En los procesos de configuración de Aranda SERVICE DESK ASDK V8, conozca la configuración para Autenticación moderna Oauth/Microsoft.

Autenticación OAuth 2.0 - Microsoft

Precondiciones

1. Una cuenta de Azure con permisos para administrar aplicaciones en Azure Active Directory (Azure AD). Cualquiera de los siguientes roles de Azure AD incluye los permisos necesarios:

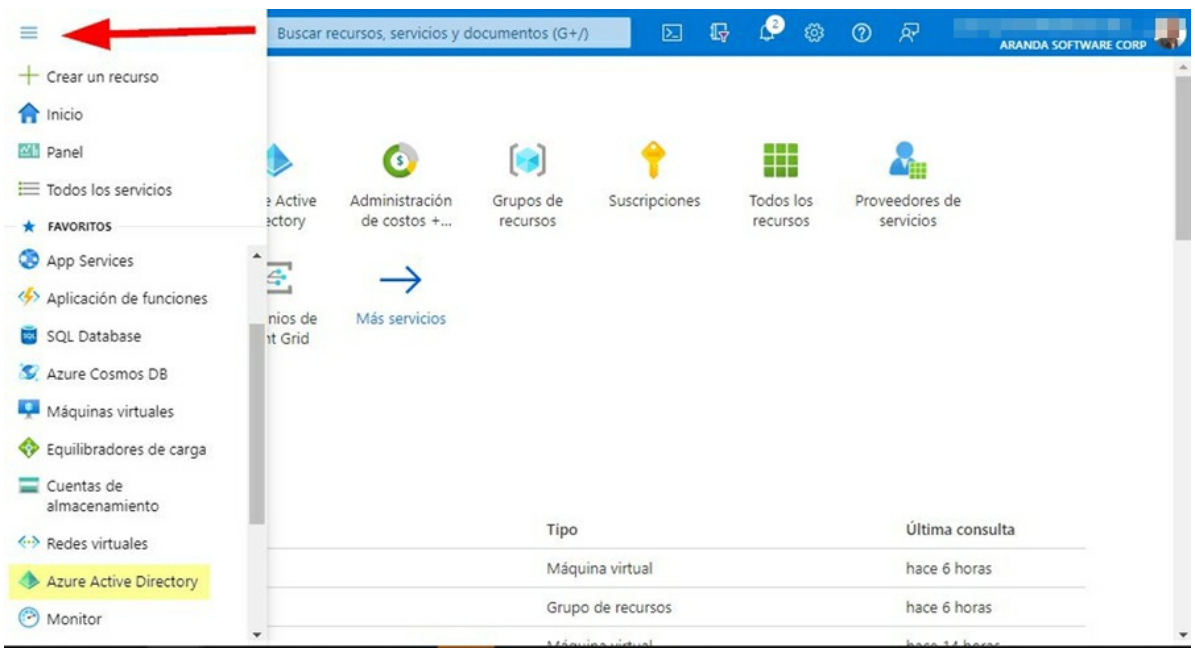
- Administrador de aplicaciones.
- Desarrollador de aplicaciones.
- Administrador de aplicaciones en la nube.

2. Aplicación POSTMAN para la solicitud del refresh_token.

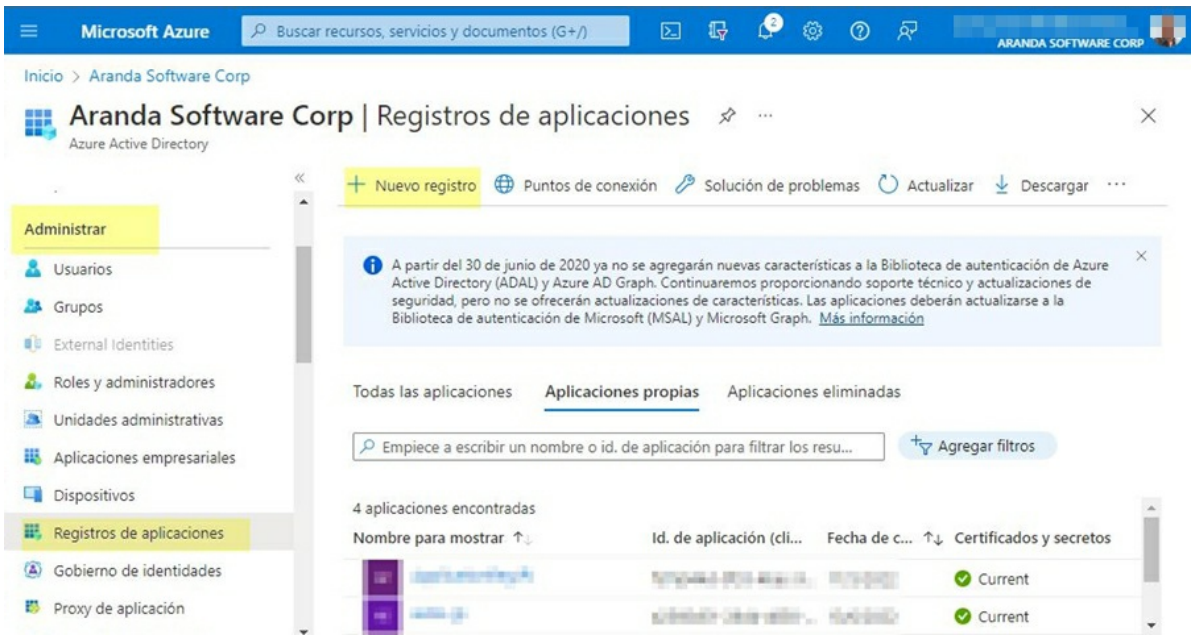
Creacion Aplicación en Azure

Cómo crear una aplicación en 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**.



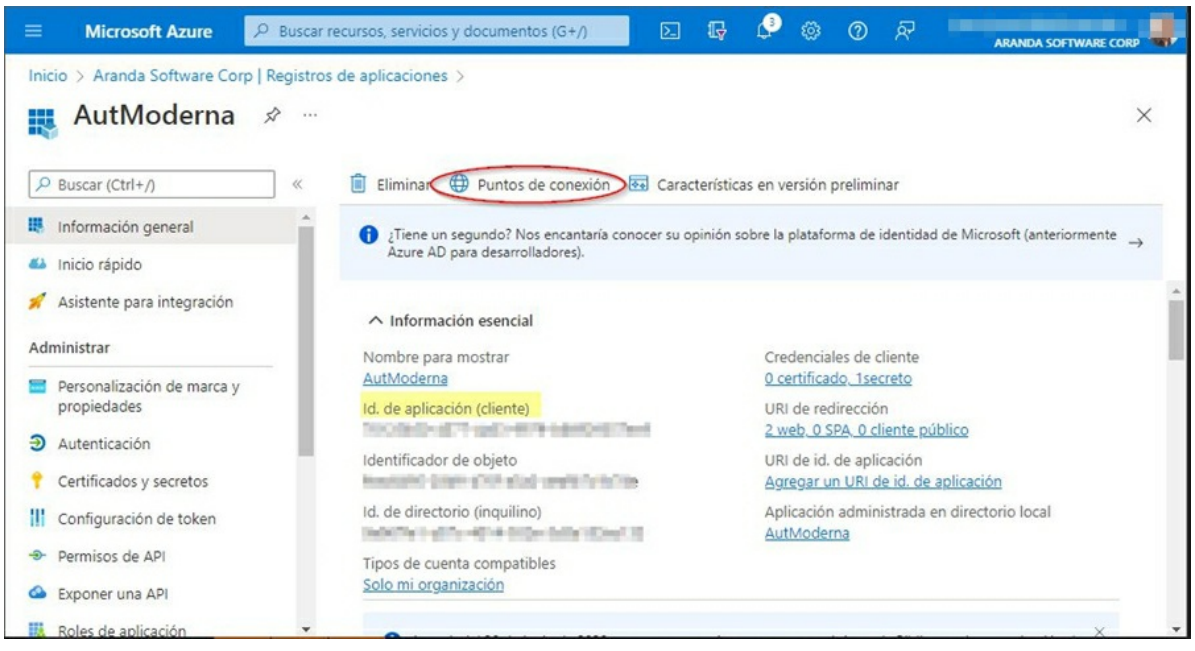
3. Se diligencia el campo del nombre y se selecciona la opción deseada en (Tipos de cuenta compatibles), clic en Registrar.

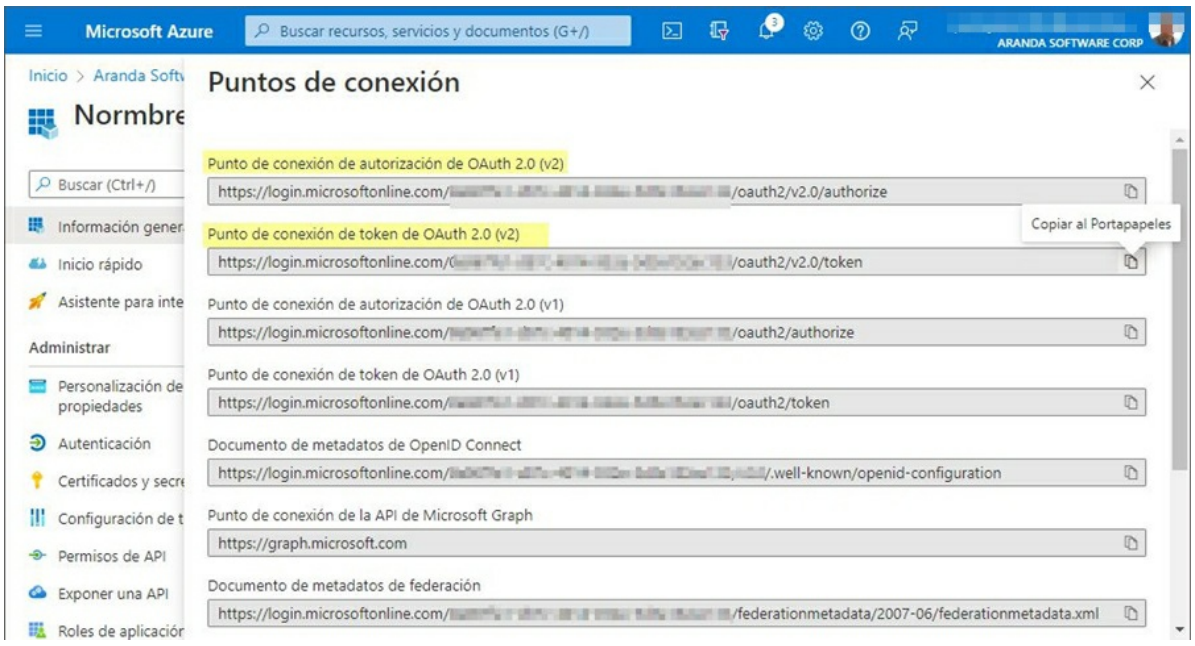
4.Cuando se tenga registrada la aplicación, guarde los siguientes datos que se requieren para la configuración en las aplicaciones de Aranda.

- 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.





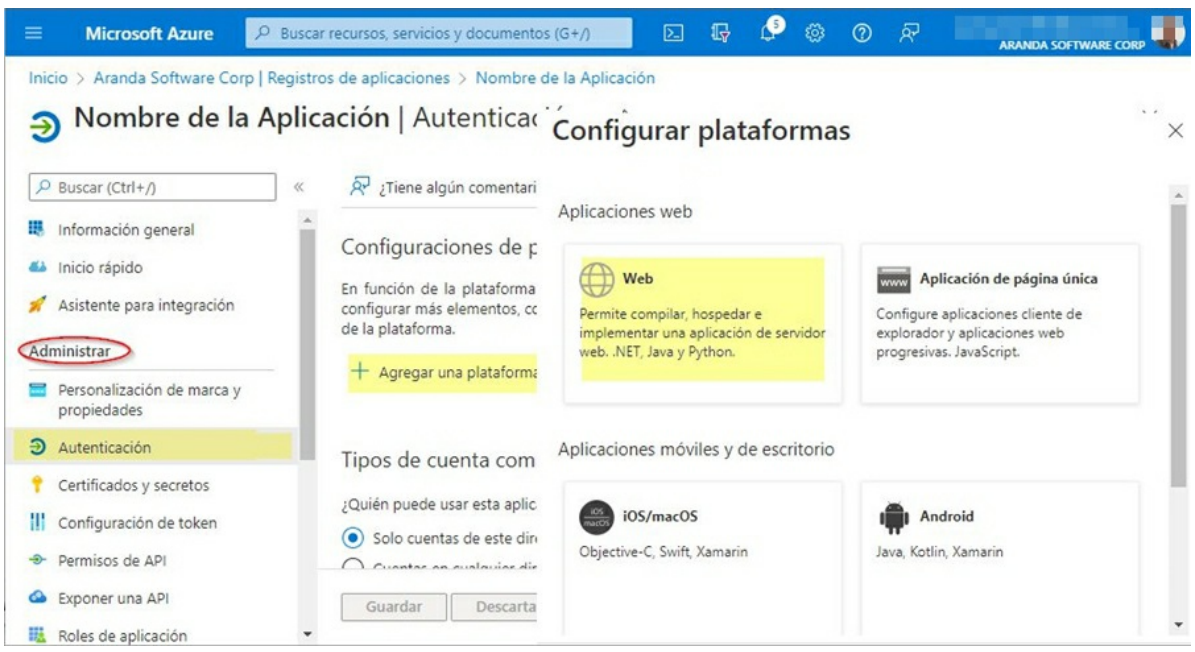
Configuración de la aplicación en el portal Azure

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

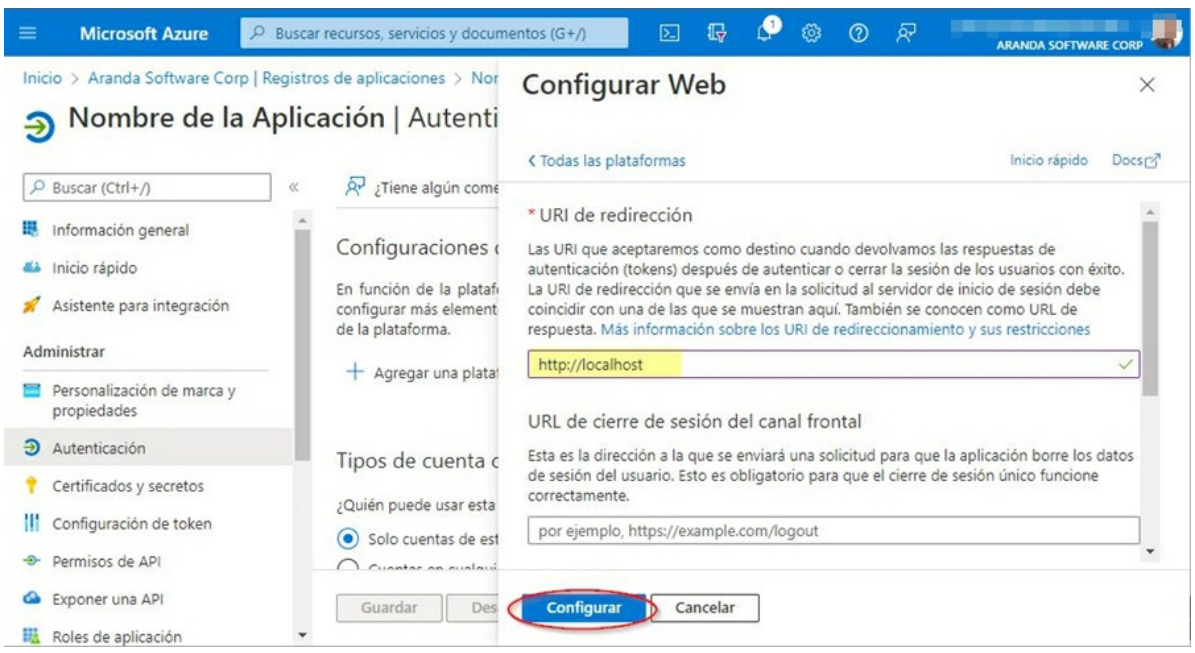
Cómo configurar la autenticación

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**.



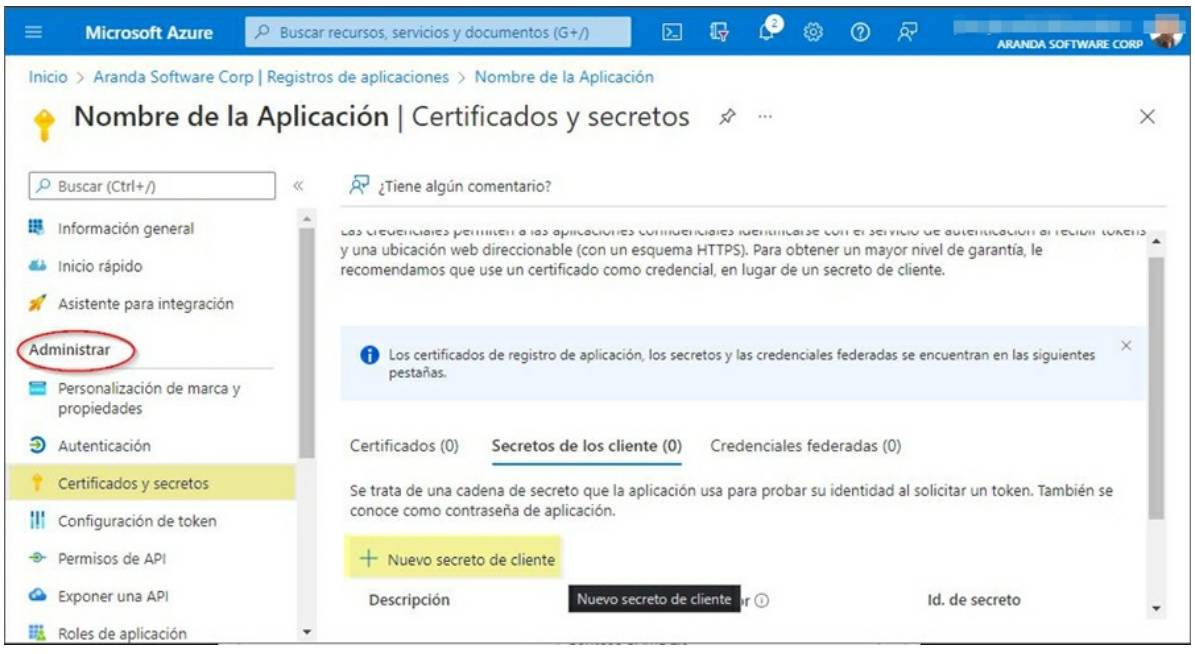
3. En el campo URI de redirección agregamos el siguiente valor http://localhost, y luego seleccionamos Configurar.



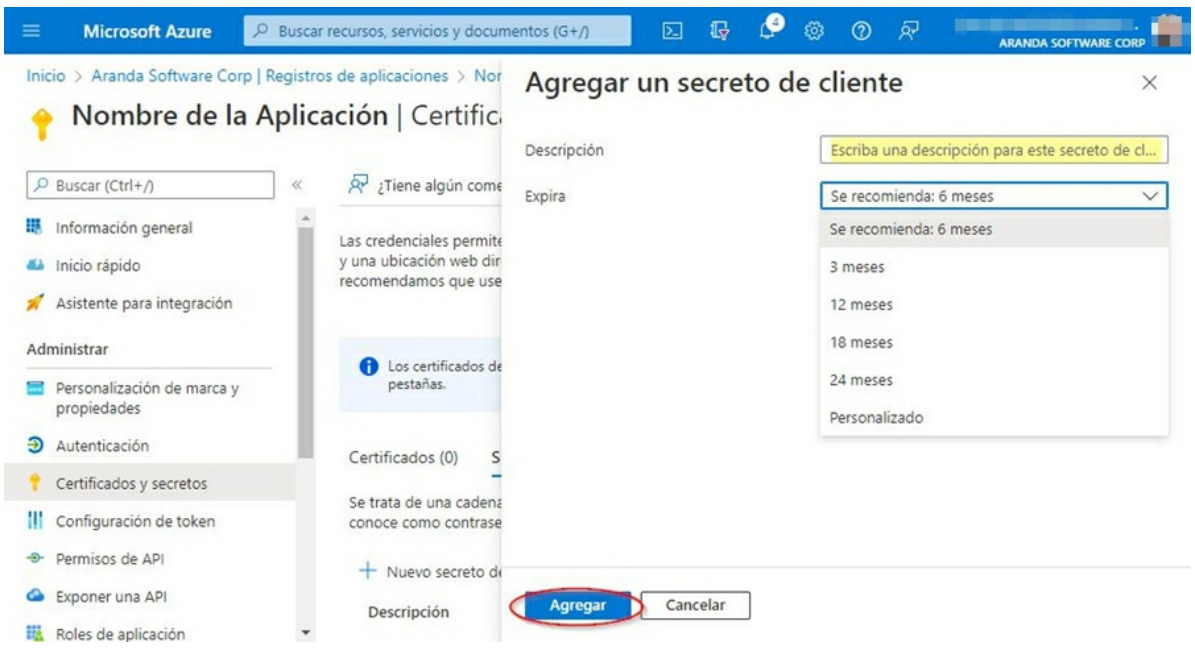
Creación del Secreto

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

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

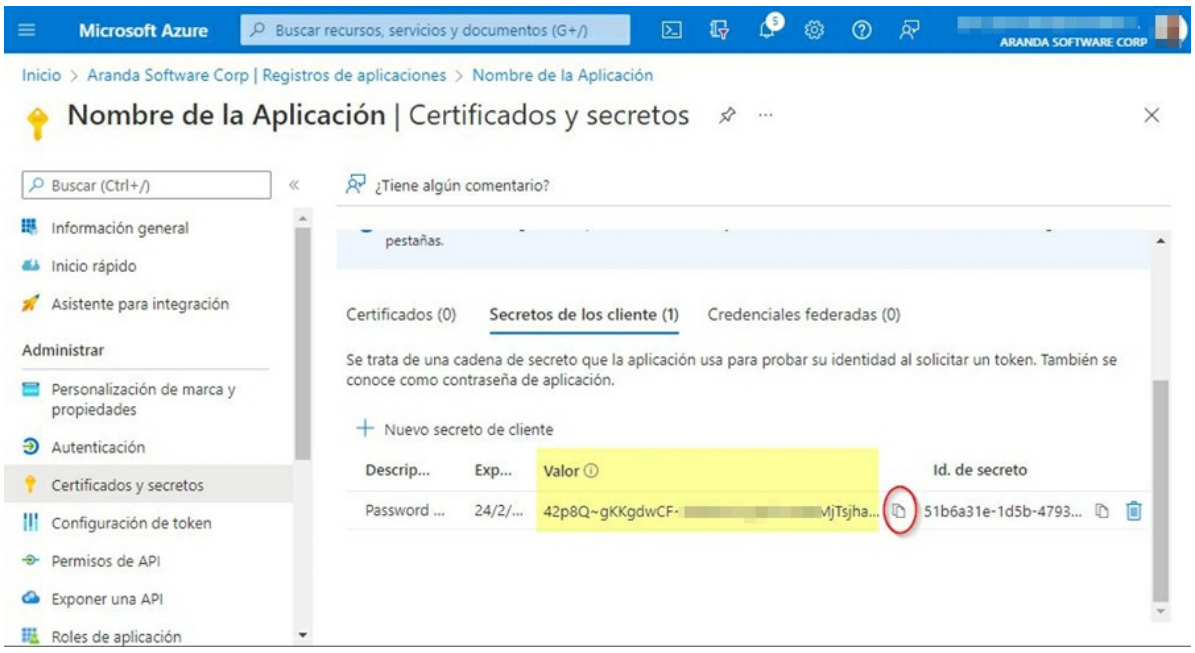


3. En la vista **Agregar un secreto de cliente** diligencie el campo **Descripción**, configurare el campo **Expira** que corresponde a la duración del secreto. Luego selecciona **Agregar** (Es importante siempre tener presente esta duración dado que, a su vencimiento, si no se actualiza, fallará la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



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

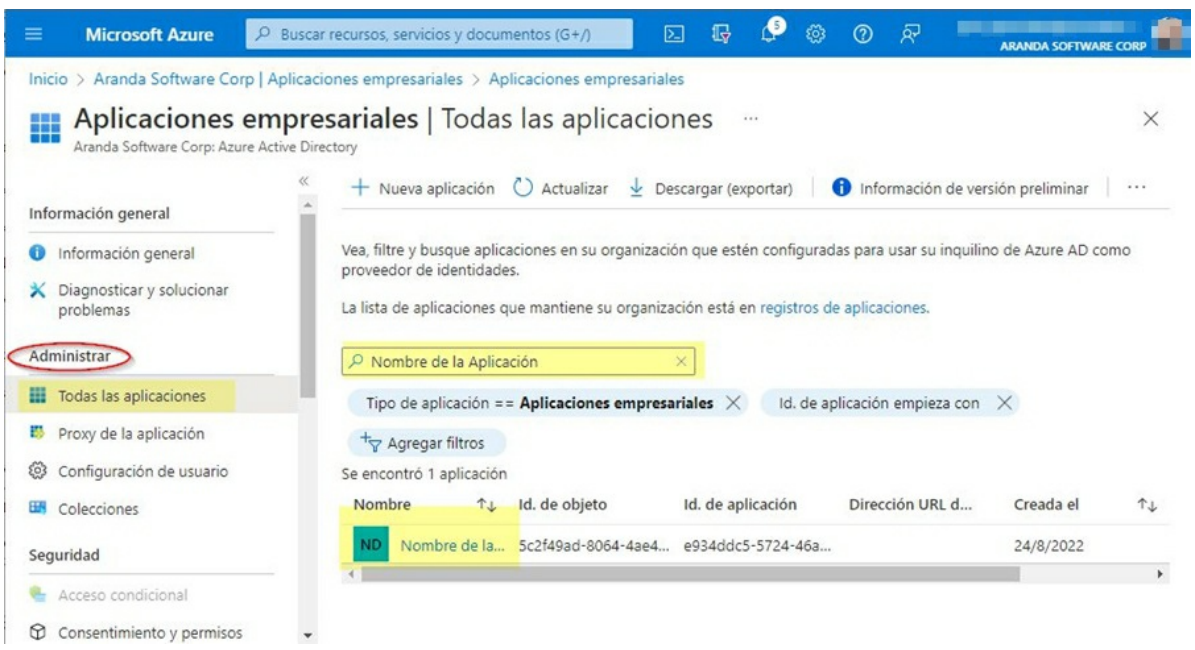
- Valor secreto de cliente -> Secreto cliente.



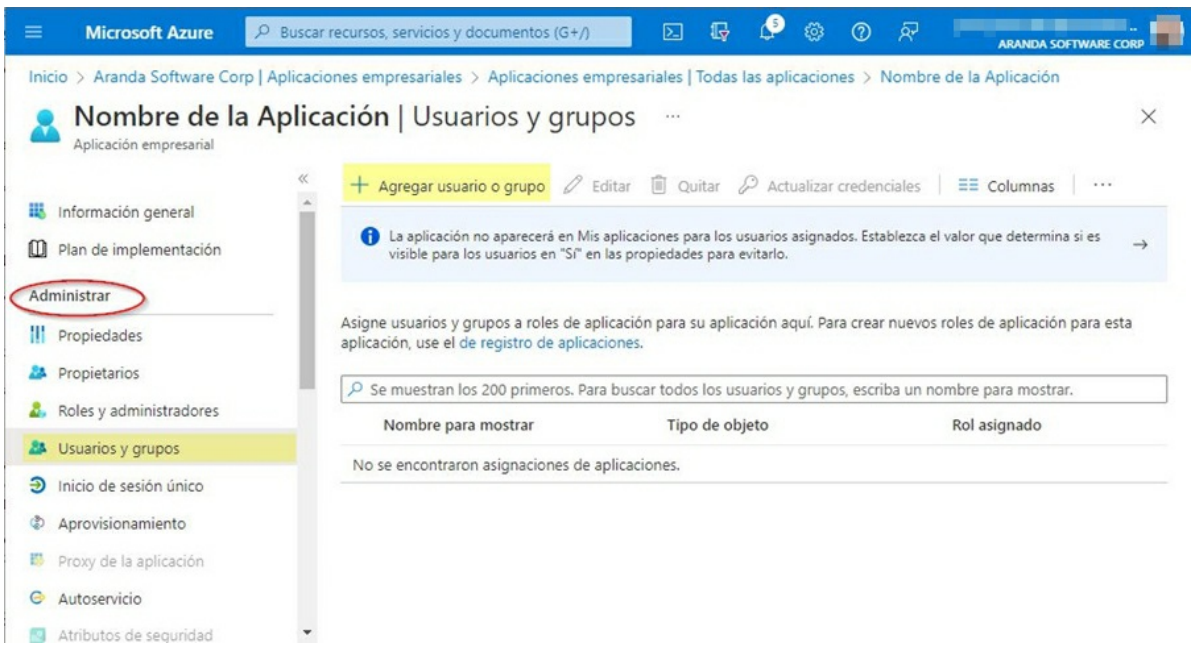
Configuración de usuarios y grupos

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

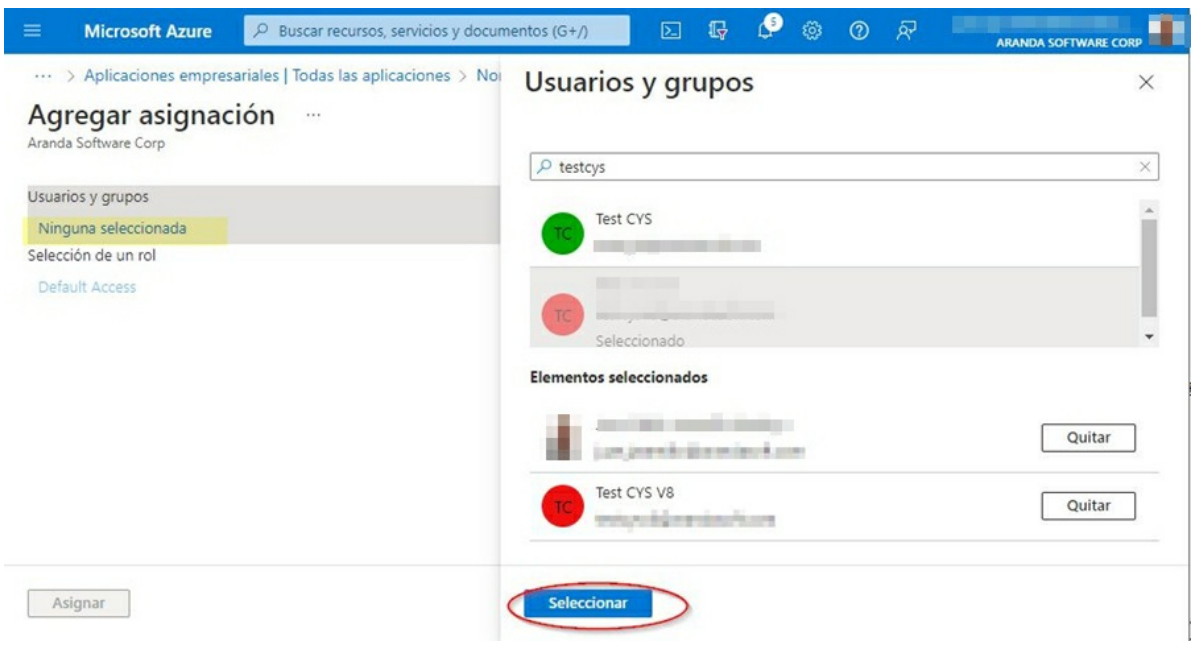
1. Se ingresa al portal de Azure> Menú> Azure Active Directory> Aplicaciones empresariales> seleccionar la aplicación creada del listado que aparece en la vista.



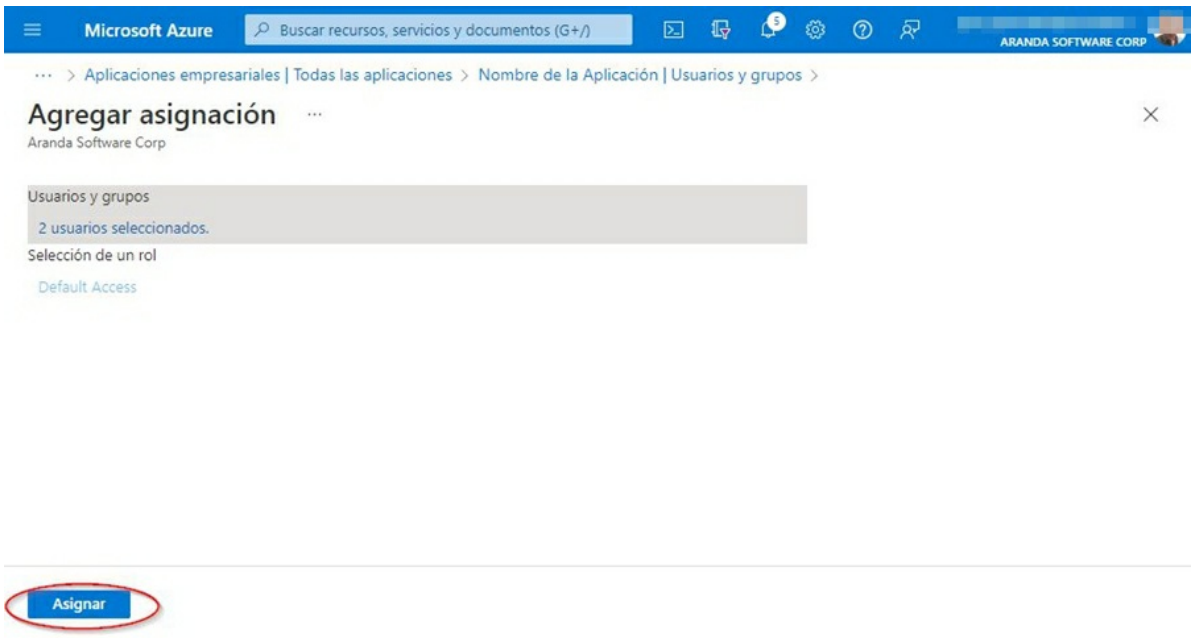
2. En la sección **Administrar** busque y seleccione **Usuarios y grupos>** y luego **Agregar usuario o grupo**.



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



4. Finalmente seleccione **Asignar**.

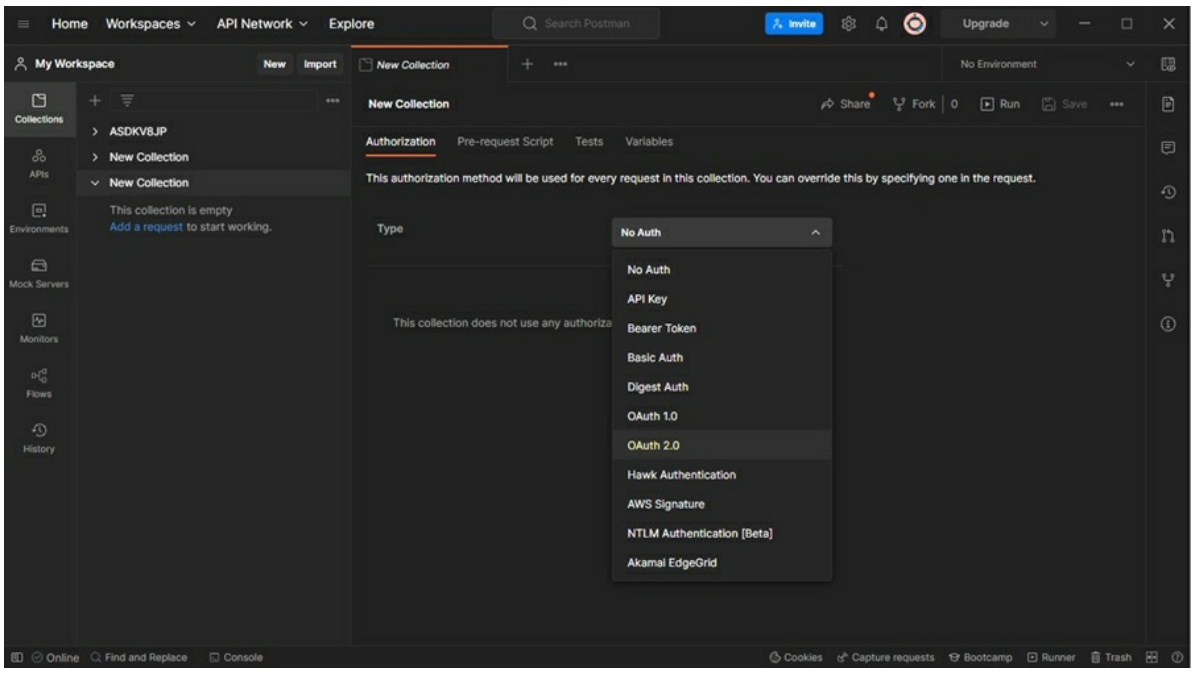


Solicitud Refresh Token

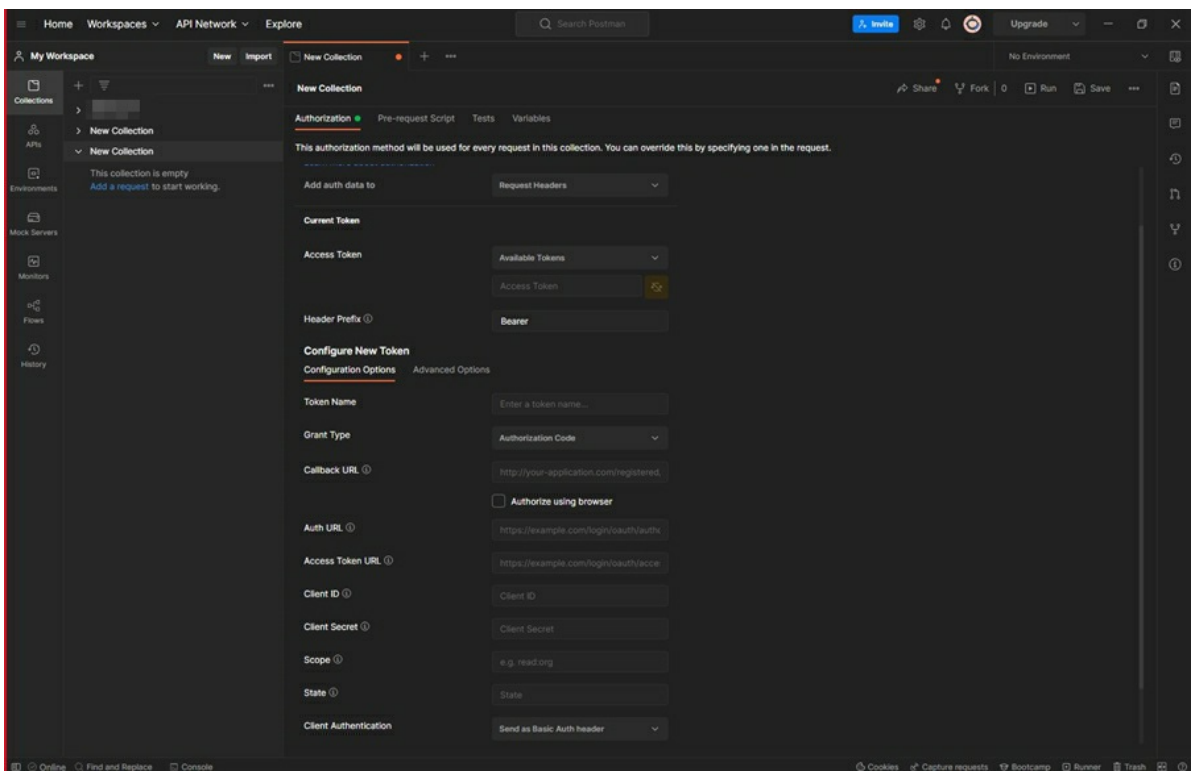
Cómo realizar la solicitud del Refresh Token Azure

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

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



2. En la vista se debe diligenciar los campos de la siguiente manera:

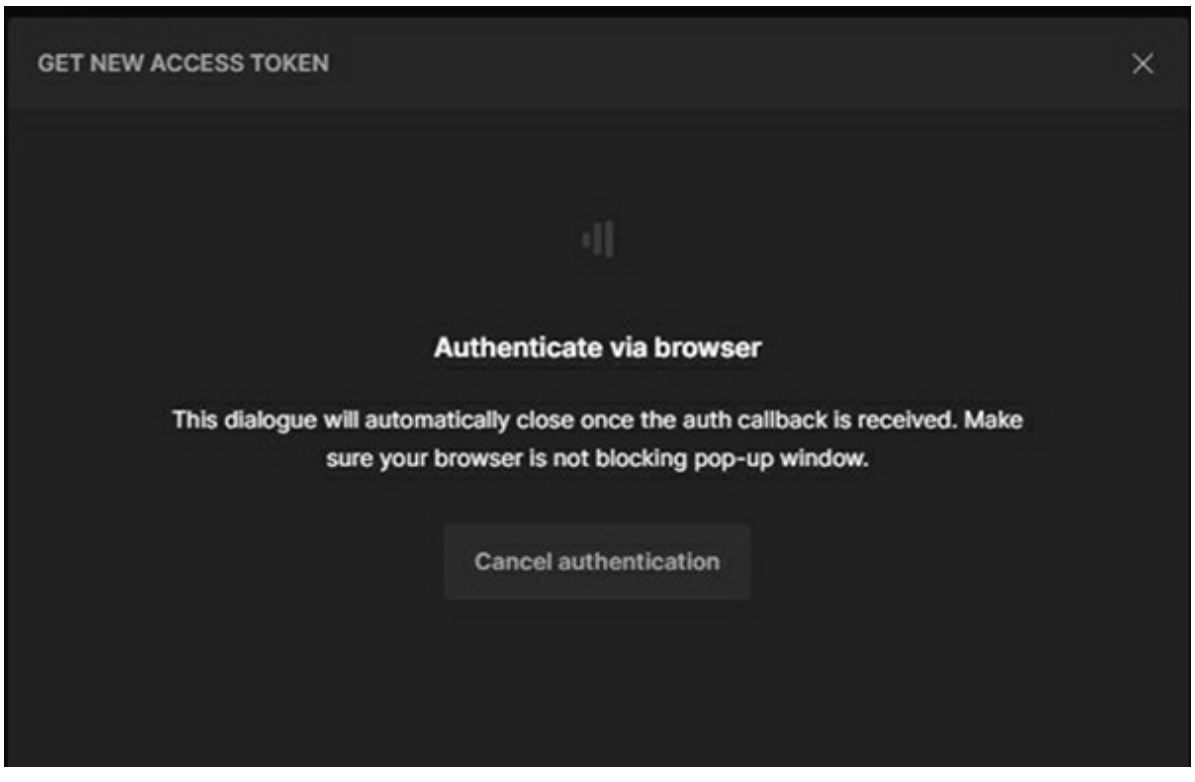


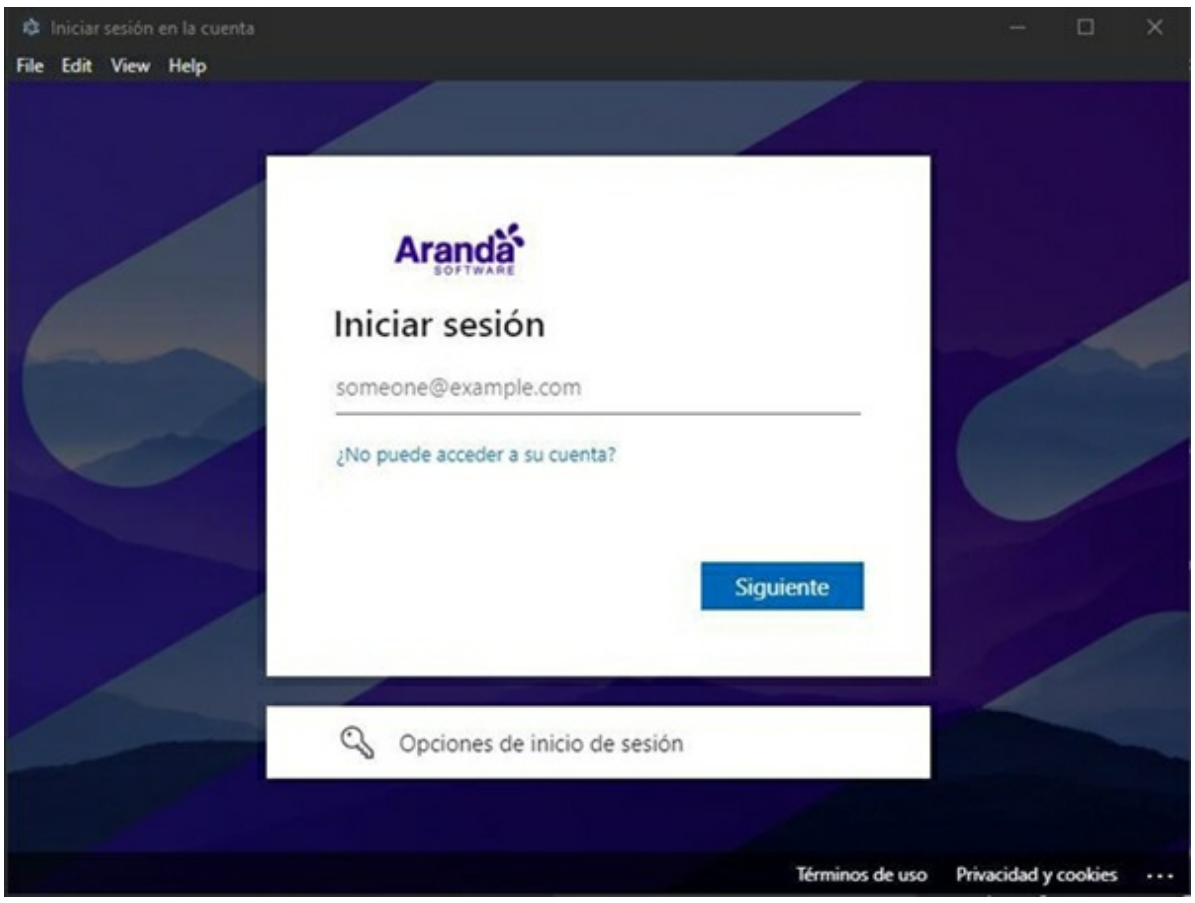
Campo	Descripción
Type	OAuth 2.0
Add auth data to	Request Headers
Acces Token	Availabe Token
Header Prefix	Bearer
Token Name	Nombre que desee para el token
Gran Type	Autorization Code
Callback URL	http://localhost
Auth URL	Ingrese el valor de Punto de conexión de autorización de OAuth 2.0 (v2).
Access Token URL	Ingrese el valor de Punto de conexión de token de OAuth 2.0 (v2).
Client ID	Ingrese el valor de Id. de aplicación (cliente).
Client Secret	Ingrese el Valor secreto de cliente.
Scope	offline_access https://outlook.office.com/SMTP.Send https://outlook.office.com/IMAP.AccessAsUser.All https://outlook.office.com/POP.AccessAsUser.All
State	Se puede dejar en blanco.
Client Authentication	Send as Basic Auth header

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

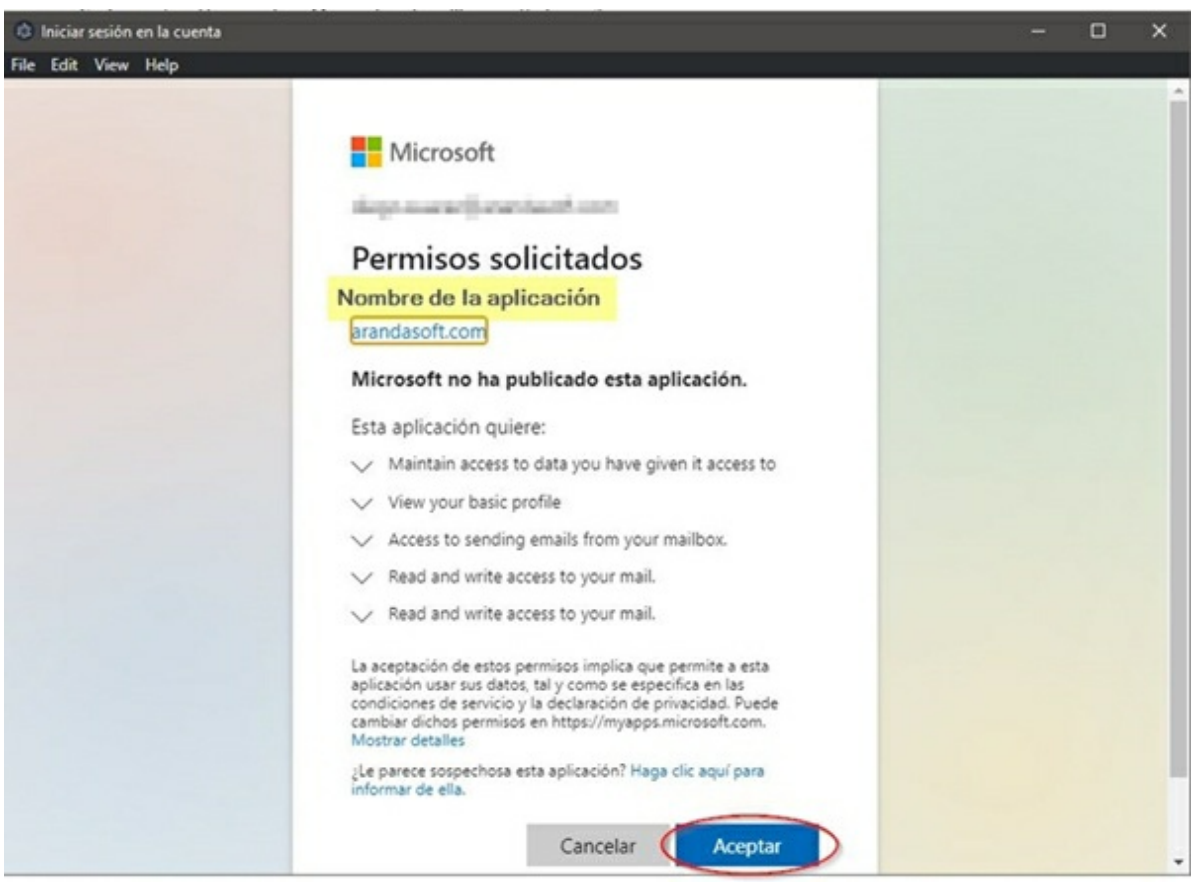
> ⚐ **Nota:** Para garantizar la generación correcta del Refresh_Token, es esencial verificar las URLs ingresadas en el Scope y asegurarse de que no contengan saltos de línea ni espacios en blanco al inicio ni al final.

4. Se abren dos ventanas, una ventana para ingresar las credenciales de acceso y la otra donde se visualiza el proceso de solicitud del Token.

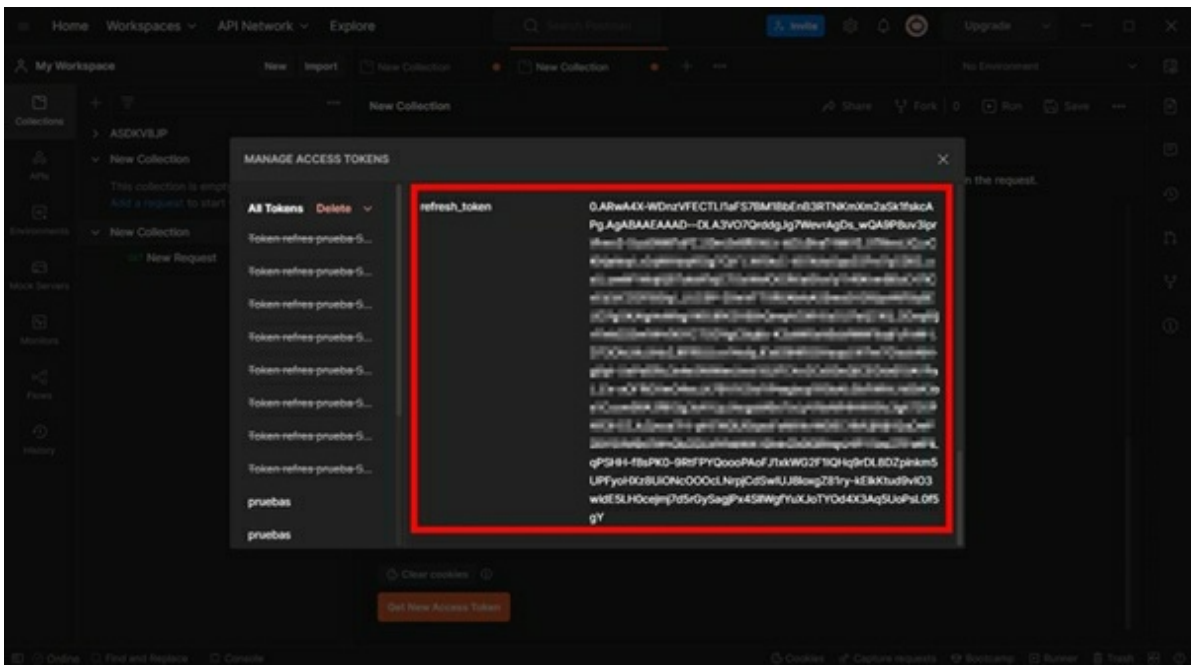




5. La sesión se debe iniciar con una de las cuentas agregadas en la [Configuración de Usuario y Grupos](), cuando el ingreso se realiza de forma correcta la sesión va a solicitar que aceptemos los permisos solicitados.



5.Posterior a la aceptación de los permisos se debe proceder a copiar el refresh_token, guarde este token dado que se usará en las configuraciones de (Correo) y (Case creator) en las aplicaciones de Aranda.



Autenticación OAuth 2.0 - Google

Precondiciones

1. Una cuenta de Google con alguno de los roles de administrador, administrador de facturación o gerente de facturación de proyectos. También puede ser la misma que usará para enviar y recibir correos electrónicos.

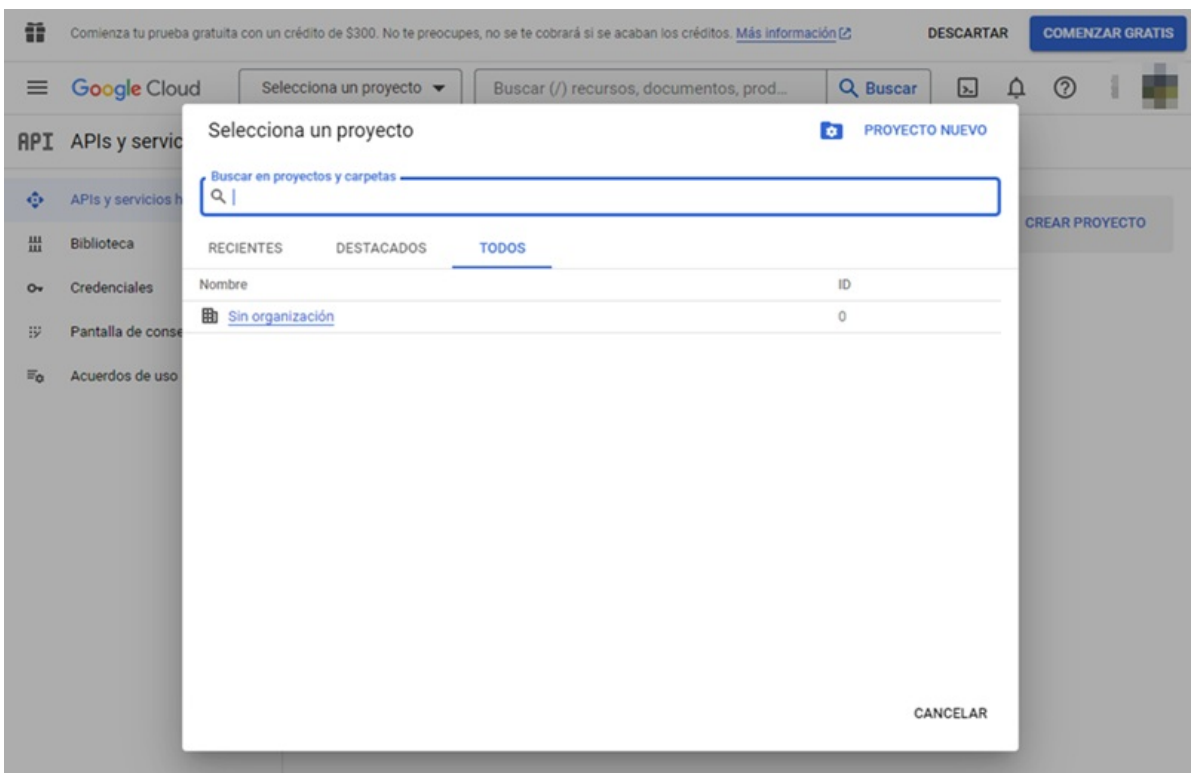
2. Aplicación POSTMAN para la solicitud del refresh_token.

Creación de proyecto en Google

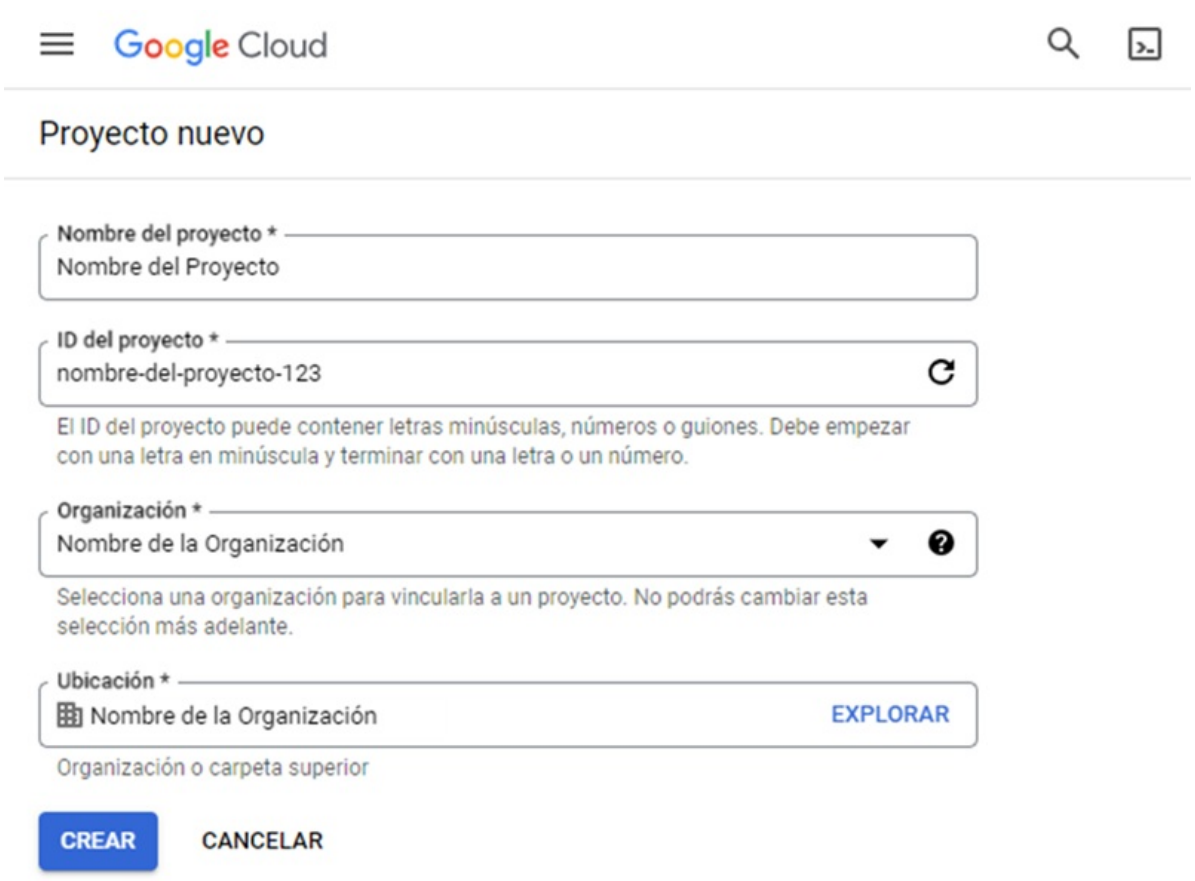
> ⚐ **Nota**: Si ya se cuenta con un proyecto configurado en Google, se puede omitir este paso.

Cómo crear un proyecto en Google

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

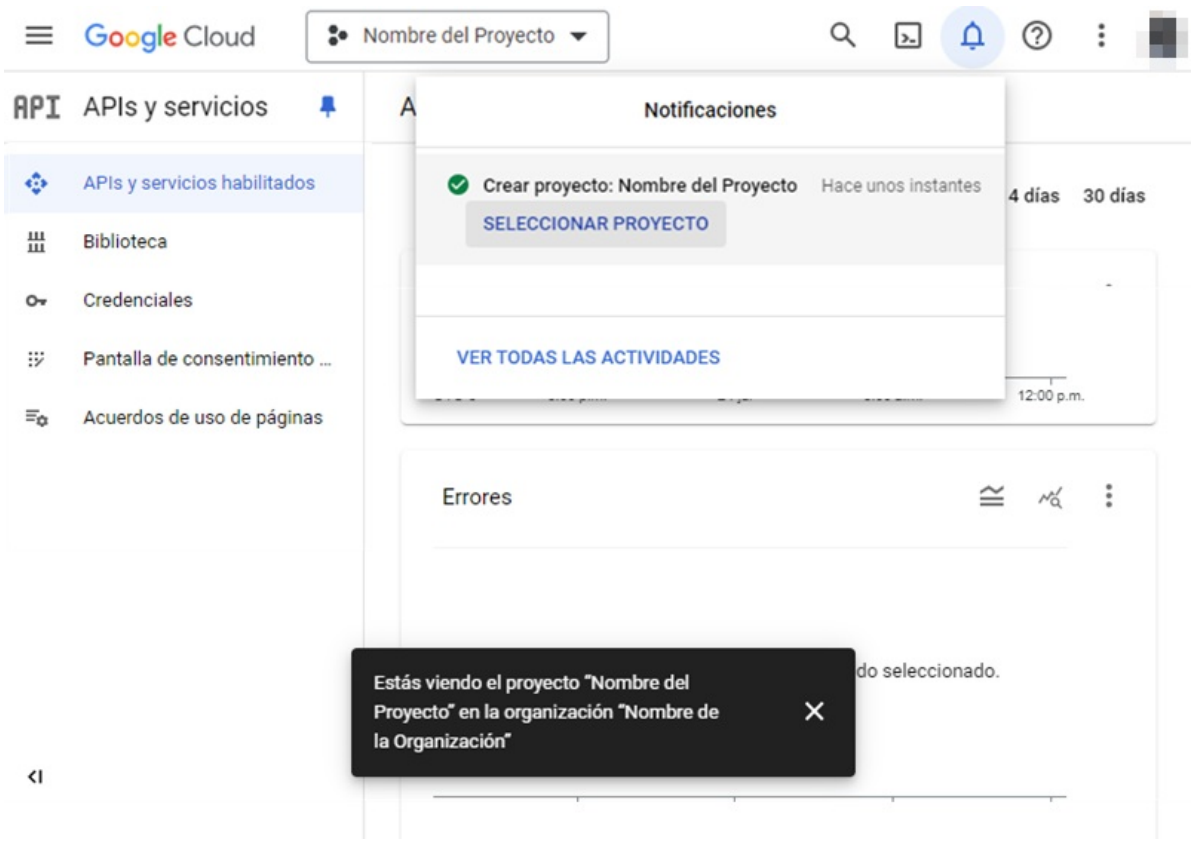


2. En la ventana **Proyecto nuevo** ingrese los cuatro campos solicitados siguiendo las recomendaciones y haga clic en el botón **CREAR**.



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

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



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

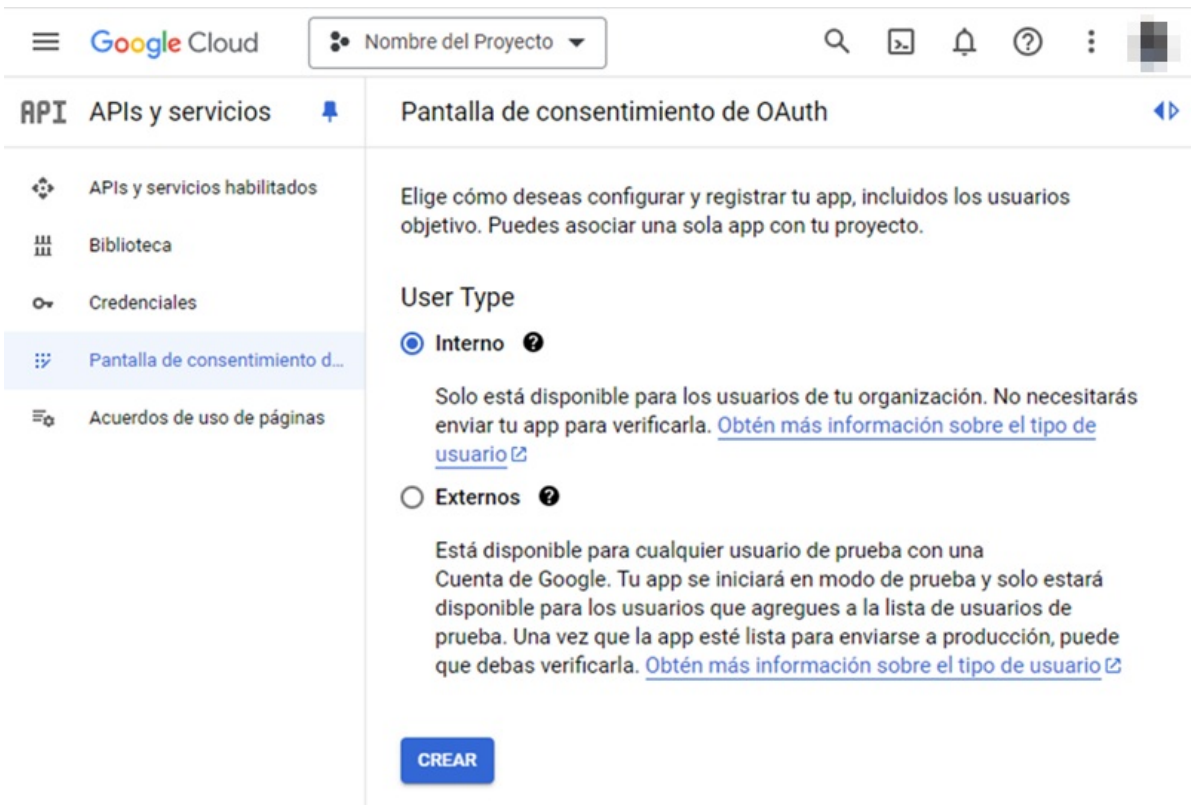
Creación y configuración de aplicación en Google

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

Cómo crear una aplicación en Google

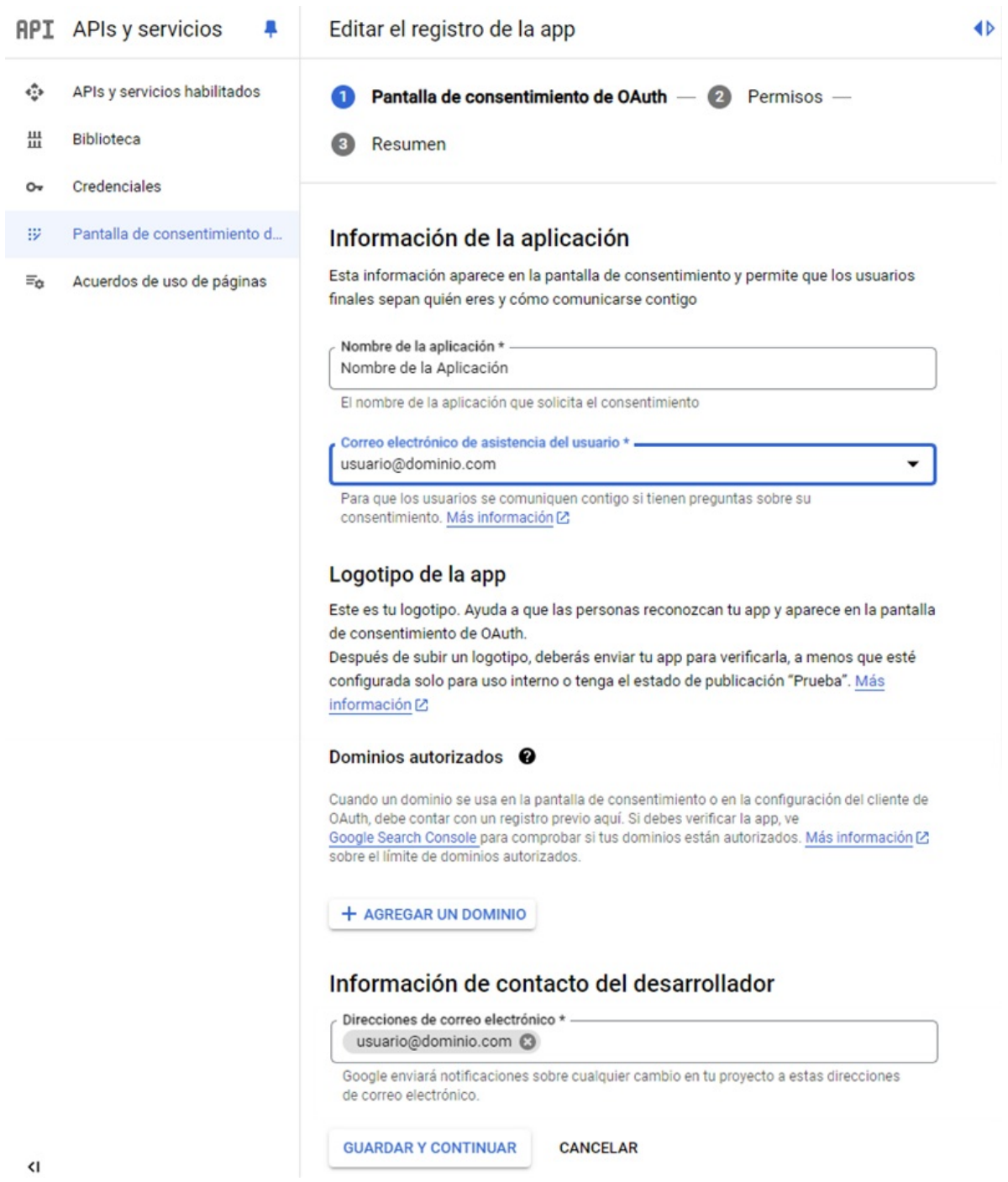
1. En la consola de Google Cloud en la sección **APIs y servicios** seleccione la opción **Pantalla de consentimiento de OAuth** y el tipo de usuario

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

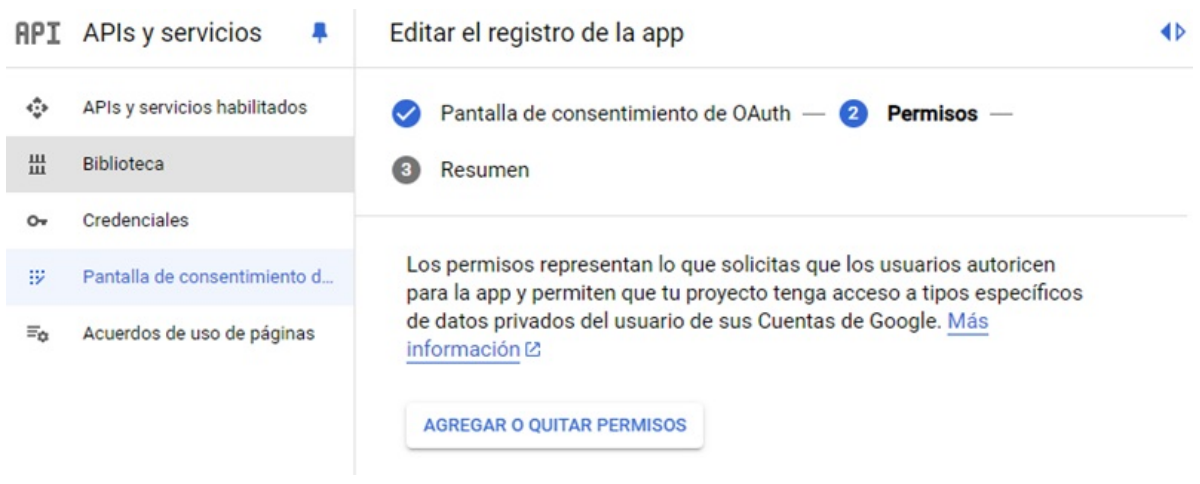


2. Haga clic en el botón CREAR.

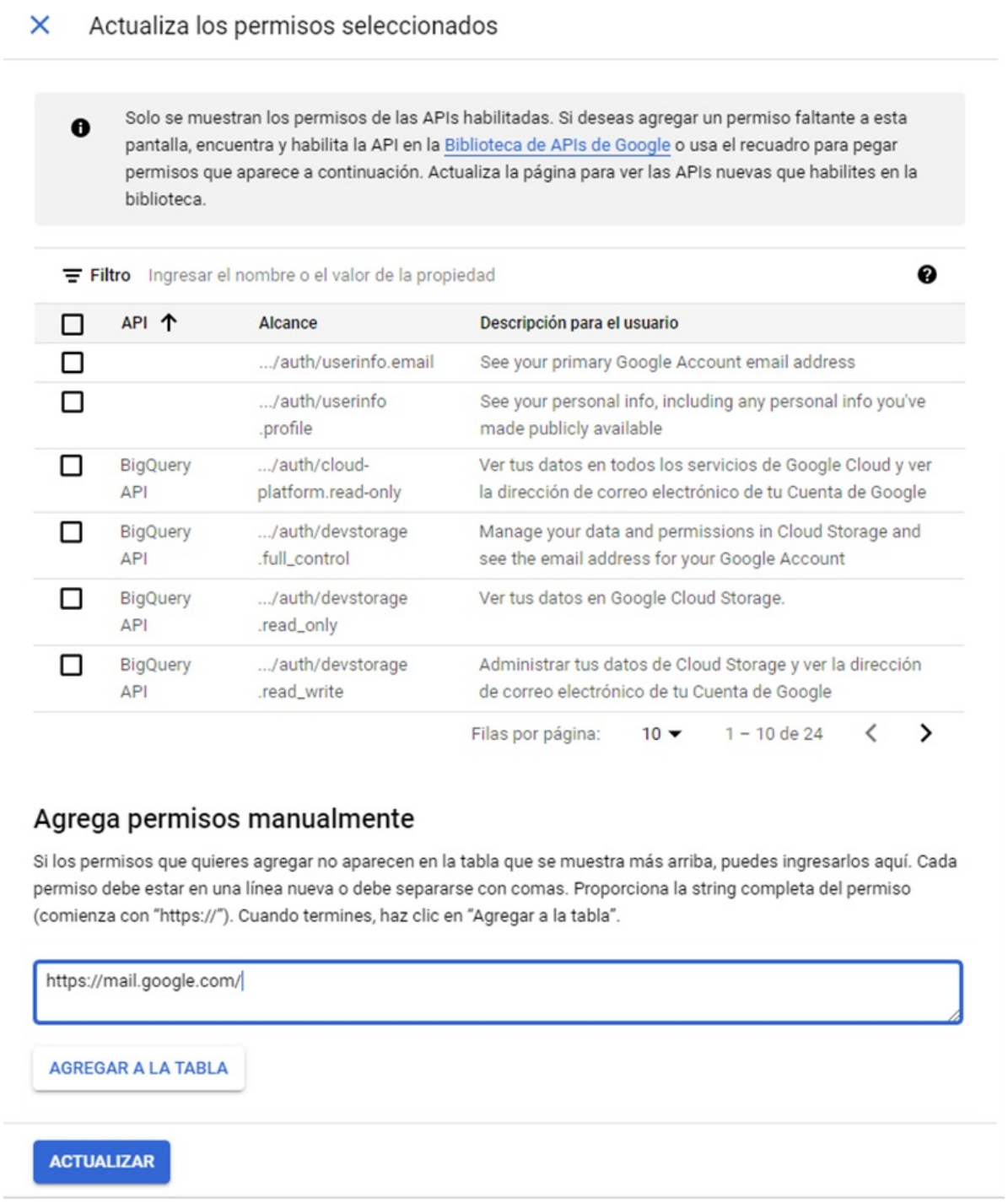
3. En la ventana **Pantalla de consentimiento de OAuth** ingrese los campo *Nombre de la aplicación*, *Correo electrónico de asistencia del usuario* en la sección **Información de la aplicación** y *Direcciones de correo electrónico* en la sección **Información de contacto del desarrollador** según las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



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

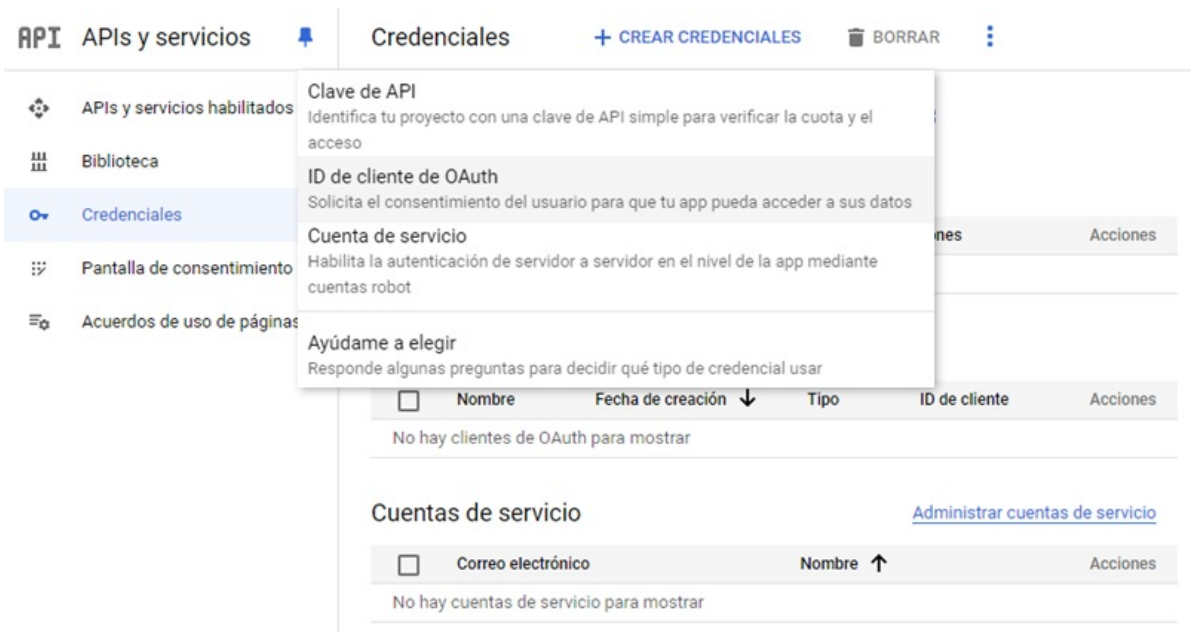


5. En la ventana **Actualiza los permisos seleccionados** en la sección **Agrega permisos manualmente** ingresa el valor https://mail.google.com/ y haga clic en el botón **AGREGAR A LA TABLA**. Luego en **ACTUALIZAR**.

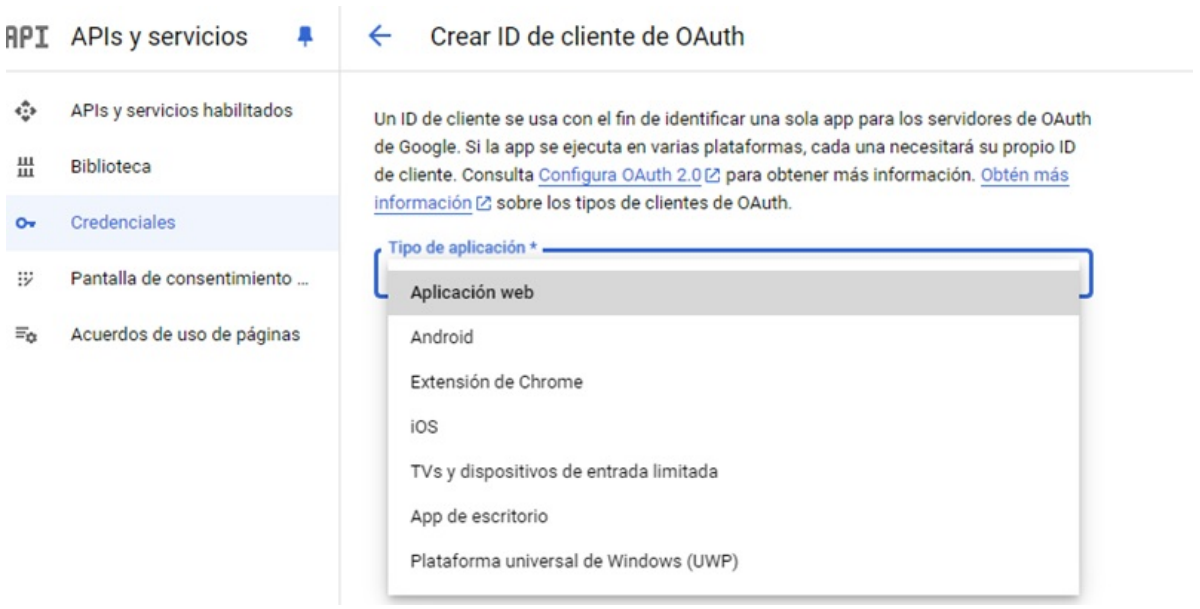


6. En la ventana **Permisos** verifique que el permiso se haya agregado en la sección **Tus permisos restringidos** y haga clic en el botón **GUARDAR Y CONTINUAR** para avanzar a la ventana **Resumen** donde podrá visualizar los datos de la nueva aplicación.

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

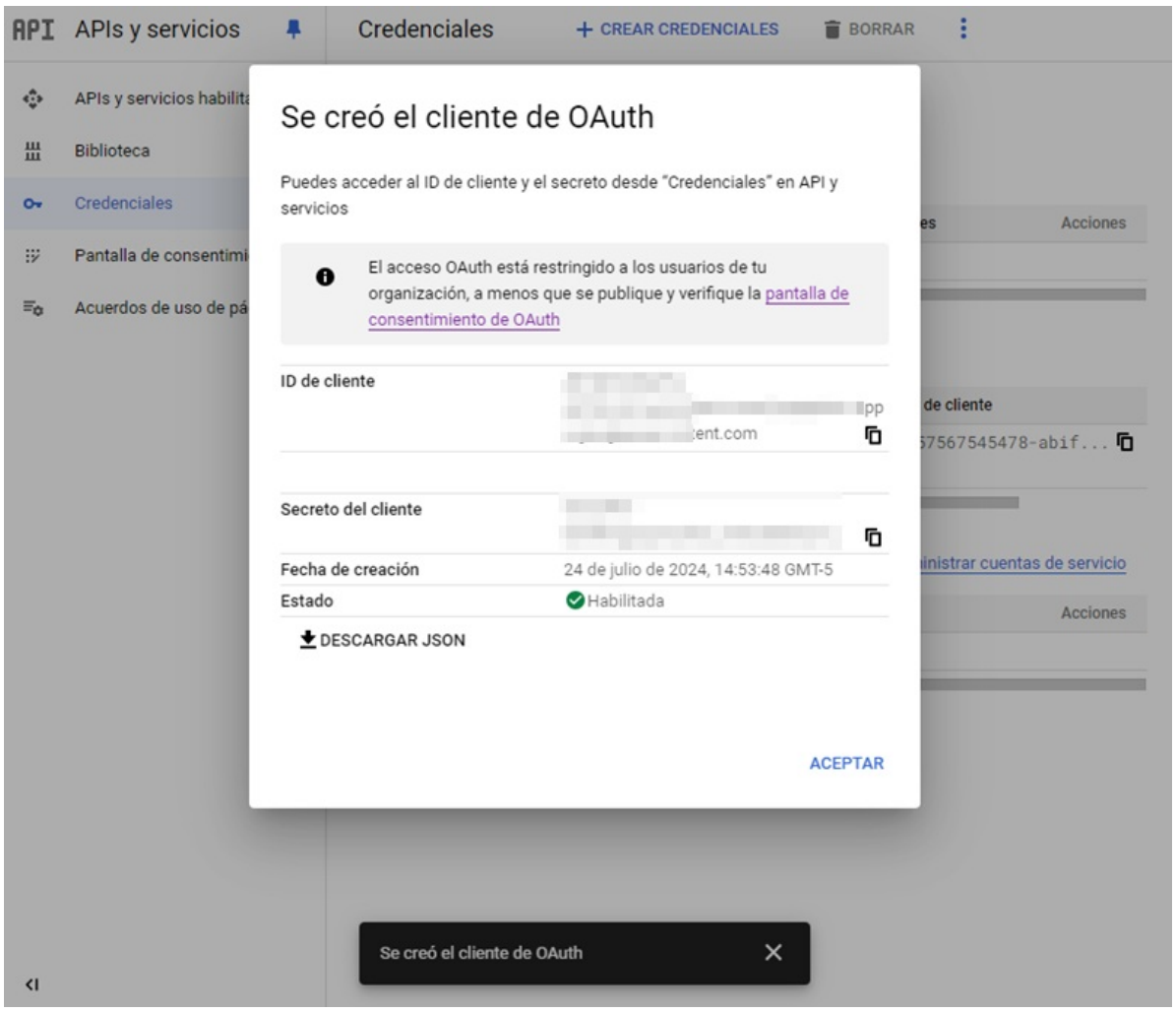


8. En la ventana **Crear ID de cliente de OAuth** en el campo *Tipo de aplicación*, seleccione la opción **Aplicación web**.



9. En la ventana **Crear ID de cliente de OAuth** en la sección **URI de redireccionamiento autorizados** agregue la URI http://localhost y 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.



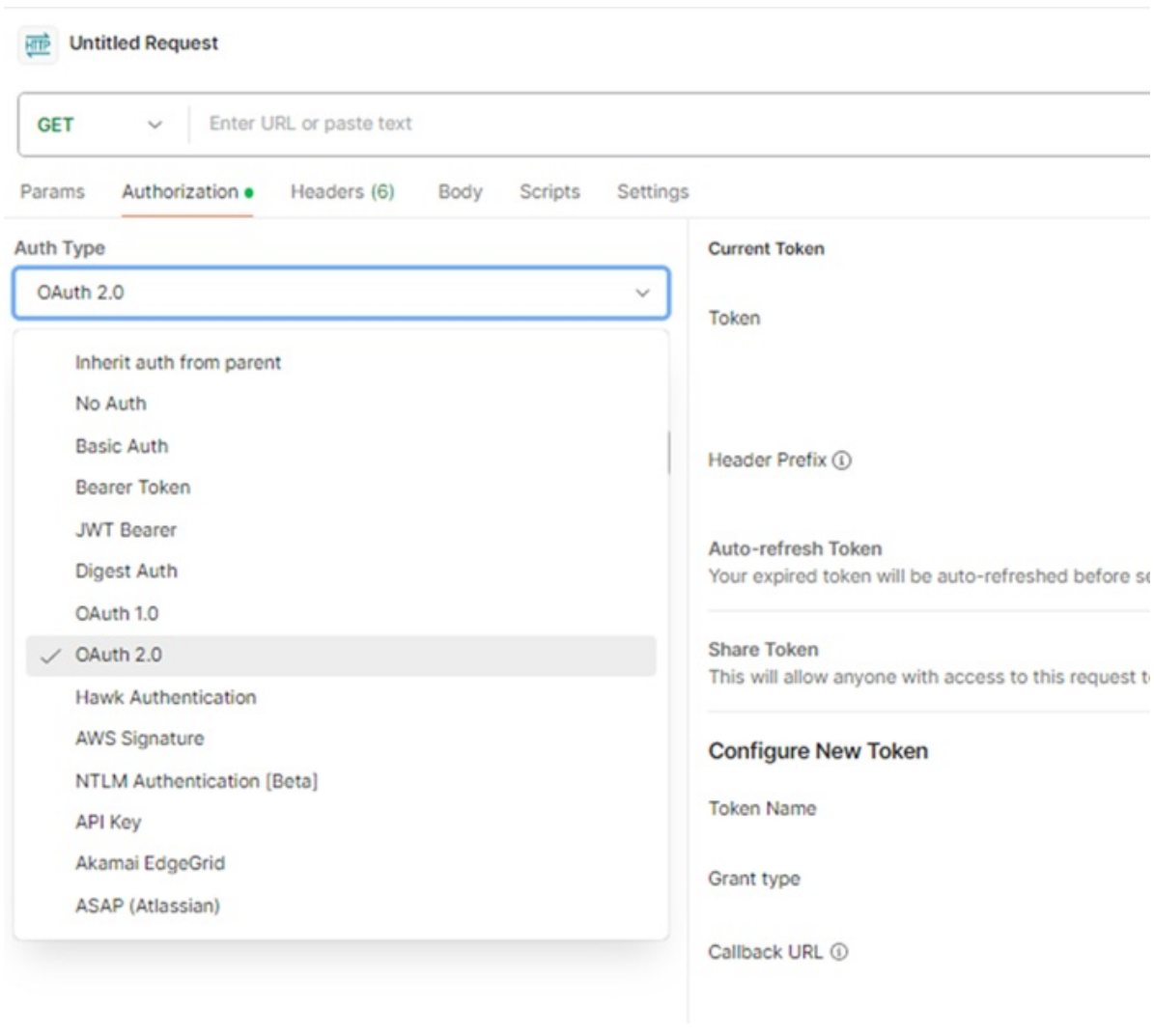
- Id. de aplicación (cliente) -> ID de cliente.
- Valor secreto de cliente -> Secreto del cliente.
- Punto de conexión de token de OAuth 2.0 (v2) -> https://oauth2.googleapis.com/token.

Solicitud Refresh Token Google

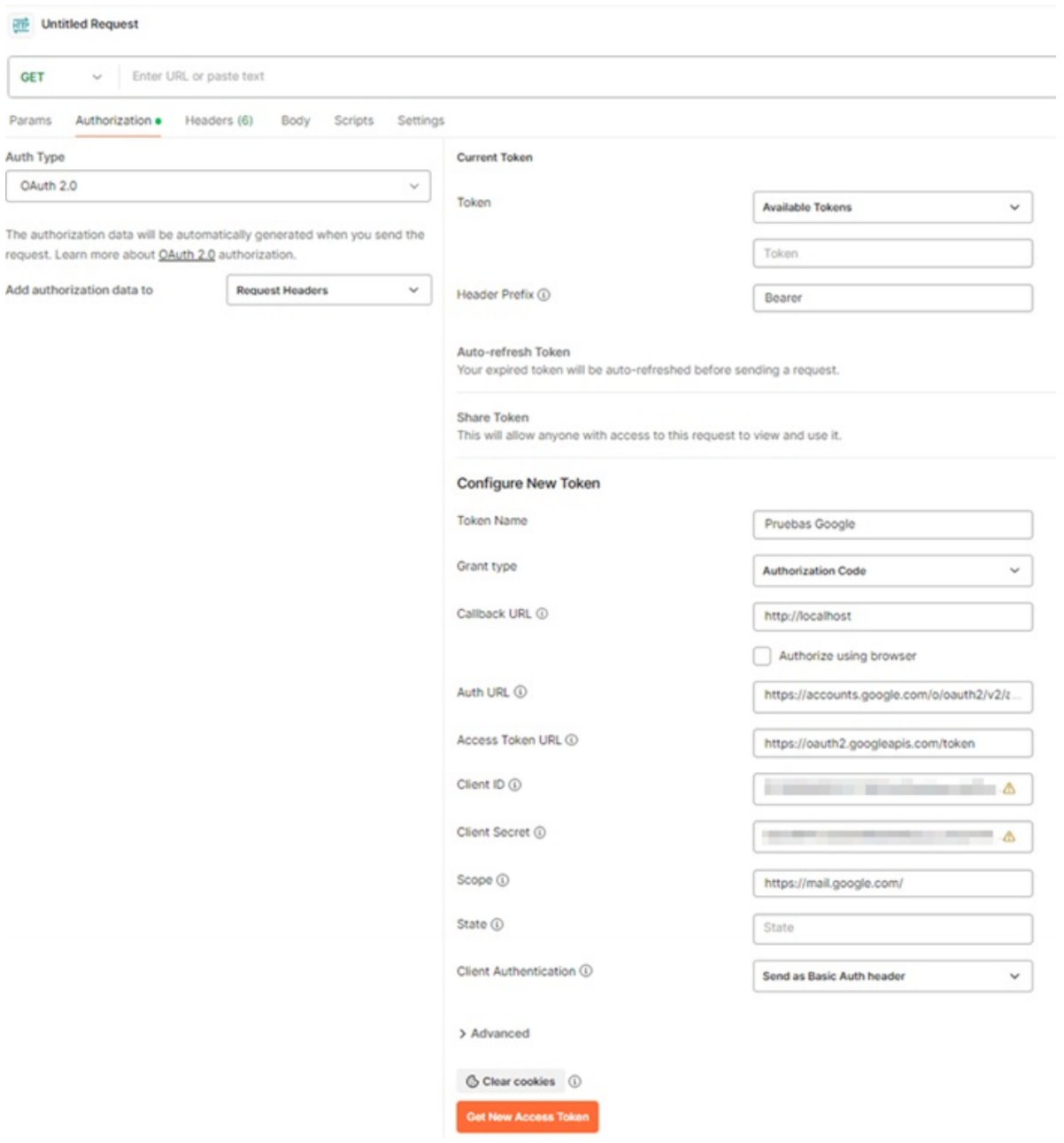
Cómo realizar la solicitud del Refresh Token Google

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

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



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

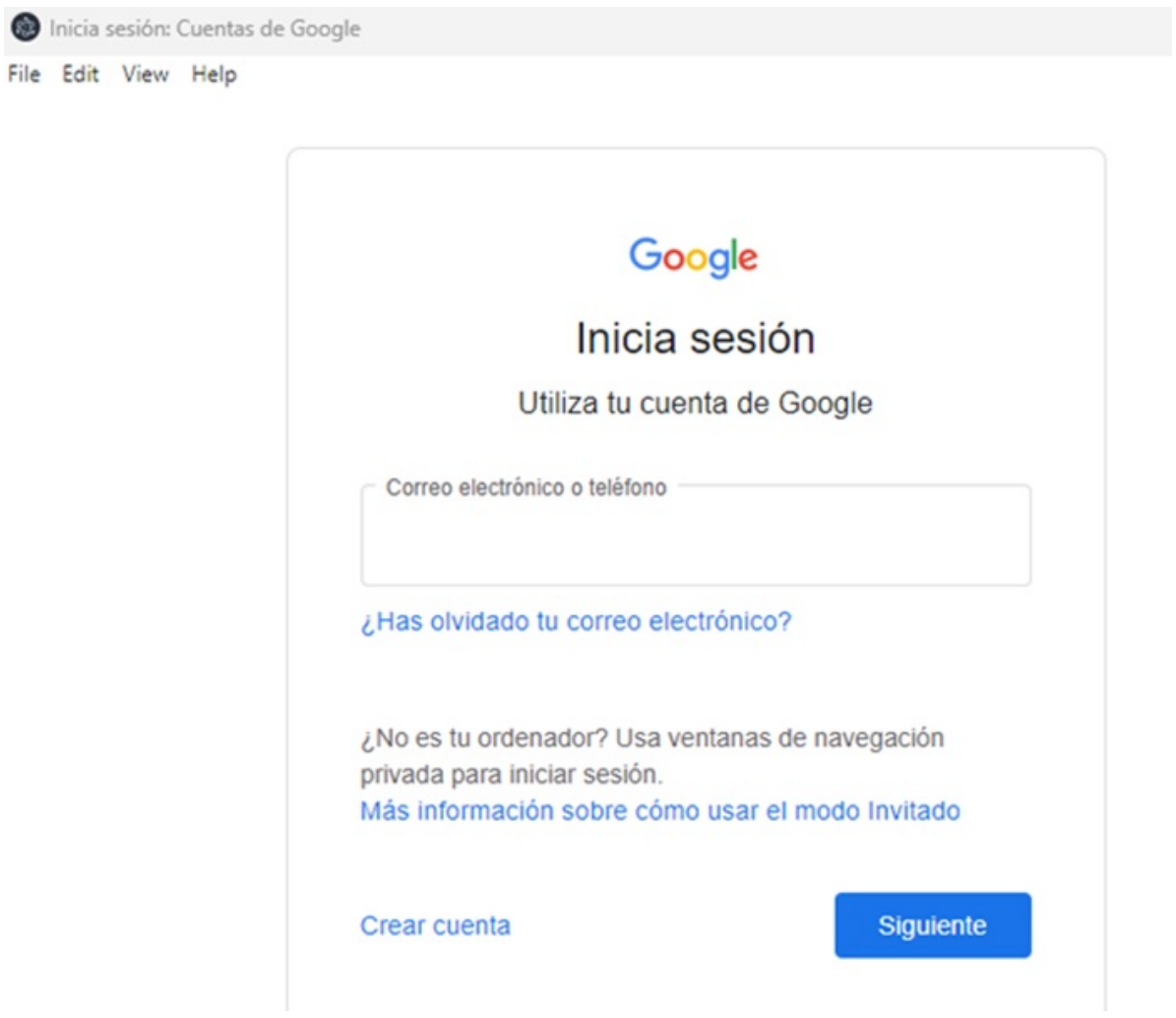


Campo	Descripción
Type	OAuth 2.0
Add auth data to	Request Headers
Acces Token	Availabe Token
Header Prefix	Bearer
Token Name	Nombre que desee para el token
Gran Type	Autorization Code
Callback URL	http://localhost
Auth URL	https://accounts.google.com/o/oauth2/v2/auth?access_type=offline
Access Token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

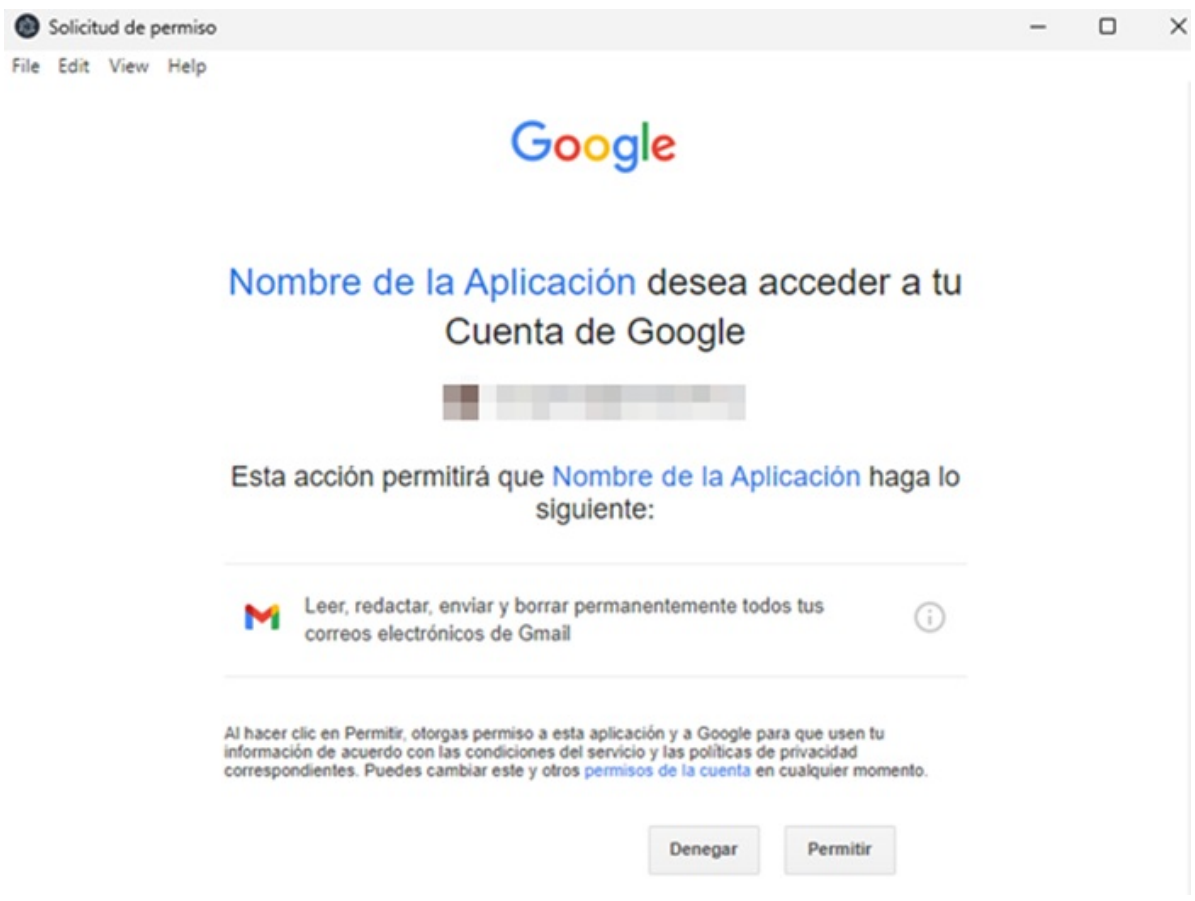
3. Al ingresar toda la información seleccione **Get New Access Token**.

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

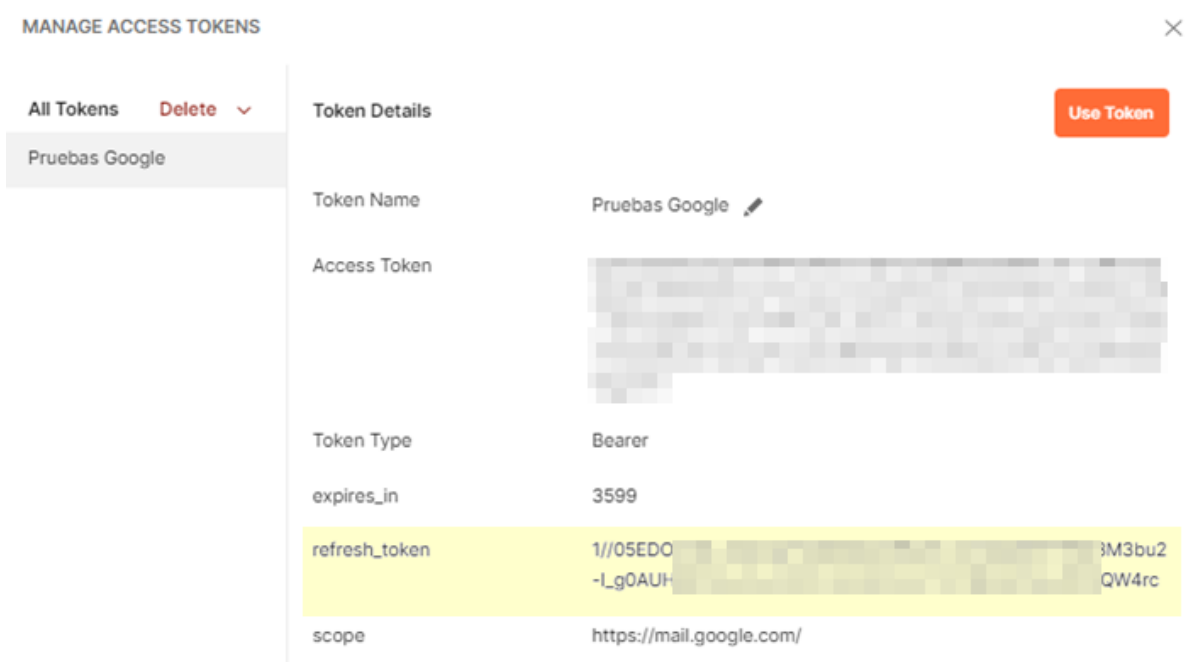
4. Se habilita la ventana de inicio de sesión en cuentas de Google; ingrese el correo y contraseña al que se requiere generar el refresh token.



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



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



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

Para ampliar mayor información consulte la documentación de Google: [Actualiza el vencimiento del token]