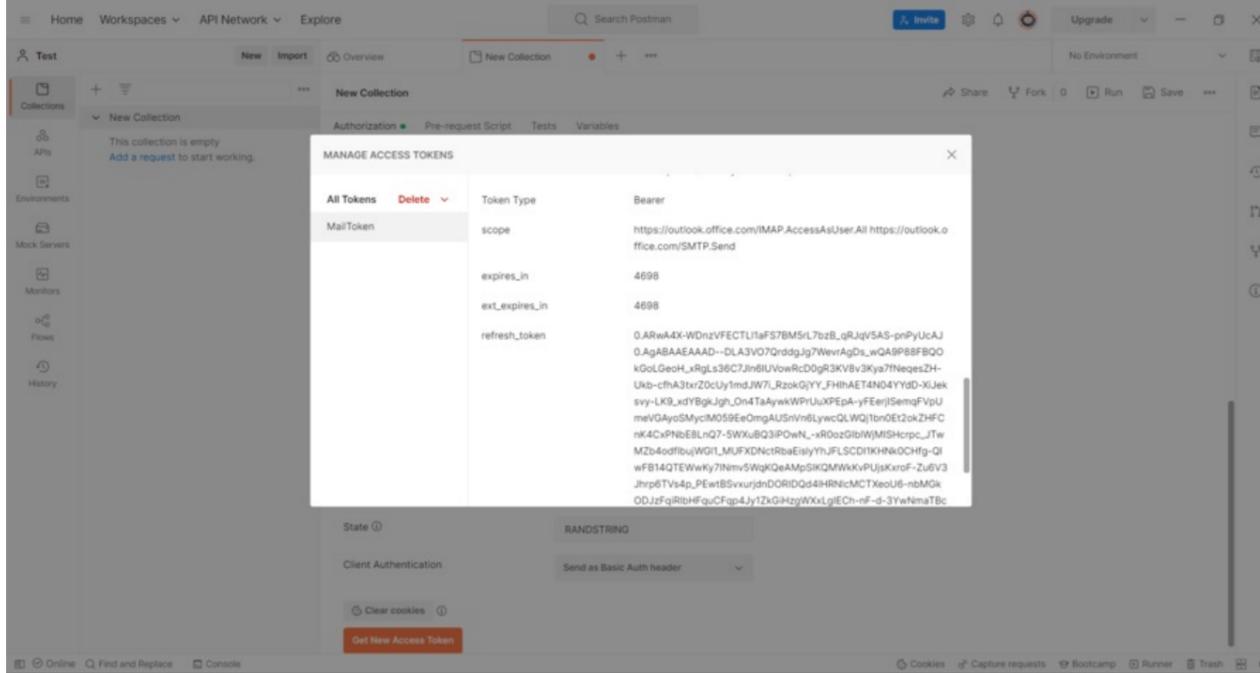


3. En la sección Configurar Nuevo Token, haga clic en el botón Nuevo Token; se habilita el formulario para registrar los siguientes campos:



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/sntp
Auth URL	Ingrese la url de autorización
Access Token URL	Ingrese la url la url del token
Client ID	Ingrese el identificador 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 desplegable 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).



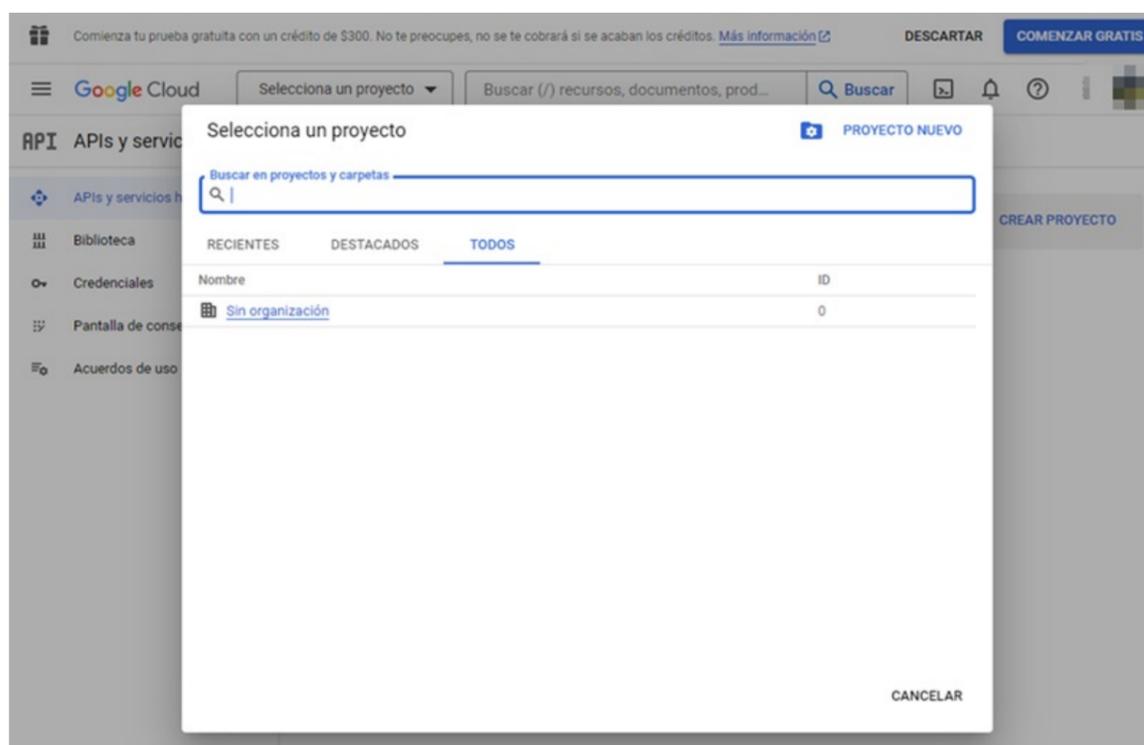
Nota: Después de realizar la configuración, el mailer enviará los correos respectivos de notificación.

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.

Proyecto nuevo

Nombre del proyecto *
Nombre del Proyecto

ID del proyecto *
nombre-del-proyecto-123 🔄

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

Organización *
Nombre de la Organización ▼ ?

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

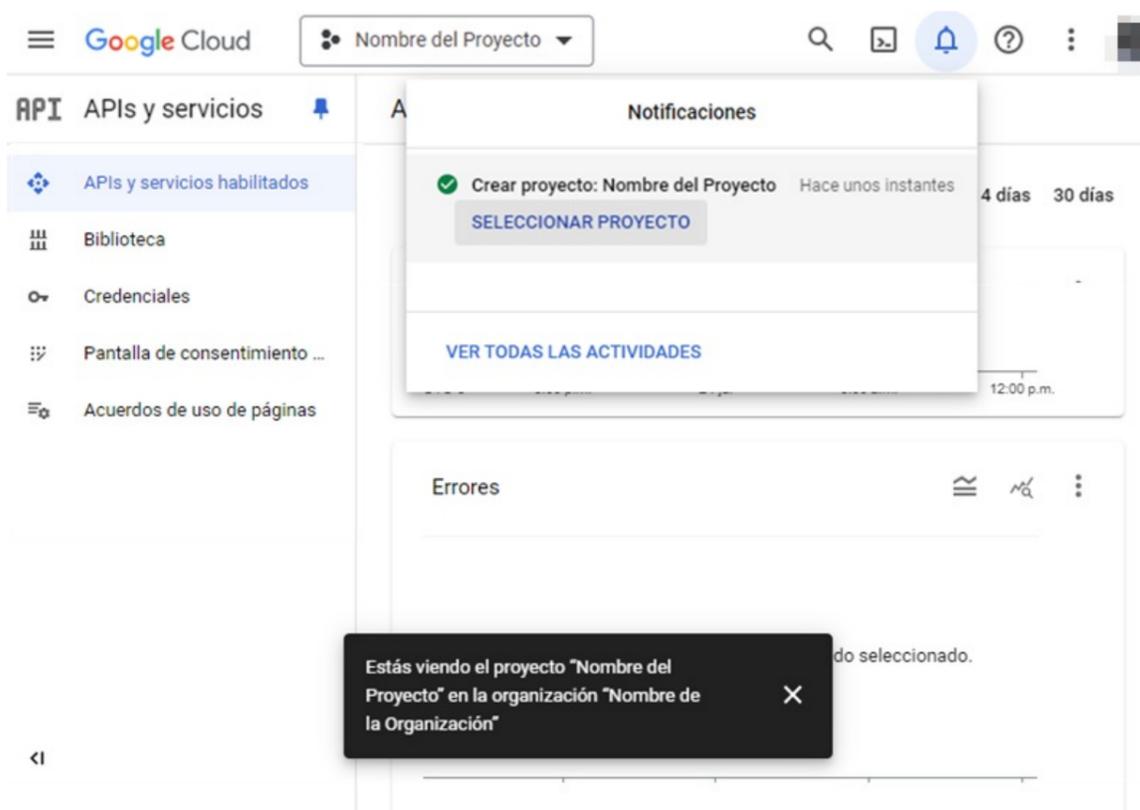
Ubicación *
📁 Nombre de la Organización EXPLORAR

Organización o carpeta superior

CREAR **CANCELAR**

Nota: 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.

The screenshot shows the Google Cloud console interface. On the left, there is a navigation menu with the following items: 'APIs y servicios' (selected), 'APIs y servicios habilitados', 'Biblioteca', 'Credenciales', 'Pantalla de consentimiento d...', and 'Acuerdos de uso de páginas'. The main content area is titled 'Pantalla de consentimiento de OAuth'. It contains the following text: 'Elige cómo deseas configurar y registrar tu app, incluidos los usuarios objetivo. Puedes asociar una sola app con tu proyecto.' Below this is the 'User Type' section with two radio buttons: 'Interno' (selected) and 'Externos'. The 'Interno' option has a help icon and a description: 'Solo está disponible para los usuarios de tu organización. No necesitarás enviar tu app para verificarla. [Obtén más información sobre el tipo de usuario](#)'. The 'Externos' option also has a help icon and a description: 'Está disponible para cualquier usuario de prueba con una Cuenta de Google. Tu app se iniciará en modo de prueba y solo estará disponible para los usuarios que agregues a la lista de usuarios de prueba. Una vez que la app esté lista para enviarse a producción, puede que debas verificarla. [Obtén más información sobre el tipo de usuario](#)'. At the bottom of the main content area is a blue 'CREAR' button.

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.

The screenshot shows the 'Editar el registro de la app' page in the Google Cloud console. The left navigation menu is the same as in the previous screenshot. The main content area is titled 'Editar el registro de la app' and has a breadcrumb trail: '1 Pantalla de consentimiento de OAuth — 2 Permisos — 3 Resumen'. Below the breadcrumb is the 'Información de la aplicación' section. It contains a text input field for 'Nombre de la aplicación *' with the value 'Nombre de la Aplicación' and a description: 'El nombre de la aplicación que solicita el consentimiento'. Below that is a dropdown menu for 'Correo electrónico de asistencia del usuario *' with the value 'usuario@dominio.com' and a description: 'Para que los usuarios se comuniquen contigo si tienen preguntas sobre su consentimiento. [Más información](#)'. The next section is 'Logotipo de la app' with a description: 'Este es tu logotipo. Ayuda a que las personas reconozcan tu app y aparece en la pantalla de consentimiento de OAuth. Después de subir un logotipo, deberás enviar tu app para verificarla, a menos que esté configurada solo para uso interno o tenga el estado de publicación "Prueba". [Más información](#)'. Below that is the 'Dominios autorizados' section with a description: 'Cuando un dominio se usa en la pantalla de consentimiento o en la configuración del cliente de OAuth, debe contar con un registro previo aquí. Si debes verificar la app, ve [Google Search Console](#) para comprobar si tus dominios están autorizados. [Más información](#) sobre el límite de dominios autorizados.' There is a '+ AGREGAR UN DOMINIO' button. The final section is 'Información de contacto del desarrollador' with a text input field for 'Direcciones de correo electrónico *' containing 'usuario@dominio.com' and a description: 'Google enviará notificaciones sobre cualquier cambio en tu proyecto a estas direcciones de correo electrónico.' At the bottom of the main content area are two buttons: 'GUARDAR Y CONTINUAR' and 'CANCELAR'.

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

API APIs y servicios  Editar el registro de la app 

- APIs y servicios habilitados
- Biblioteca**
- Credenciales
- Pantalla de consentimiento d...
- Acuerdos de uso de páginas

Pantalla de consentimiento de OAuth — **2 Permisos** —
 Resumen

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

AGREGAR O QUITAR PERMISOS

5. 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.

Actualiza los permisos seleccionados

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

Filtro Ingresar el nombre o el valor de la propiedad 

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

Filas por página: 10 ▼ 1 – 10 de 24 < >

Agrega permisos manualmente

Si los permisos que quieres agregar no aparecen en la tabla que se muestra más arriba, puedes ingresarlos aquí. Cada permiso debe estar en una línea nueva o debe separarse con comas. Proporciona la string completa del permiso (comienza con "https://"). Cuando termines, haz clic en "Agregar a la tabla".

`https://mail.google.com/`

AGREGAR A LA TABLA

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.

API APIs y servicios  **Credenciales** **+ CREAR CREDENCIALES** **BORRAR** 

- APIs y servicios habilitados
- Biblioteca
- Credenciales**
- Pantalla de consentimiento
- Acuerdos de uso de páginas

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

ID de cliente de OAuth
 Solicita el consentimiento del usuario para que tu app pueda acceder a sus datos

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

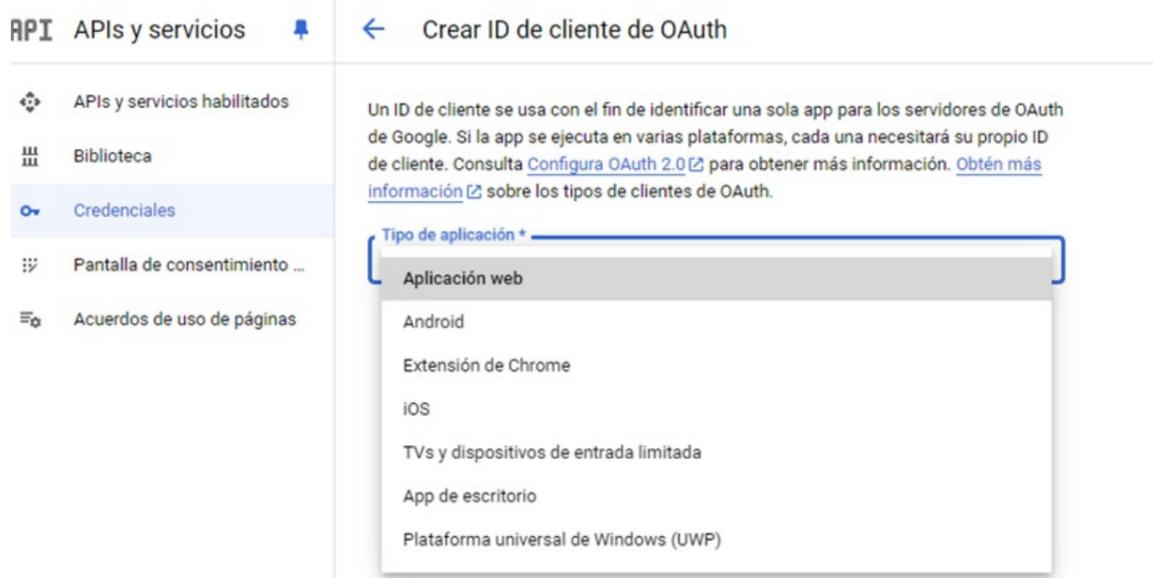
Ayúdame a elegir
 Responde algunas preguntas para decidir qué tipo de credencial usar

<input type="checkbox"/>	Nombre	Fecha de creación ↓	Tipo	ID de cliente	Acciones
No hay clientes de OAuth para mostrar					

Cuentas de servicio [Administrar cuentas de servicio](#)

<input type="checkbox"/>	Correo electrónico	Nombre ↑	Acciones
No hay cuentas de servicio para mostrar			

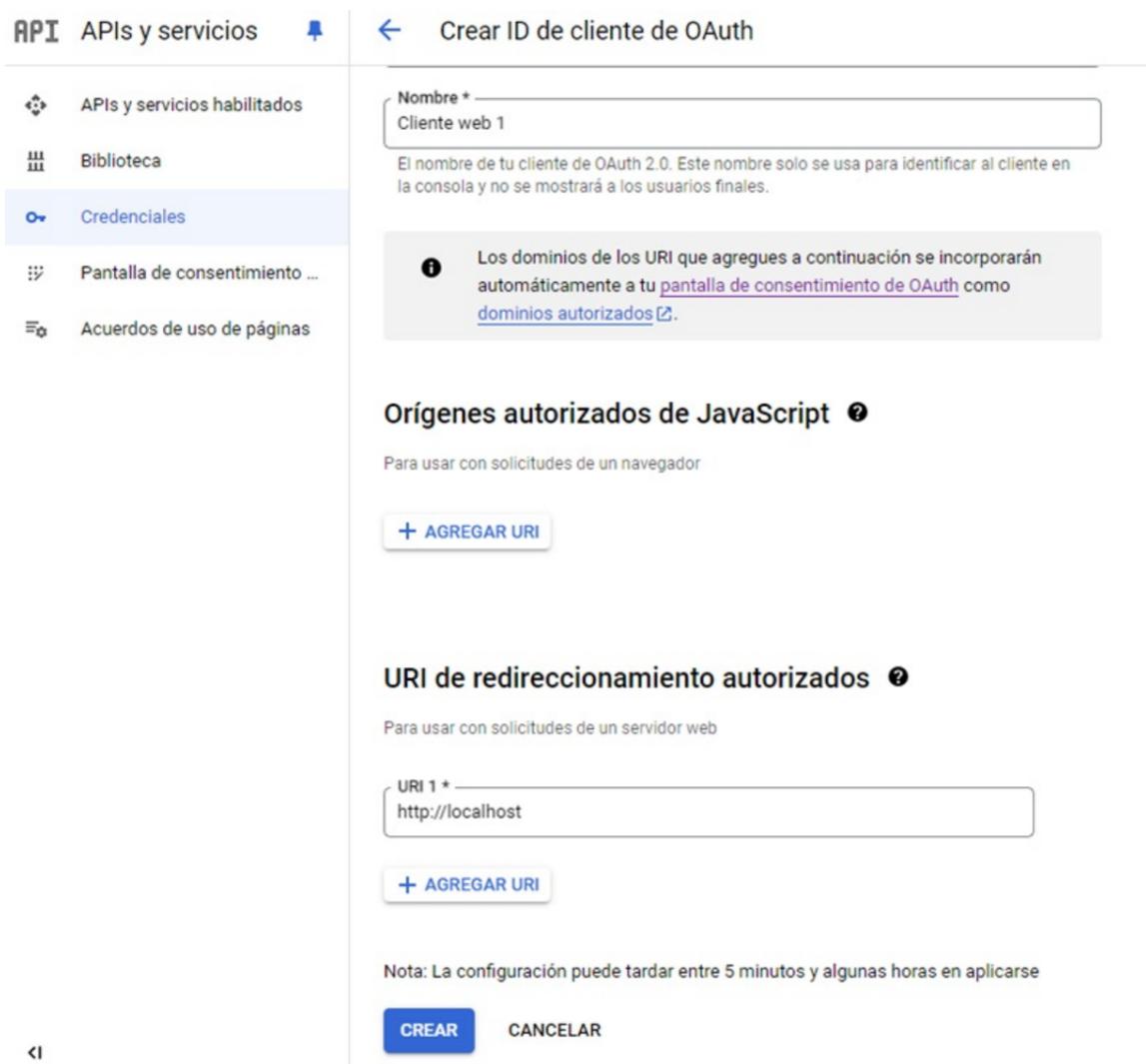
8. En la ventana Crear ID de cliente de OAuth en el campo Tipo de aplicación, seleccione la opción Aplicación web.



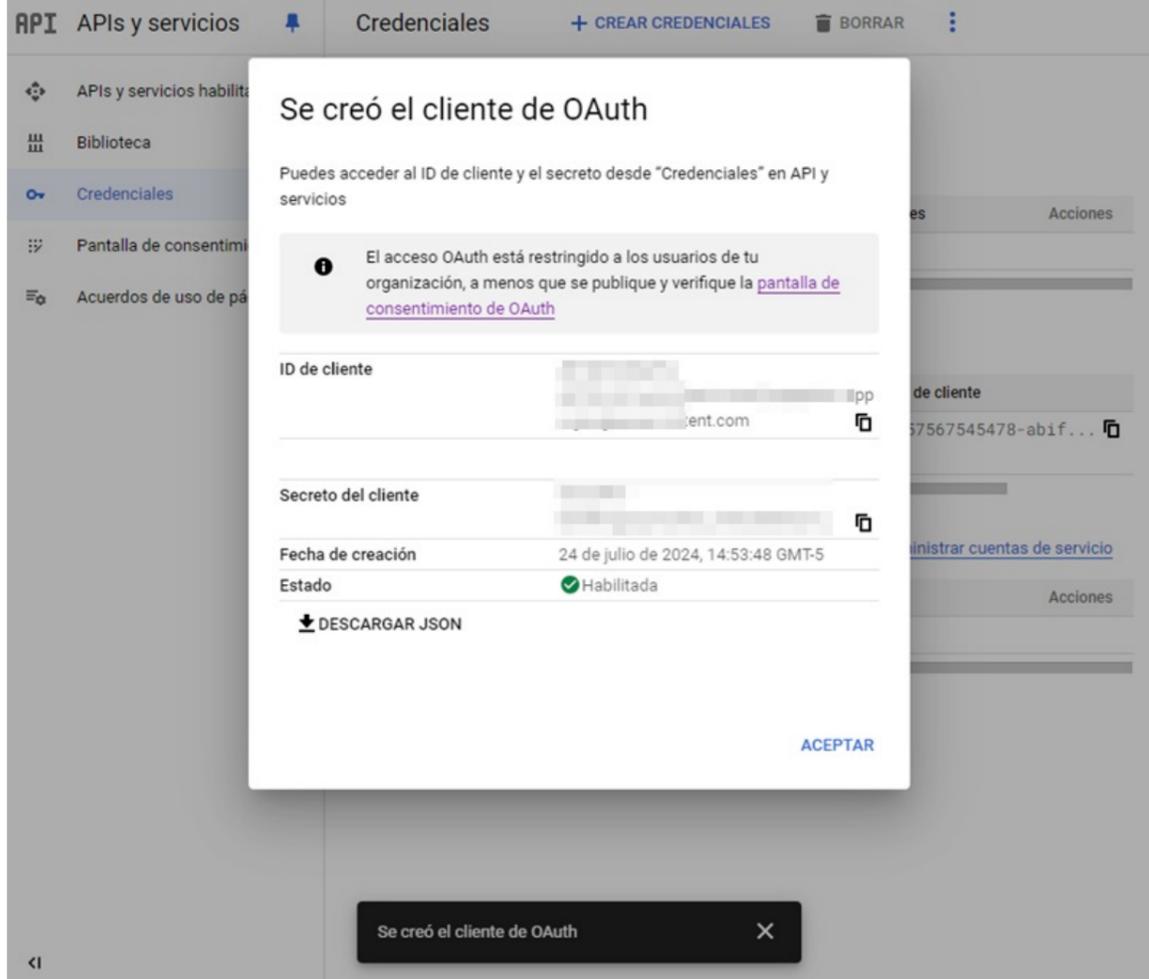
9. En la ventana Crear ID de cliente de OAuth en la sección URI de redireccionamiento autorizados, ingrese la URI correspondiente para el producto Aranda Service Management (ASMS) de la siguiente manera:

- 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](#).

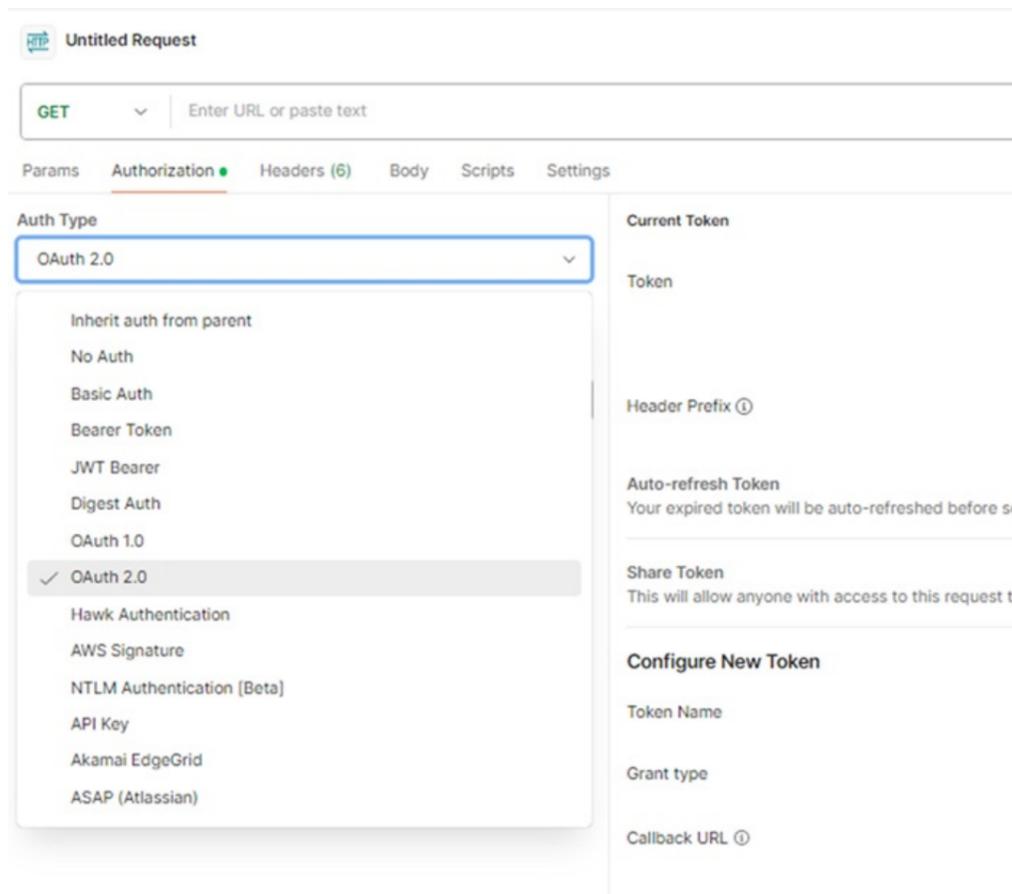


- Identificador de cliente -> ID de cliente.
- Valor secreto de cliente -> Secreto del cliente.
- Url del token -> <https://oauth2.googleapis.com/token>.
- Url de autorización -> <https://accounts.google.com/o/oauth2/v2/auth>

Solicitud Refresh Token Google

Para la solicitud del refresh_ 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:

Untitled Request

GET

Params Authorization Headers (6) Body Scripts Settings

Auth Type: OAuth 2.0

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

Add authorization data to: Request Headers

Current Token

Token: Available Tokens

Header Prefix: Bearer

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

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

Configure New Token

Token Name: Pruebas Google

Grant type: Authorization Code

Callback URL: http://localhost

Authorize using browser

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

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

Client ID:

Client Secret:

Scope: https://mail.google.com/

State: State

Client Authentication: Send as Basic Auth header

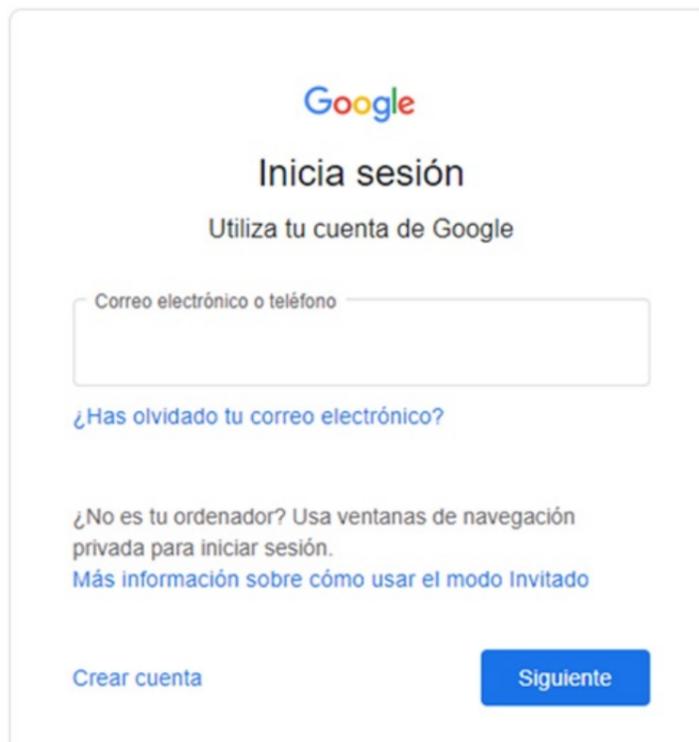
> Advanced

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

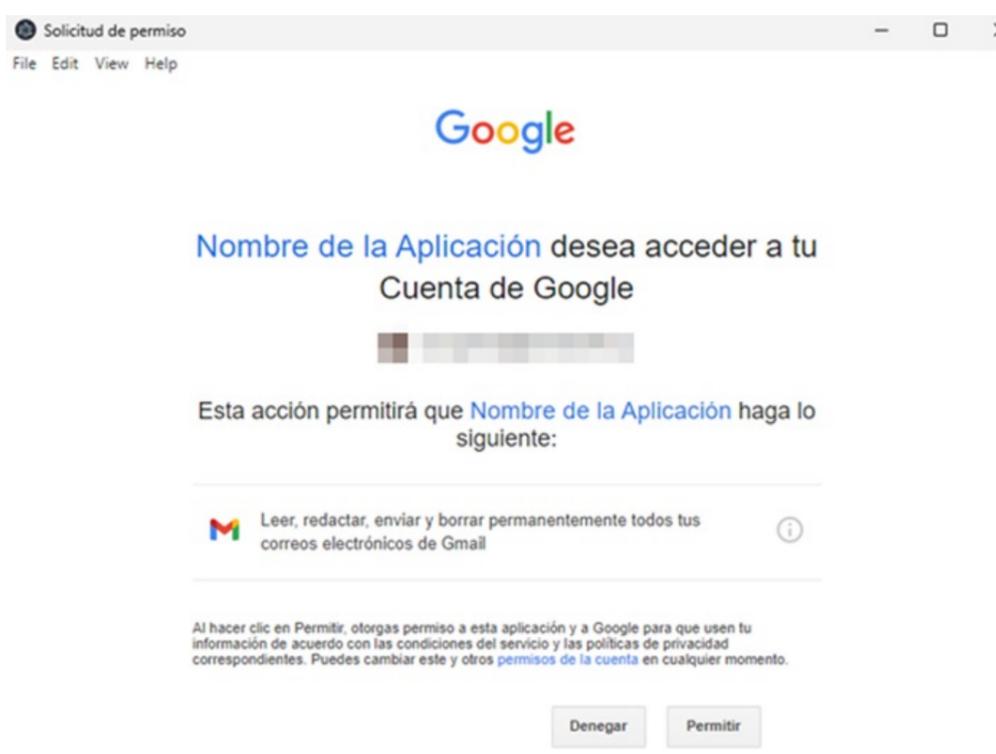
3. Al ingresar toda la información seleccione Get New Access Token.

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.

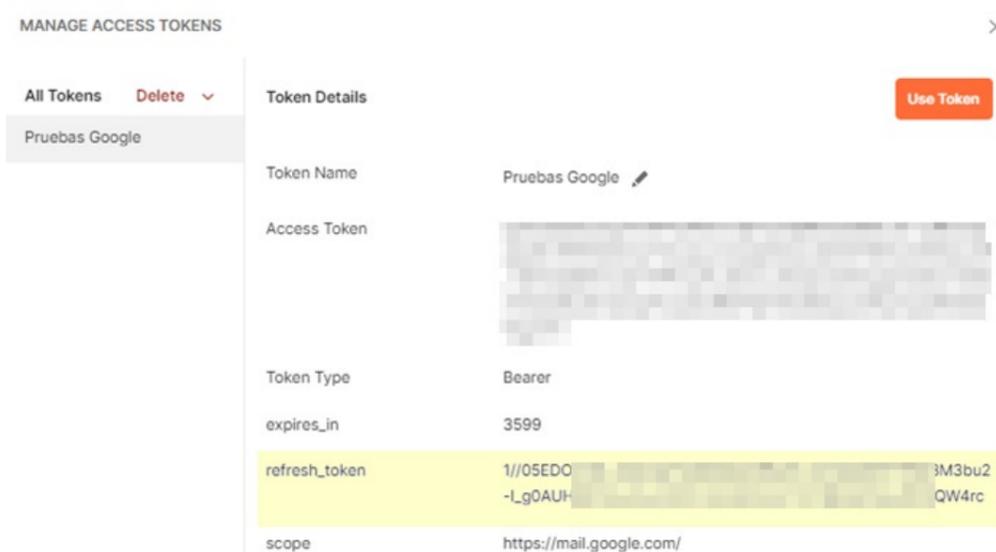
4. Se habilita la ventana de inicio de sesión en cuentas de Google; ingrese el correo y contraseña al que se requiere generar el refresh token.



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](#)

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.

<input type="checkbox"/>	Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
<input type="checkbox"/>	OU outlook	outlookoffice365.com	Basic	Diana Cortes	diana.cortes@arandasoft.c...
<input type="checkbox"/>	SN servidor Notificaciones	smtpoffice365.com	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...
<input type="checkbox"/>	SC Servidor Correo	https://dev-components-net...	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...

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

<input type="checkbox"/>	Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
<input type="checkbox"/>	OU outlook	outlookoffice365.com	Basic	Diana Cortes	diana.cortes@arandasoft.c...
<input type="checkbox"/>	SN servidor Notificaciones	smtpoffice365.com	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...
<input type="checkbox"/>	SC Servidor Correo	https://dev-components-net...	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...

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](#)

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

*Nombre del correo: *Servidor:

*Puerto: Nombre del remitente: Correo del remitente:

Establecer por defecto: NO
Habilitar SSL: NO

Tipo de autenticación

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

Básica Oauth

Requiere autenticación: NO

4. En la pestaña Tipo de Autenticación, podrá establecer 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.

The screenshot shows the 'Servidor de correo' configuration window. At the top, it says 'Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar'. Below this, there are input fields for '*Nombre del correo' and '*Servidor'. To the right, there are icons for save, close, and a dropdown. Below these are fields for '*Puerto' (set to 0), 'Nombre del remitente', and 'Correo del remitente'. On the right side, there are two toggle switches: 'Establecer por defecto' (set to NO) and 'Habilitar SSL' (set to NO). A section titled 'Tipo de autenticación' is highlighted. Below it, the text says 'Selección el tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar'. There are two radio buttons: 'Básica' (selected) and 'Oauth'. Below that, a toggle switch for 'Requiere autenticación' is set to 'SI'. A note says 'Los campos con * son obligatorios'. At the bottom, there are input fields for '*Usuario' and '*Contraseña'.

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 información relevante al proveedor de correo Oauth en el portal de Azure, generando los parámetros requeridos para los campos de autenticación 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 información relevante al proveedor de correo Oauth en el portal de Google, generando los parámetros requeridos para los campos de autenticación del servidor de correo:

- [ID del cliente, url de autorización, url de token y Secreto del Cliente](#)
- [Token de acceso y Token de actualización.](#)

The screenshot shows the 'Tipo de autenticación' configuration window. At the top, it says 'Selección el tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar'. There are two radio buttons: 'Básica' and 'Oauth' (selected). Below that, a dropdown menu for 'Proveedor' is set to 'Microsoft'. A note says 'Los campos con * son obligatorios'. Below this, there are four input fields: '*ID Cliente', '*Secreto del cliente (contraseña)', '*URL de autorización', and '*URL de token'. At the bottom, there are two more input fields: '*Token de acceso' and '*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.

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

Buscar todos los conceptos NUEVO ELIMINAR

<input type="checkbox"/>	Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
<input type="checkbox"/>	OU outlook	outlookoffice365.com	Basic	Diana Cortes	diana.cortes@arandasoft...
<input checked="" type="checkbox"/>	SN servidor Notificaciones	smtpoffice365.com	Basic	Notificaciones Documentac...	francisco.ramirez@arand...
<input type="checkbox"/>	SC Servidor Correo	https://dev-components-n...	Basic	Notificaciones Documentac...	francisco.ramirez@arand...

< 1 > Mostrando 1 al 3 de 3 registros

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

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

SN

*Nombre del correo: servidor Notificaciones

*Servidor: smtpoffice365.com

*Puerto: 0

Nombre del remitente: Notificaciones Documentacion

Correo del remitente: francisco.ramirez@arandasoft.com

Establecer por defecto: NO

Habilitar SSL: NO

Tipo de autenticación

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

Básica OAuth

Requiere autenticación: NO

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



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

Buscar todos los conceptos NUEVO ELIMINAR

<input type="checkbox"/>	Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
<input type="checkbox"/>	OU outlook	outlookoffice365.com	Basic	Diana Cortes	diana.cortes@arandasoft.c...
<input checked="" type="checkbox"/>	SN servidor Notificaciones	smtppoffice365.com	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...
<input type="checkbox"/>	SC Servidor Correo	https://dev-components-net...	Basic	Notificaciones Documentacion	francisco.ramirez@arandas...

< 1 > Mostrando 1 al 3 de 3 registros

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.

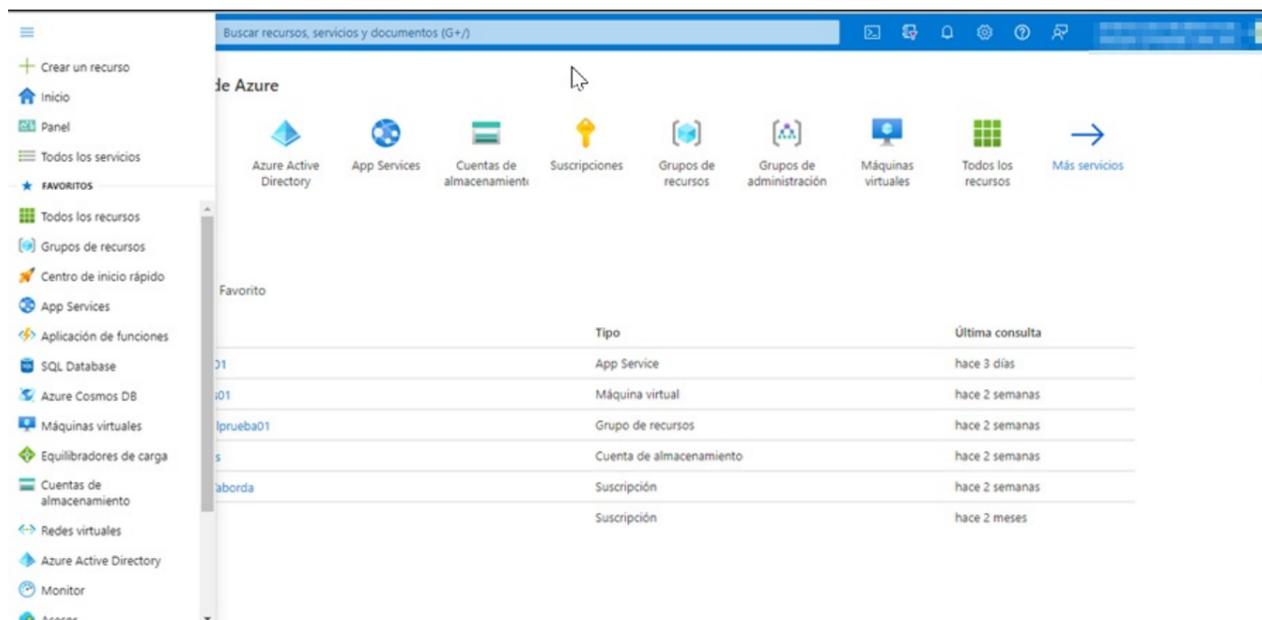
Para mayor información consulte la [Gestión Servicio de Directorios](#).

Sincronización Ldap/Microsoft Entra ID

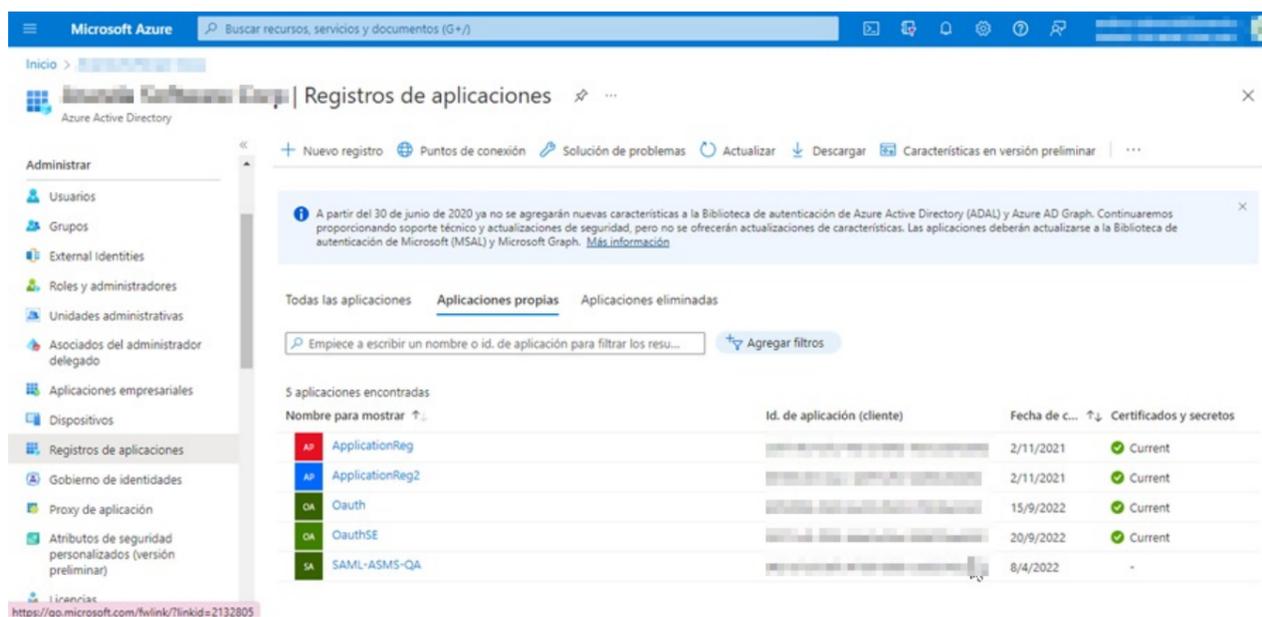
Crear Aplicación en Azure

► Requisitos Autenticación Azure: ►

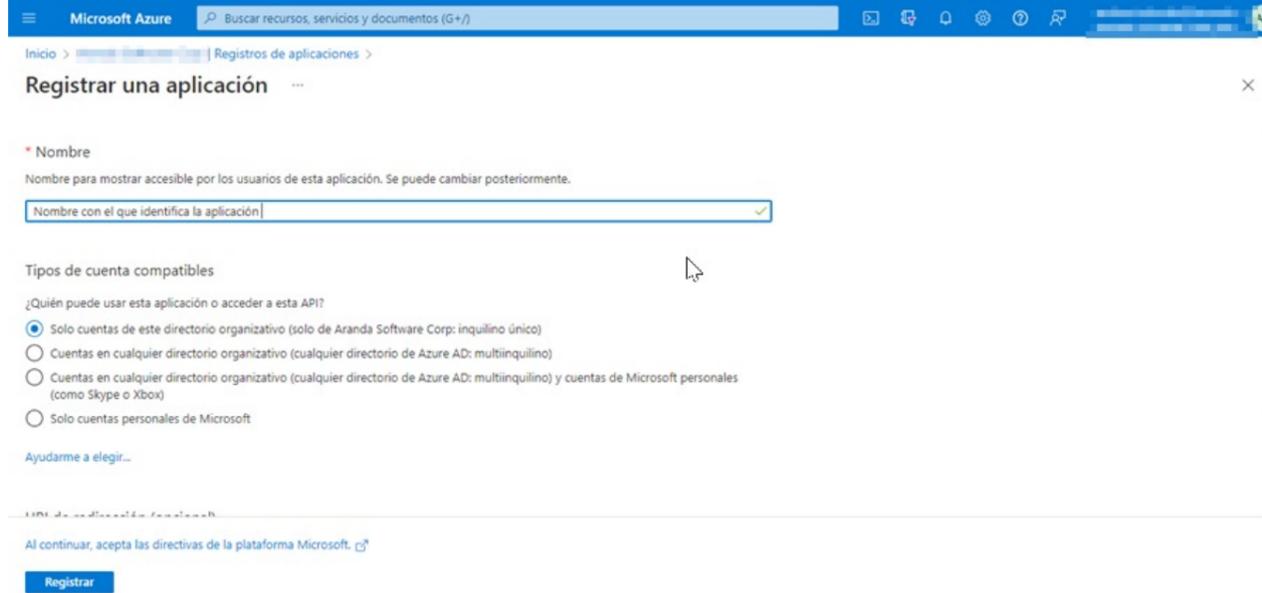
1. Se accede al portal de Azure [Ver Microsoft Azure](#), busque y seleccione Microsoft Entra ID.



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.

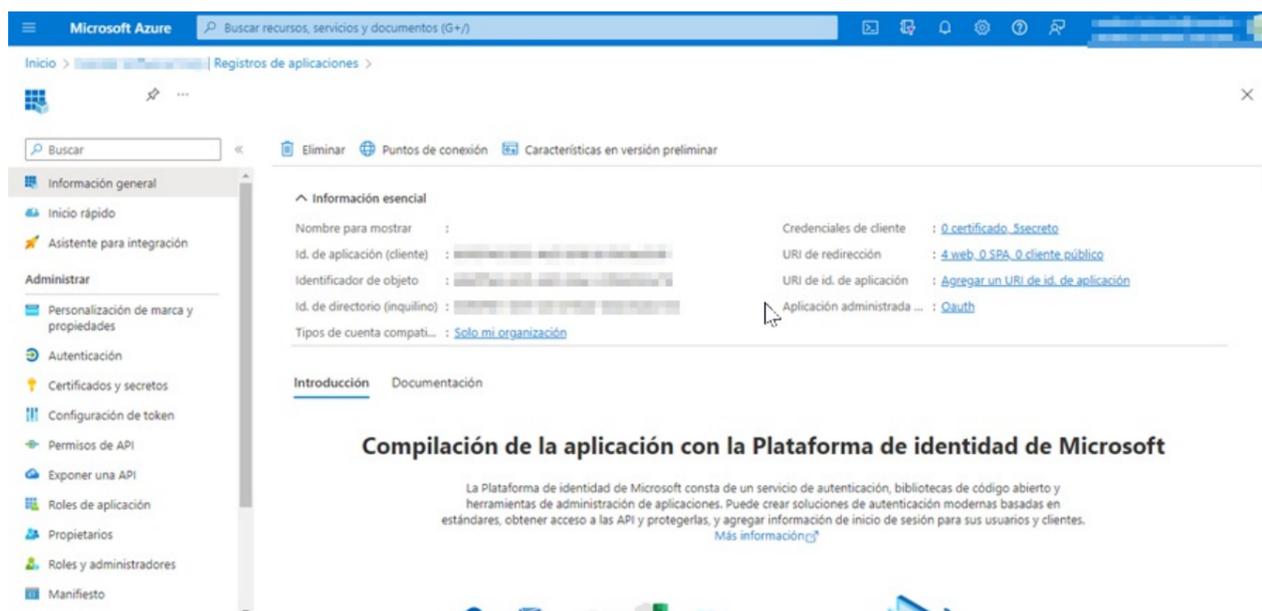


4. Cuando se tenga registrada la aplicación, guarde los siguientes datos que se requieren para la configuración en la sincronización de LDAP con Microsoft Entra ID.

- 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

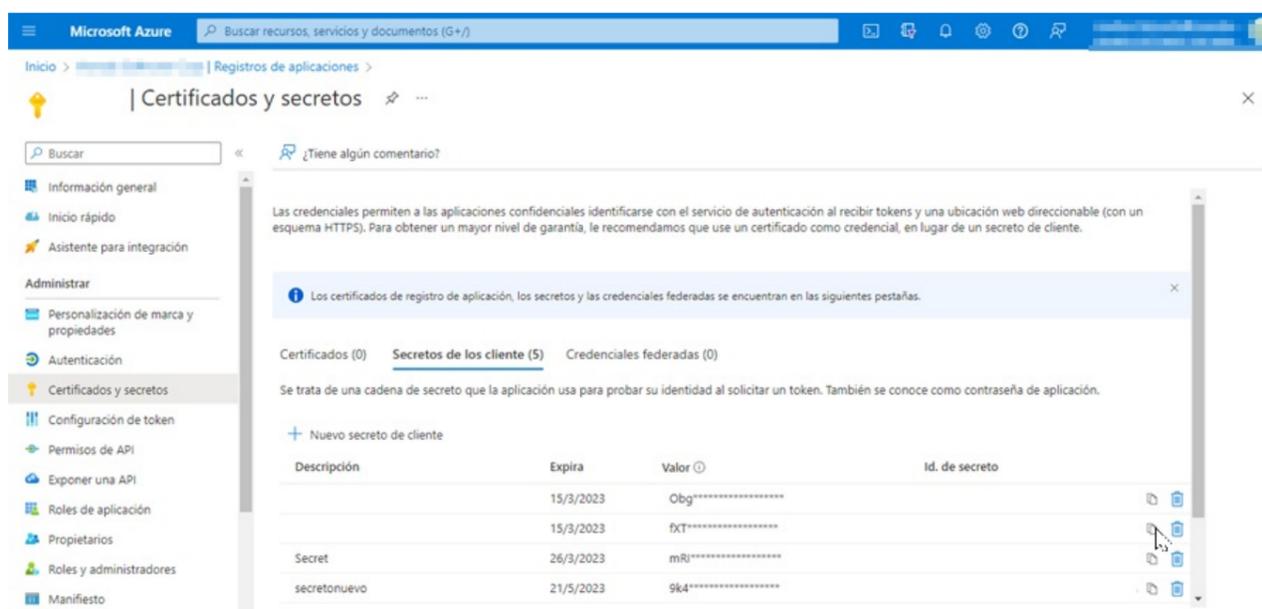


Configurar Aplicación Azure

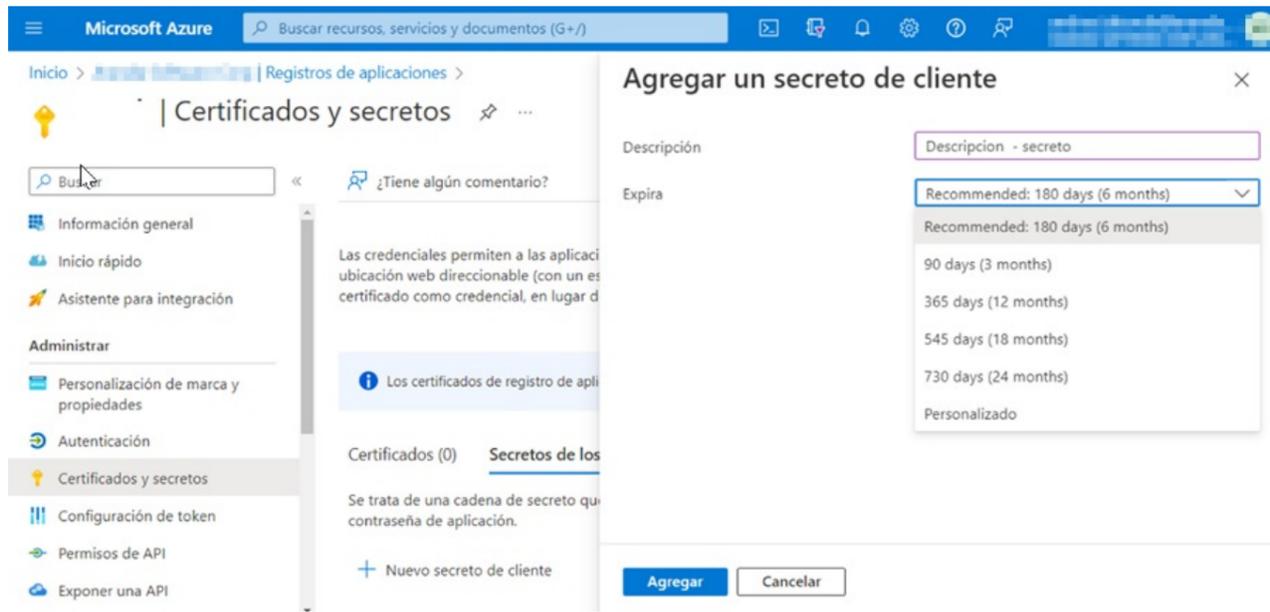
Cuando se tenga la aplicación creada y los datos guardados, podrá configurar la aplicación de la siguiente manera:

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.

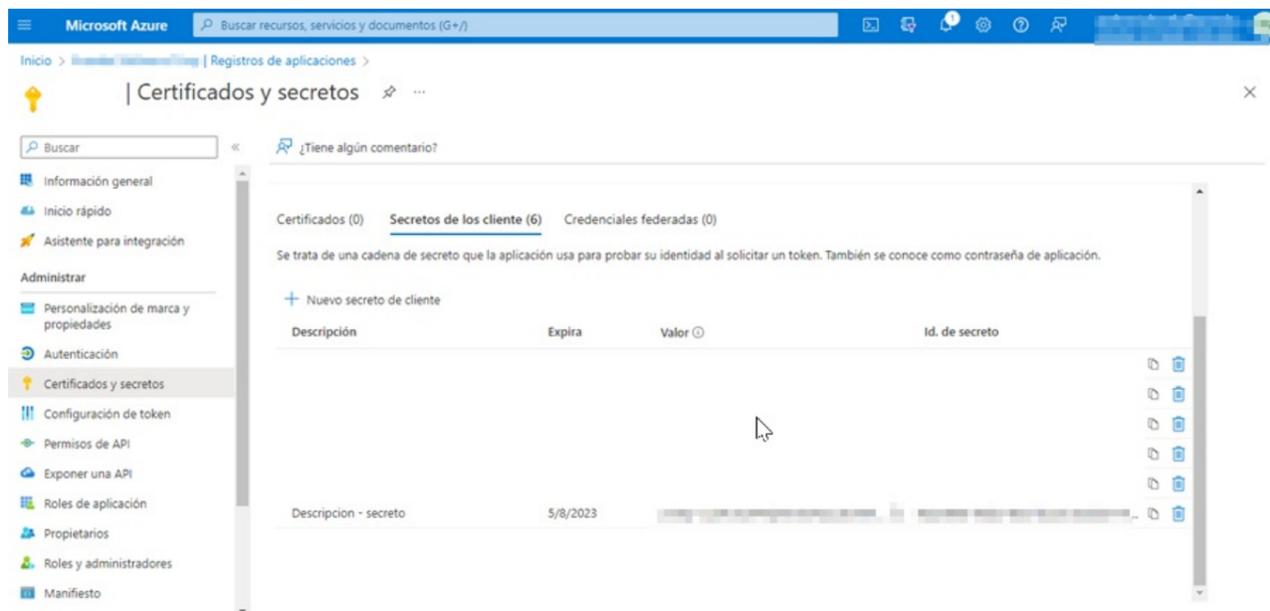


3. En la ventana Agregar un secreto de cliente diligencie el campo Descripción, defina la duración del secreto en el campo Expira y haga clic en el botón Agregar.



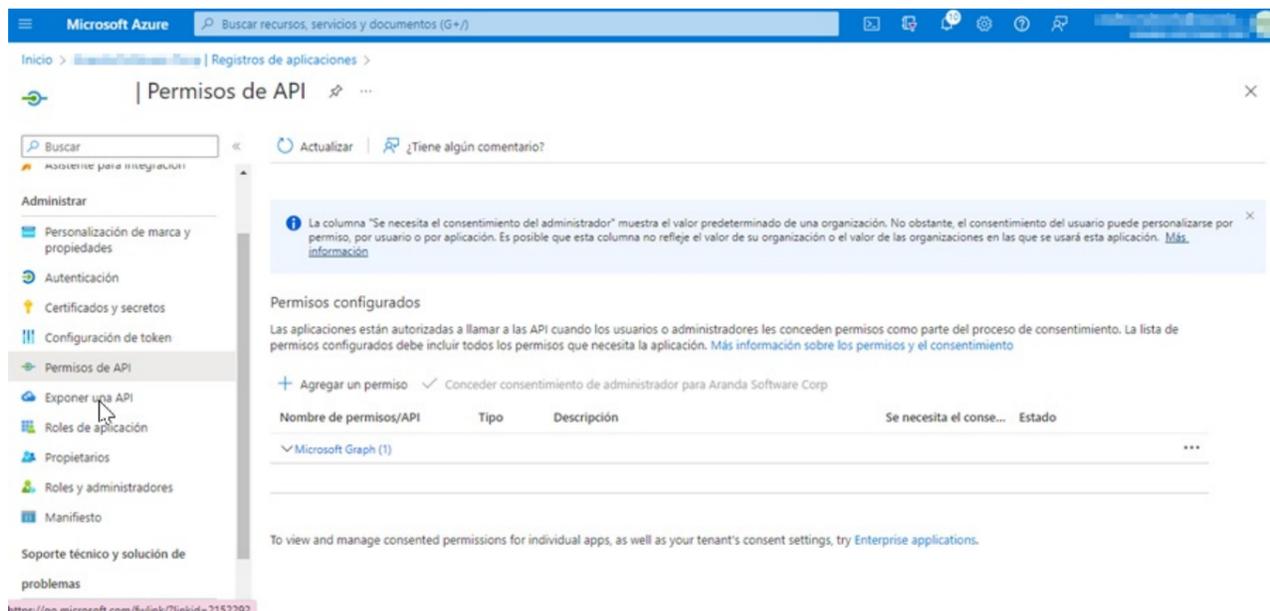
4. El valor del secreto sólo es visible cuando se crea; se debe guardar para usarlo más adelante o consultarlo durante las configuraciones que se requieran en los productos de Aranda.

- Valor secreto de cliente = Cliente secreto.

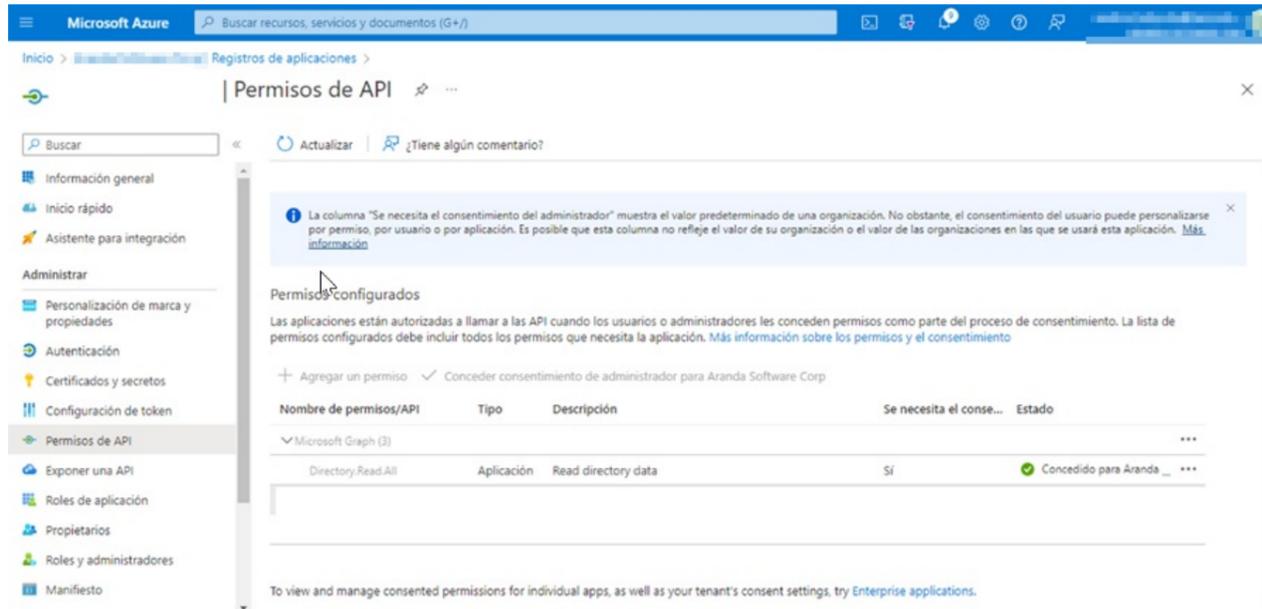
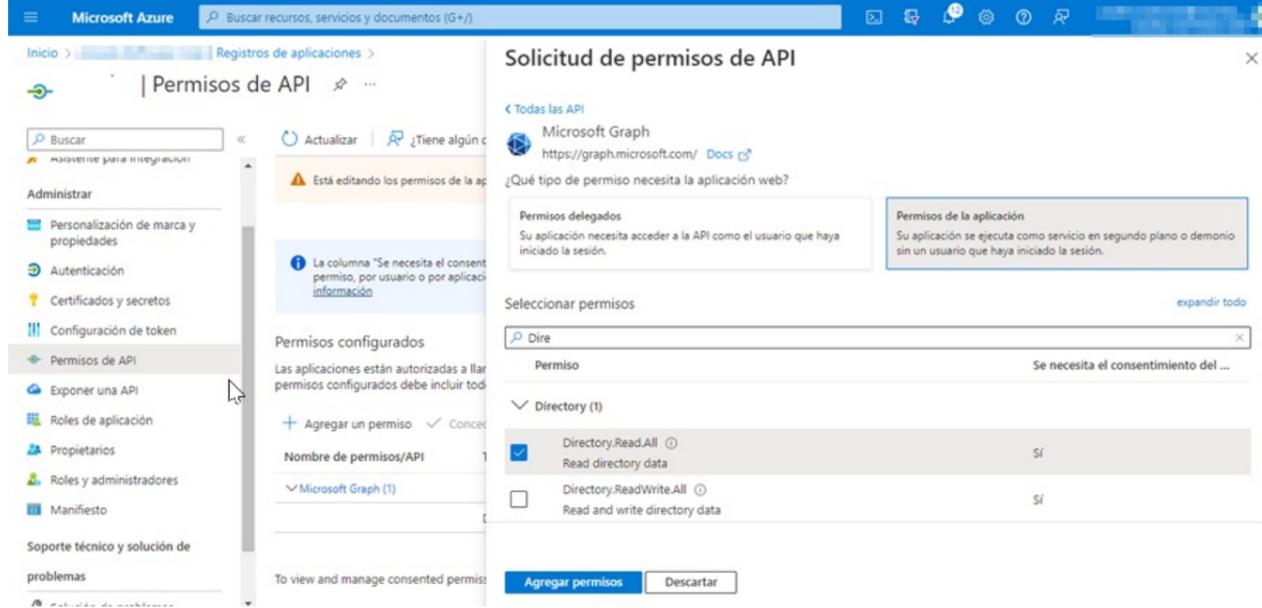


Configurar permisos de API

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

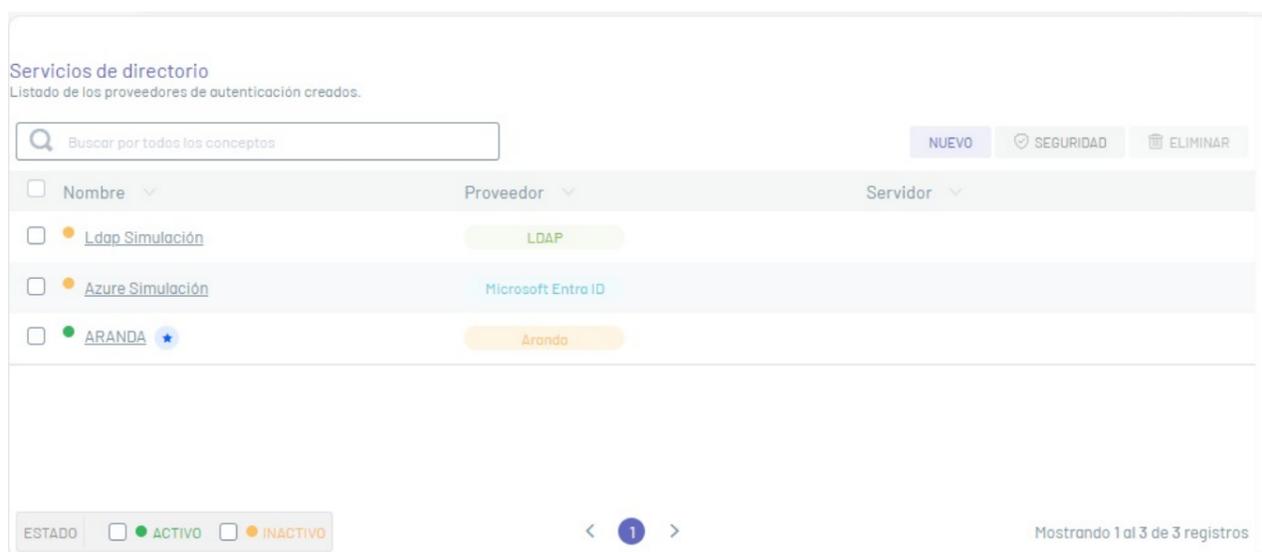
Para realizar la configuración de Ldap con Microsoft Entra ID en las aplicaciones Aranda, verifique el siguiente enlace:

- [Ver Sincronización y configuración 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.

Nombre	Proveedor	Servidor
<input type="checkbox"/> pruebaADM	External	192.168.3.2
<input type="checkbox"/> Ldap	LDAP	
<input type="checkbox"/> Azure	Microsoft Entra ID	
<input checked="" type="checkbox"/> ARANDA	Aranda	

Datos Básicos

2. En la ventana que se habilita podrá 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](#)

Nombre completo
INACTIVO

*Nombre completo
|

*Servidor LDAP
|

*Puerto
|

*Tipo de autenticación
Seleccione

*Formato de usuario
Seleccione

Estado ACTIVO INACTIVO

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

LDAP
Cree uno o varios directorios empresariales.

Microsoft Entra ID
Importar usuario de office 365.

Utilizar proveedor por defecto
 Usar distinción de nombre DN
 Habilitar SSL

IMPORTAR

Tipo de Autenticación

4. En la sección Tipo de Autenticación, podrá establecer 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 Microsoft, 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.

Importar
Seleccione el tipo de proveedor de autenticación para importar.

FR Francisco Jose Ramirez
LDAP

Servidor LDAP: <https://dev-components-netframework.azurewebsites.net/directoryservice>
 Usar distinción de nombre DN
 Utilizar proveedor por defecto

Puerto: 1
 Habilitar SSL
 Inactivo

*Tipo de autenticación: Básica
*Formato de usuario: Sólo nombre de usuario (usuario)

*Usuario:
*Contraseña:

Nombre distintivo: DC=interseq=DCLocal

Mapeo de usuarios | Mapeo de grupos

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

*Identificador único:

*Nombre de usuario	Correo electrónico	Nombre completo	Jefe Inmediato
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Identificación	País	Departamento	Ciudad
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Teléfono	Teléfono oficina	Teléfono oficina 2	Fax
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Móvil	Compañía	Ubicación oficina	Dirección
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Sede	Piso en el edificio	Cargo dentro de la compañía	Área de compañía
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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.

Importar
Seleccione el tipo de proveedor de autenticación para importar.

LS Ldap Simulación
LDAP

Servidor LDAP: <https://dev-components-netframework.azurewebsites.net/directoryservice>
 Usar distinción de nombre DN
 Utilizar proveedor por defecto

Puerto: 0
 Habilitar SSL
 Inactivo

*Tipo de autenticación: Anónima
*Formato de usuario: Sólo nombre de usuario (usuario)

*Usuario:
*Contraseña:

Nombre distintivo: DC=interseq=DCLocal

Mapeo de usuarios | **Mapeo de grupos**

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

Identificador único:

Nombre del grupo:

6. 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 sincronizar



y en la ventana que se habilita active la sincronización.

 Última ejecución
dd/MM/yyyy h:mm a Activo

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

Ejecutar ahora Programar

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.

 Última ejecución
dd/MM/yyyy h:mm a Activo

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

Ejecutar ahora Programar

Periodicidad

Una Vez Por Hora

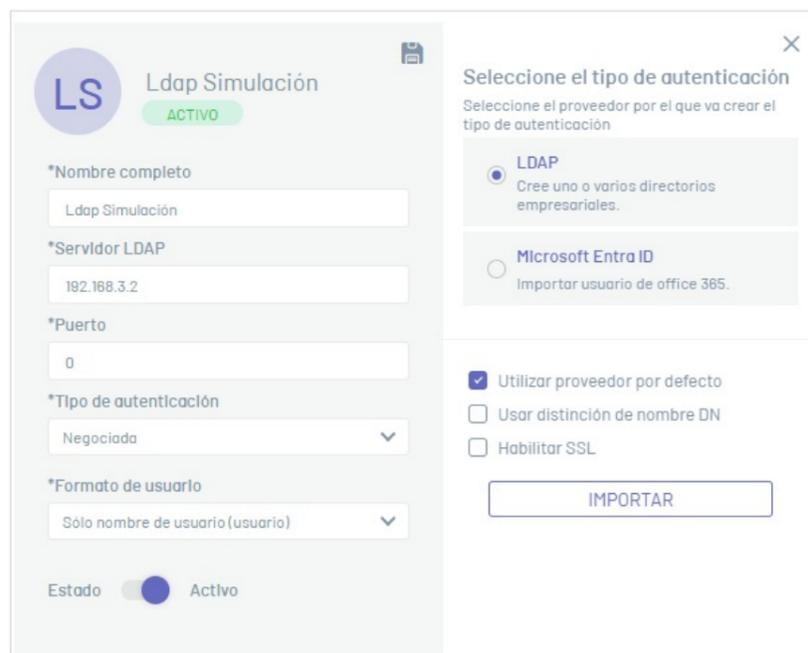
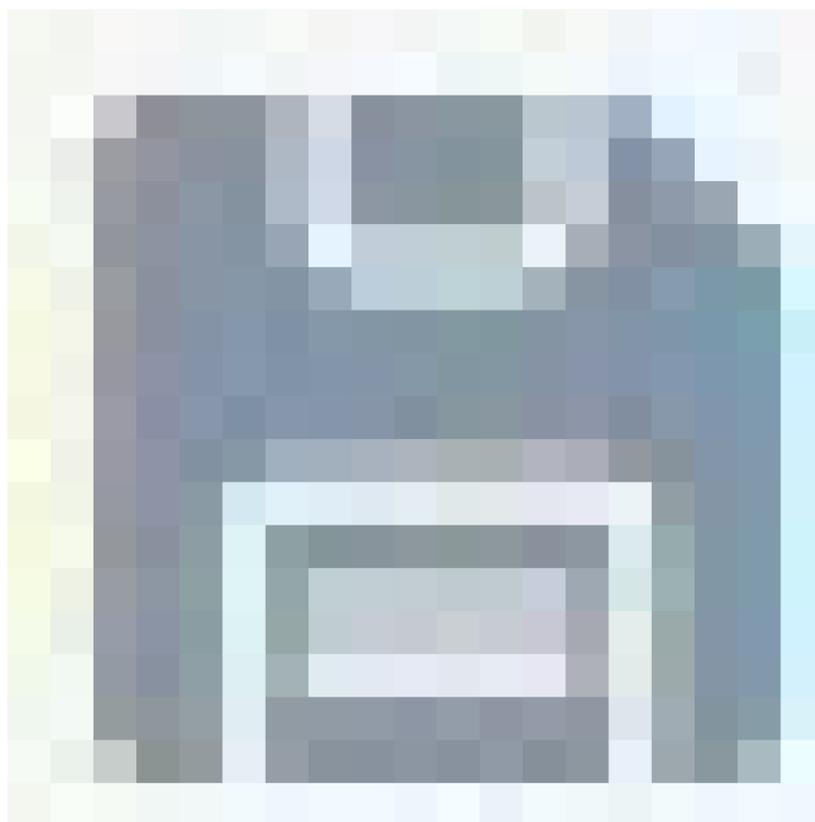
Iniciar en: 

Repetir cada: Hora(s)

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.

Importar
Seleccione el tipo de proveedor de autenticación para importar.

M MS
Microsoft Entra ID

*URL de autoridad *Identificador del cliente *Secreto del cliente

Mapeo de usuarios Mapeo de grupos

*Ingrese el filtro de usuario para tener en cuenta en la importación *Identificador único

*Nombre de usuario Correo electrónico Nombre completo Jefe inmediato

Identificación País Departamento Ciudad

Teléfono Teléfono oficina Teléfono oficina 2 Fax

Móvil Compañía Ubicación oficina Dirección

Sede Piso en el edificio Cargo dentro de la compañía Área de compañía

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.

Importar
Seleccione el tipo de proveedor de autenticación para importar.

P Proveedor
Microsoft Entra ID

*URL de autoridad *Identificador del cliente *Secreto del cliente

Mapeo de usuarios **Mapeo de grupos**

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

Nombre del grupo

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 sincronizar



y en la ventana que se habilita active la sincronización.

 Última ejecución
dd/MM/yyyy h:mm a Activo

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

Ejecutar ahora Programar

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 CONFIRMAR SINCRONIZACIÓN.

 Última ejecución
dd/MM/yyyy h:mm a Activo

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

Ejecutar ahora Programar

Periodicidad

Una Vez Por Hora

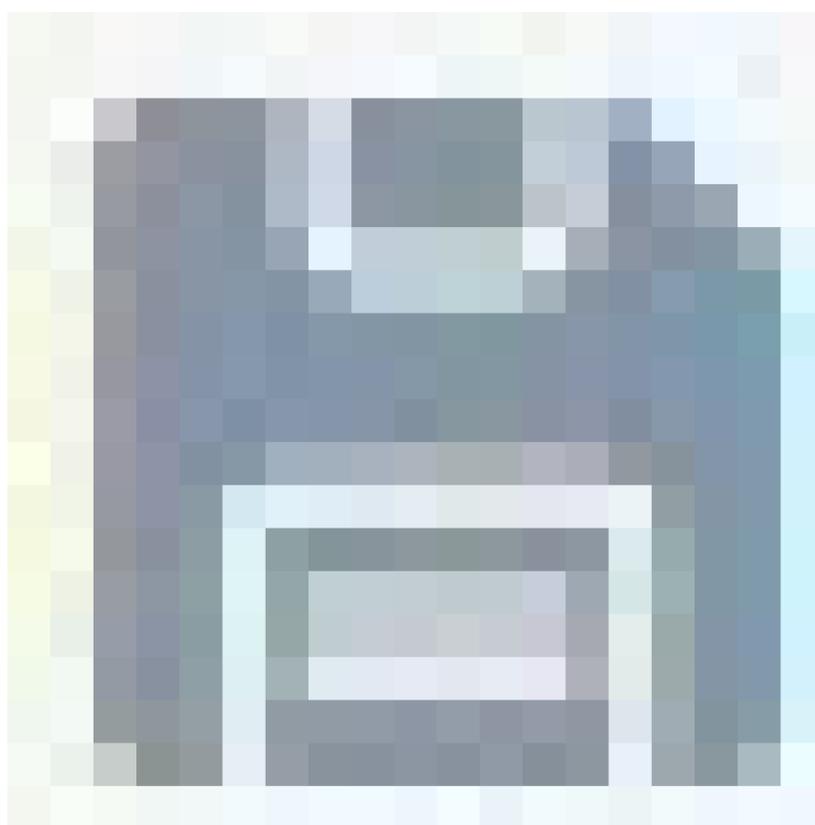
Iniciar en: 

Repetir cada: Hora(s)

9. Al terminar la configuración del directorio de Microsoft 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 la 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

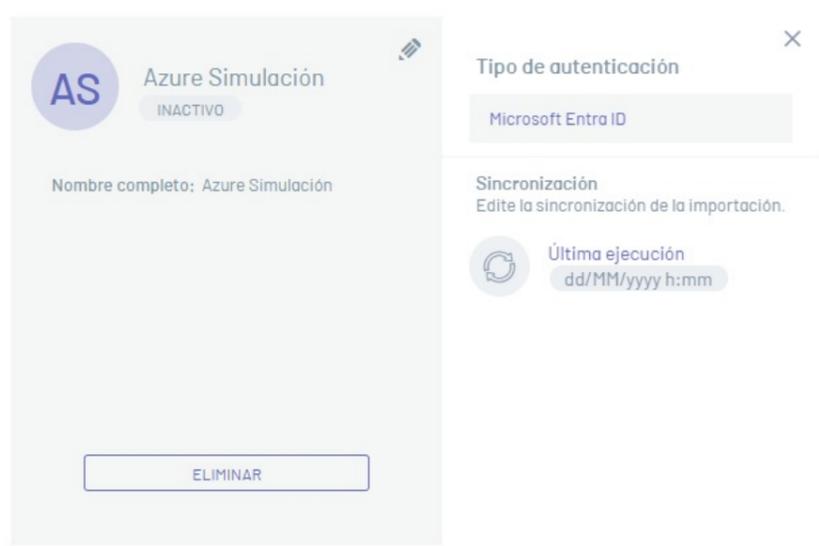
1. Para editar un directorio o proveedor de autenticación, en la vista de información de servicios de directorios , seleccione un registro del listado de proveedores existentes.

Nombre	Proveedor	Servidor
<input type="checkbox"/> pruebaADM	External	192.168.3.2
<input type="checkbox"/> Ldap	LDAP	
<input type="checkbox"/> Azure	Microsoft Entra ID	
<input checked="" type="checkbox"/> ARANDA	Aranda	

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



Servicios de directorio
Listado de los proveedores de autenticación creados.

Buscar por todos los conceptos

NUEVO SEGURIDAD ELIMINAR

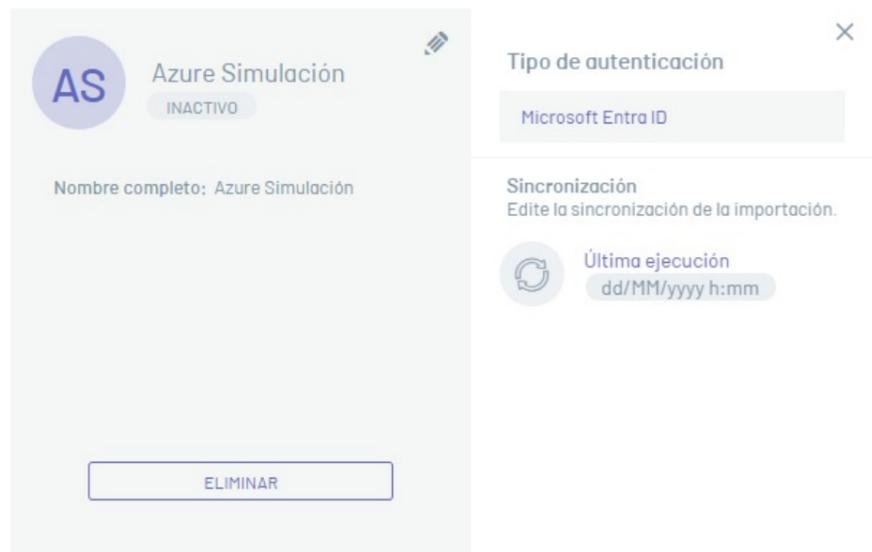
Nombre	Proveedor	Servidor
<input type="checkbox"/> pruebaADM	External	192.168.3.2
<input type="checkbox"/> Ldap	LDAP	
<input checked="" type="checkbox"/> Azure	Microsoft Entra ID	
<input type="checkbox"/> ARANDA	Aranda	

ESTADO ACTIVO INACTIVO

< 1 >

Mostrando 1 al 4 de 4 registros

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



Servicios de directorio

Listado de los proveedores de autenticación creados.

Buscar por todos los conceptos			NUEVO	SEGURIDAD	ELIMINAR
Nombre	Proveedor	Servidor			
<input type="checkbox"/> pruebaADM	External	192.168.3.2			
<input type="checkbox"/> Ldap Simulación	LDAP				
<input type="checkbox"/> Azure Simulación	Microsoft Entra ID				
<input type="checkbox"/> ARANDA	Aranda				

ESTADO ACTIVO INACTIVO

< 1 >

Mostrando 1 al 4 de 4 registros

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



reCAPTCHA

INACTIVO

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

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

Configuración

Seleccione la versión

Ninguna

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.

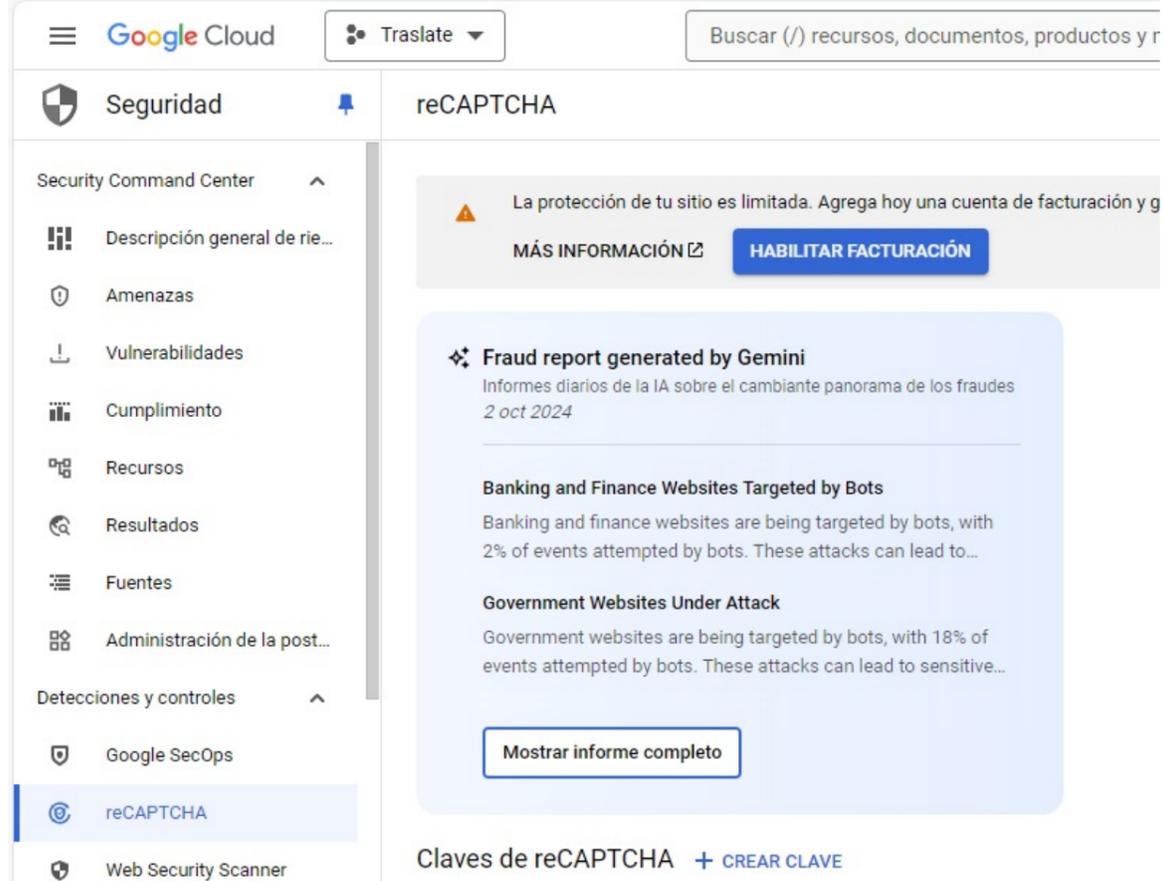
Nota: Se realiza redireccionamiento en la página, donde se permitirá la creación de las credenciales.

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.

Nombre visible *

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

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

Elegir tipo de plataforma *

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

Elegir tipo de plataforma *

- Sitio web
- App para Android
- App para iOS

Nota: Aparecerá la sección Lista de dominios.

6. Ingrese el nombre de dominio del sitio web:

Lista de dominios

AGREGAR UN DOMINIO

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

[FIREWALL DE APLICACIÓN WEB \(WAF\), VERIFICACIÓN DE DOMINIOS, PÁGINAS DE AMP Y DESAFÍO](#)

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

Nota: 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.

Tipo de clave

- Firewall de aplicación web (WAF) 
Para las implementaciones en la capa perimetral.
- This is a testing key
This key will return the same score for every assessment. A test key can't be changed to a regular key.
- Inhabilitar la verificación del dominio
- Use checkbox challenge 
Verifies users by requiring them to check "I'm not a robot" checkbox.
It can't be changed after the key is created.
- Permitir que esta clave funcione con las páginas AMP

```
- 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.  
<center></center>  
- Haga clic en Crear clave.  
<center></center>
```

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

DEMO ID: 6L

bxs 

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.

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

- 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.

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

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

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

- 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.
```

```
<center></center> - Haga clic en Crear clave.
```

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

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

Configurar reCAPTCHA V2

reCAPTCHA Versión 2

- Estando registrado en google ingrese a la [administración](#) de reCAPTCHA

WHAT IS RECAPTCHA?



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

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

[Learn More](#)

2. Agregue el valor del campo Etiqueta

Etiqueta ⓘ

demo.com

8 / 50

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"

Tipo de reCAPTCHA ⓘ

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

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



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

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

4. Agregue el valor del campo Dominios.

Dominios ⓘ

+ midemodominio.com

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

Google Cloud Platform

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

Nombre del proyecto*

reCaptcha

9 / 30

GOOGLE CLOUD PLATFORM

CANCELAR

ENVIAR

Nota: 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.

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

 **COPIAR CLAVE DE SITIO**

6Lcbd GDQKFtJr WEv HsEz

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

 **COPIAR CLAVE SECRETA**

6Lcbd AAFgCW r_DNAOr9B W1Ja3p

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

IR A CONFIGURACIÓN

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

Etiqueta 

demo.com

Tipo de reCAPTCHA: Casilla de verificación v2

Claves de reCAPTCHA 

Dominios 

 midemodominio.com

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

Propietarios

 arandasoftautomate@gmail.com

 Ingresar direcciones de correo electrónico

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

Preferencia de seguridad

La configuración más fácil para los usuarios La configuración más segura

Verificar el origen de las soluciones de reCAPTCHA

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

Enviar alertas a los propietarios

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

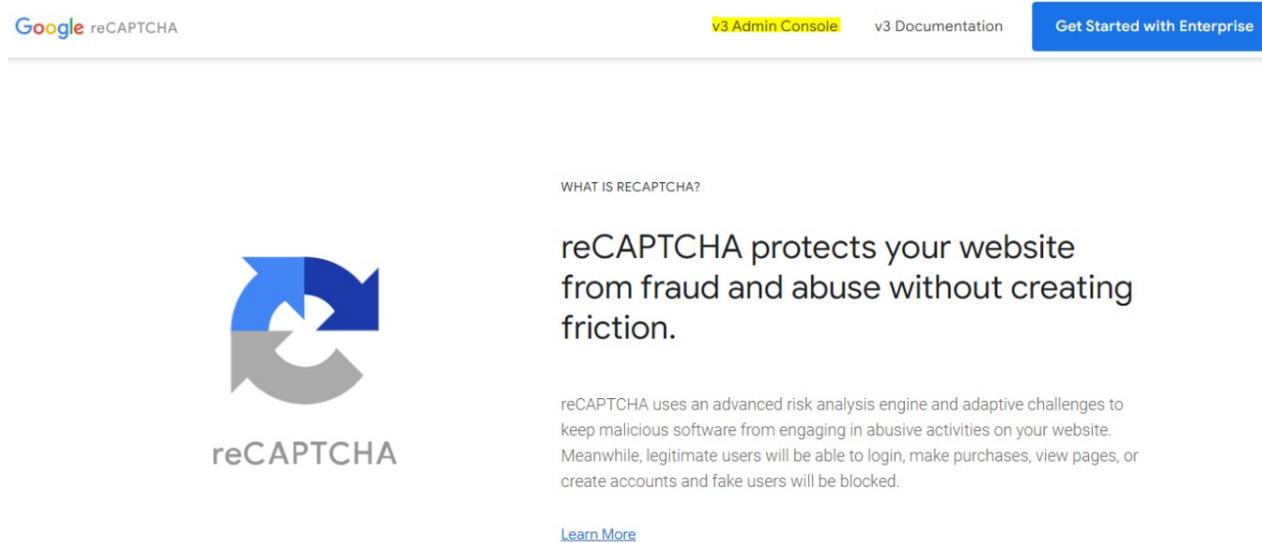
CANCELAR

GUARDAR

Configurar reCAPTCHA V3

reCAPTCHA Versión 3

1. Estando en registrado en google ingrese a la [administración](#) de reCAPTCHA



2. Agregue el valor del campo Etiqueta

Etiqueta i

demo.com

8 / 50

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

Tipo de reCAPTCHA i

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

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



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

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

4. Agregue el valor del campo Dominios.

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

Google Cloud Platform

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

Nombre del proyecto*

9 / 30

^ GOOGLE CLOUD PLATFORM

CANCELAR

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.

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

🔑 COPIAR CLAVE DE SITIO

6Lcbd GDQKFtJr WEv HsEz

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

🔑 COPIAR CLAVE SECRETA

6Lcbd AAFgCW r_DNAOr9B W1Ja3p

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

IR A CONFIGURACIÓN

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

Etiqueta

demo.com

Tipo de reCAPTCHA: v3

[VER EN LA CONSOLA DE CLOUD !\[\]\(f1c6cbc058dfea4ba2a2b55c6ed6b047_img.jpg\)](#)

Claves de reCAPTCHA 

Dominios

 midemo.com

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

Propietarios

 arandasoftautomate@gmail.com

 Ingresar direcciones de correo electrónico

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

- Verificar el origen de las soluciones de reCAPTCHA**
Si esta opción está inhabilitada, debes [revisar el nombre del host](#) en tu servidor al verificar una solución.
- Permitir que esta clave funcione con las páginas AMP**
Debes marcar esta casilla de verificación para usar [amp-recaptcha-input](#) en las páginas de AMP.
- Enviar alertas a los propietarios**
Recibe alertas si Google detecta problemas con tu sitio, como un error de configuración o un aumento del tráfico sospechoso.

CANCELAR

GUARDAR

Módulo 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:

Autenticación externa		
Listado de proveedores de autenticación creados.		
<input type="text" value="Buscar por nombre"/>	NUEVO  ELIMINAR	
<input type="checkbox"/> Nombre	Consola para la autenticación	Url de la consola
<input type="checkbox"/> ● Microsoft prueba	ASDK-Administrator.ExternalProviders	https://google.com.co

ESTADO ACTIVO INACTIVO Mostrando 1 al 1 de 1 registros

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).

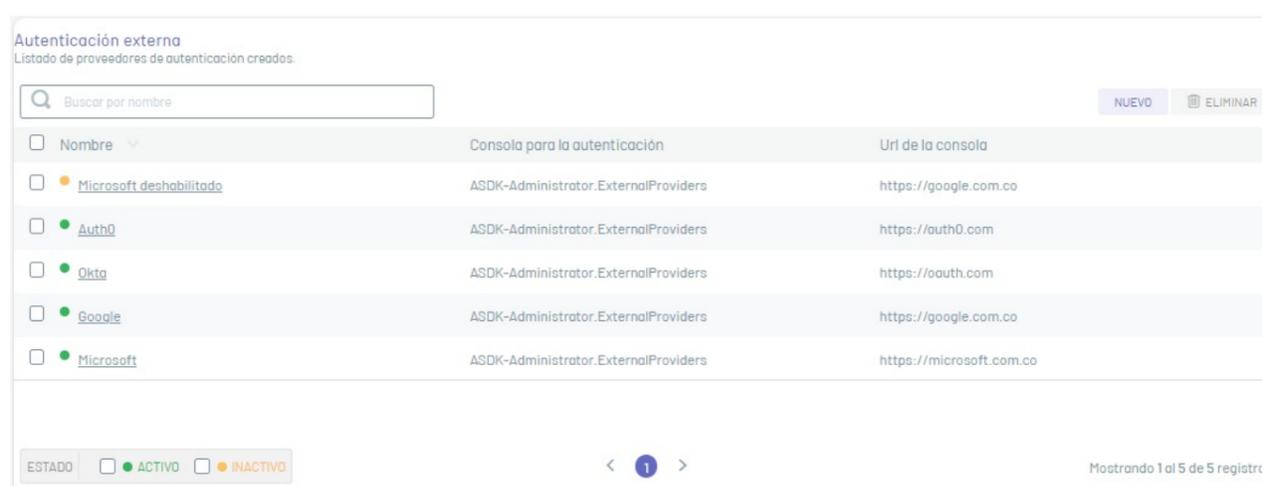
2. En la vista de información de proveedores externos, tendrá habilitadas acciones de gestión y organización de la información. [Vista de Información en Entorno Commons](#)

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.

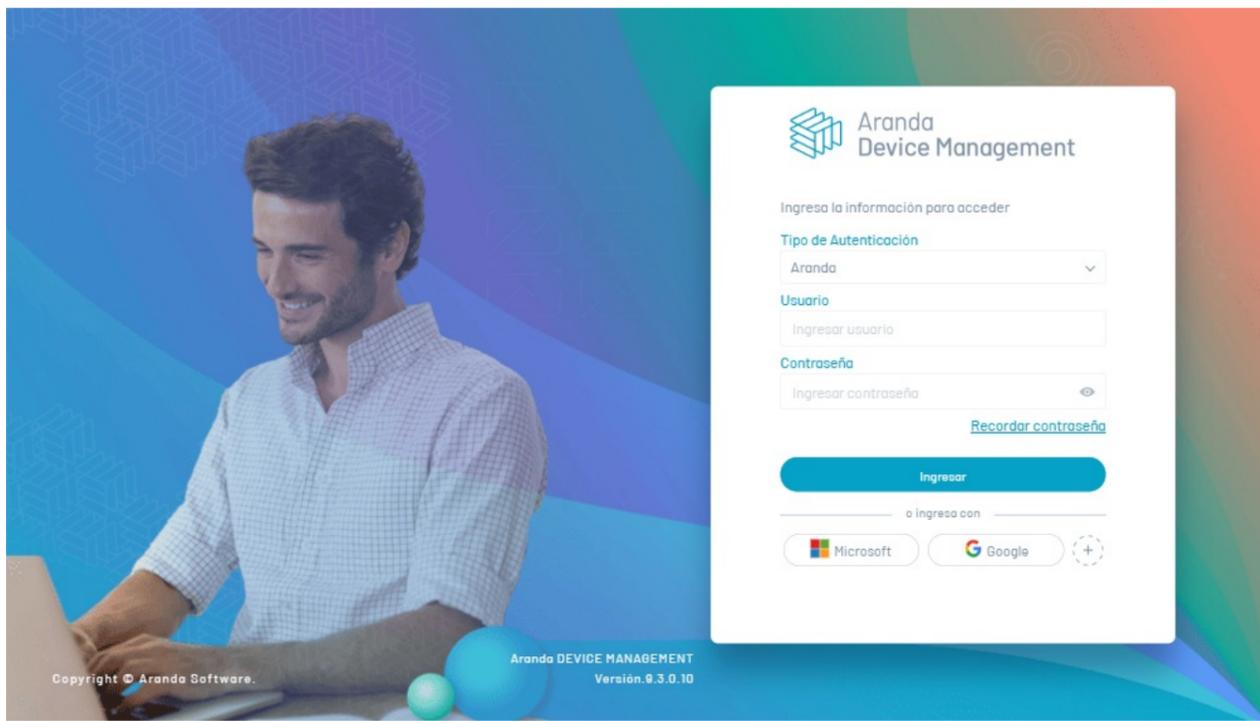
Cada uno de los campos de proveedor externo deben tener en cuenta las [especificaciones para campos](#)

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.

Autenticación externa
Listado de proveedores de autenticación creados.

Buscar por nombre NUEVO ELIMINAR

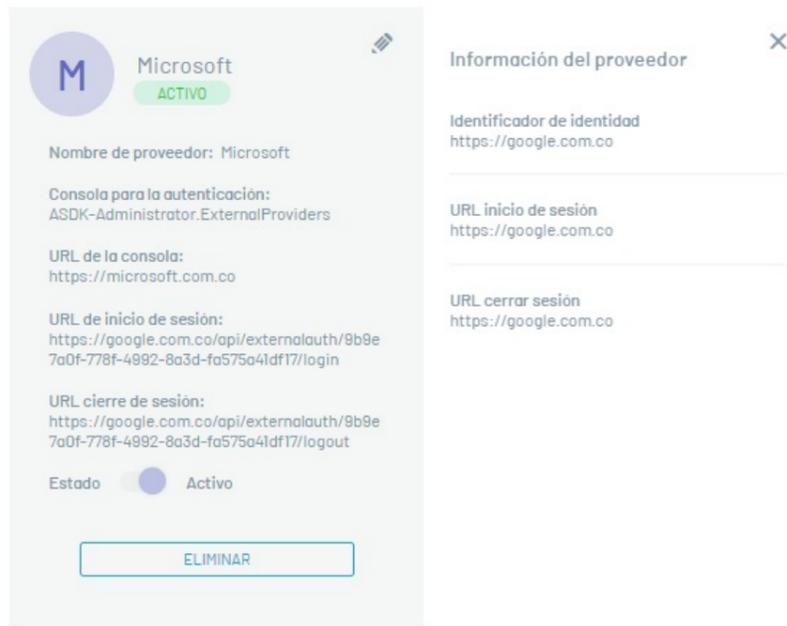
<input type="checkbox"/> Nombre	Consola para la autenticación	Url de la consola
<input type="checkbox"/> Microsoft deshabilitado	ASDK-Administrator.ExternalProviders	https://google.com.co
<input type="checkbox"/> Auth0	ASDK-Administrator.ExternalProviders	https://auth0.com
<input type="checkbox"/> Okta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

ESTADO ACTIVO INACTIVO < 1 > Mostrando 1 al 5 de 5 registros

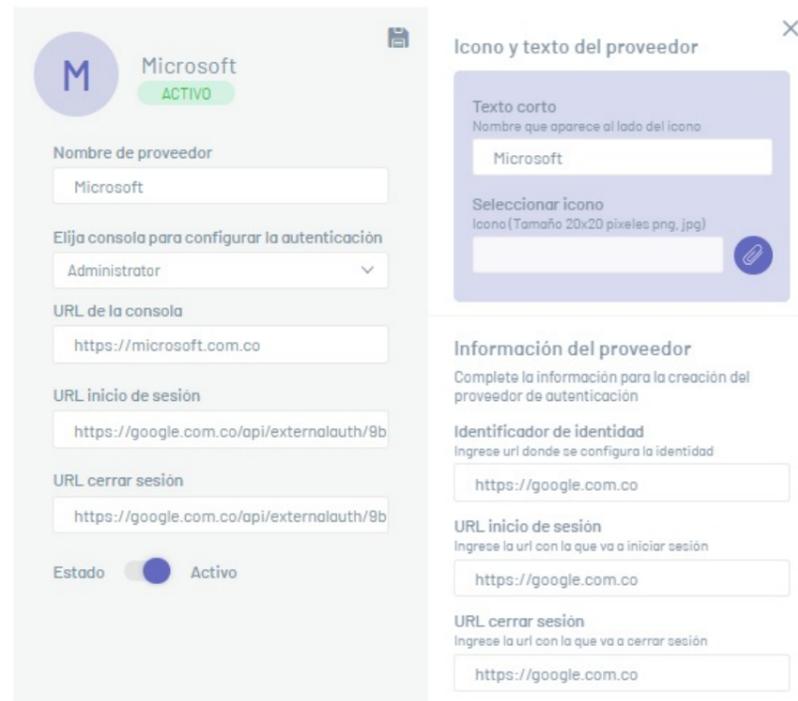
2. En la vista de detalle del proveedor, haga clic en el icono Editar



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 icono 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 creó 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



Autenticación externa
Listado de proveedores de autenticación creados.

Buscar por nombre NUEVO ELIMINAR

<input type="checkbox"/> Nombre	Consola para la autenticación	Uri de la consola
<input type="checkbox"/> ● Microsoft deshabilitado	ASDK-Administrator.ExternalProviders	https://google.com.co
<input checked="" type="checkbox"/> ● Auth0	ASDK-Administrator.ExternalProviders	https://auth0.com
<input checked="" type="checkbox"/> ● Okta	ASDK-Administrator.ExternalProviders	https://oauth.com
<input type="checkbox"/> ● Google	ASDK-Administrator.ExternalProviders	https://google.com.co
<input type="checkbox"/> ● Microsoft	ASDK-Administrator.ExternalProviders	https://microsoft.com.co

ESTADO ● ACTIVO ● INACTIVO Mostrando 1 al 5 de 5 registros

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

Google
ACTIVO

Nombre de proveedor: Google

Consola para la autenticación:
ASDK-Administrator.ExternalProviders

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

URL de inicio de sesión:
https://google.com.co/api/externalauth/9b9e7a0f-778f-4992-8a3d-fa575a4df17/login

URL cierre de sesión:
https://google.com.co/api/externalauth/9b9e7a0f-778f-4992-8a3d-fa575a4df17/logout

Estado: Activo

[ELIMINAR](#)

Información del proveedor

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

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

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

3. 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:

Configuración de API
Listado de tokens de conexiones de API creados.

Buscar por todos los conceptos NUEVO ELIMINAR

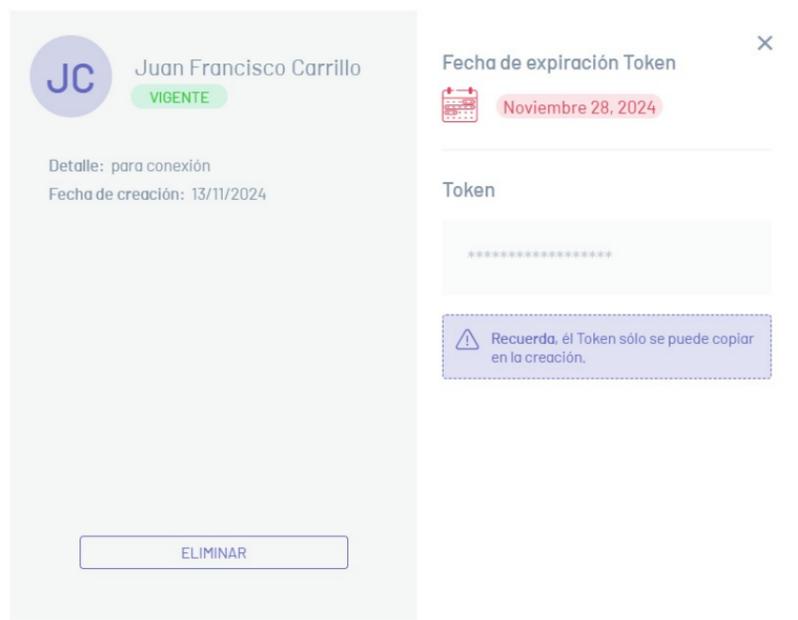
<input type="checkbox"/> Nombre de usuario	Descripción	Fecha de creación	Fecha de expiración Token
<input type="checkbox"/> ● APPLICATION ADMINISTRATOR	token datos	19/11/2024 9:47:23 am	04/11/2024 11:59:00 pm
<input type="checkbox"/> ● APPLICATION ADMINISTRATOR	Token descripcion	19/11/2024 9:46:57 am	23/11/2024 11:59:00 pm

ESTADO ● VIGENTE ● VENCIDO Mostrando 1 al 2 de 2 registros

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.

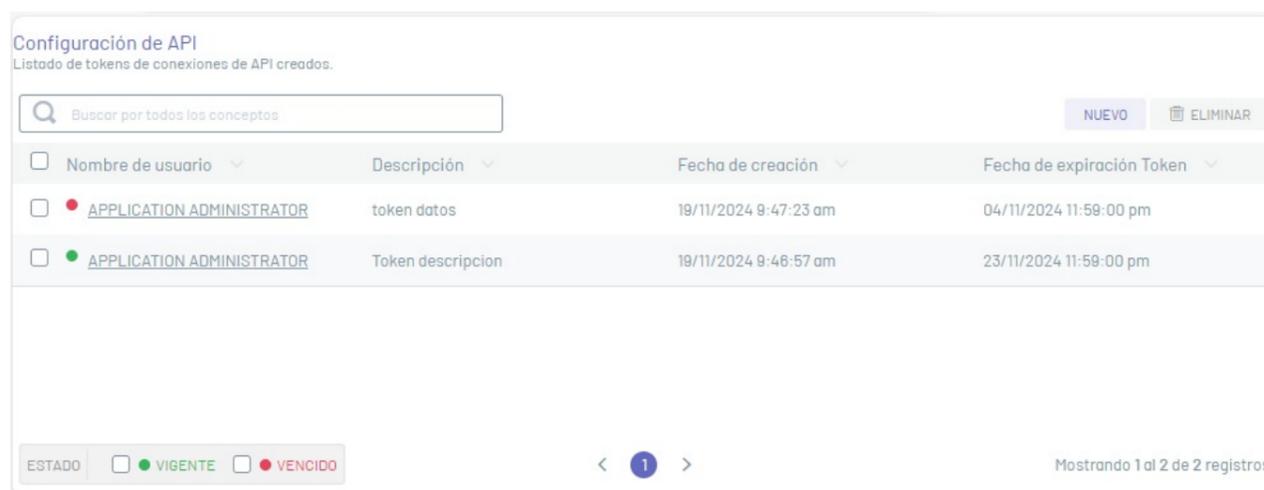


Enlaces Relacionados:

- [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](#)



ELIMINAR

para borrar la información asociada.

Configuración de API
Listado de tokens de conexiones de API creados.

Buscar por todos los conceptos NUEVO ELIMINAR

<input type="checkbox"/> Nombre de usuario	Descripción	Fecha de creación	Fecha de expiración Token
<input type="checkbox"/> ● APPLICATION ADMINISTRATOR	Documentacion	19/11/2024 10:41:28 am	28/11/2024 11:59:00 pm
<input checked="" type="checkbox"/> ● APPLICATION ADMINISTRATOR	token datos	19/11/2024 9:47:23 am	04/11/2024 11:59:00 pm
<input type="checkbox"/> ● APPLICATION ADMINISTRATOR	Token descripcion	19/11/2024 9:46:57 am	23/11/2024 11:59:00 pm

ESTADO ● VIGENTE ● VENCIDO < 1 > Mostrando 1 al 3 de 3 registros

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