CONFIGURACIÓN PARA LA AUTENTICACIÓN MODERNA -OAUTH2.0

Aranda SOFTWARE

Contenido

Configuración para la Autenticación Moderna Oauth 2.0 2
Precondiciones 2
Crear Aplicación en portal Azure y captura de datos. 2
Configuración de la Aplicación en el portal Azure 4
Configurar la Autenticación 4
Creación del Secreto 5
Configuración de usuarios y grupos 7
Solicitud del Refresh_Token 9

Configuración para la Autenticación Moderna Oauth 2.0

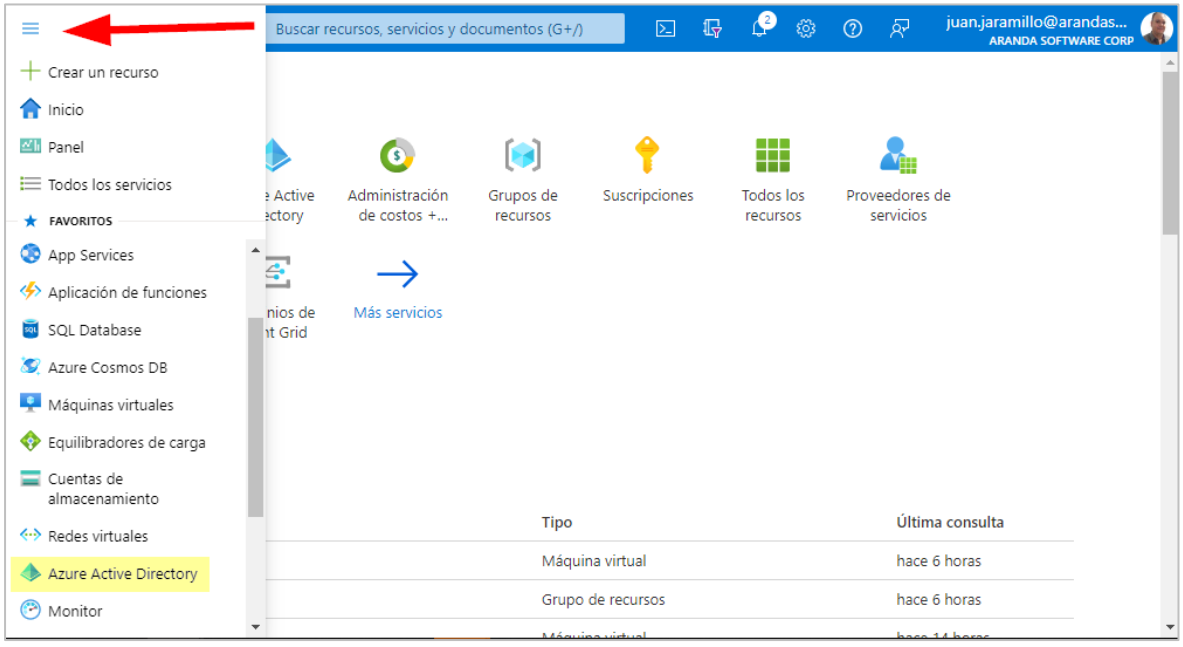
Precondiciones

- 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.

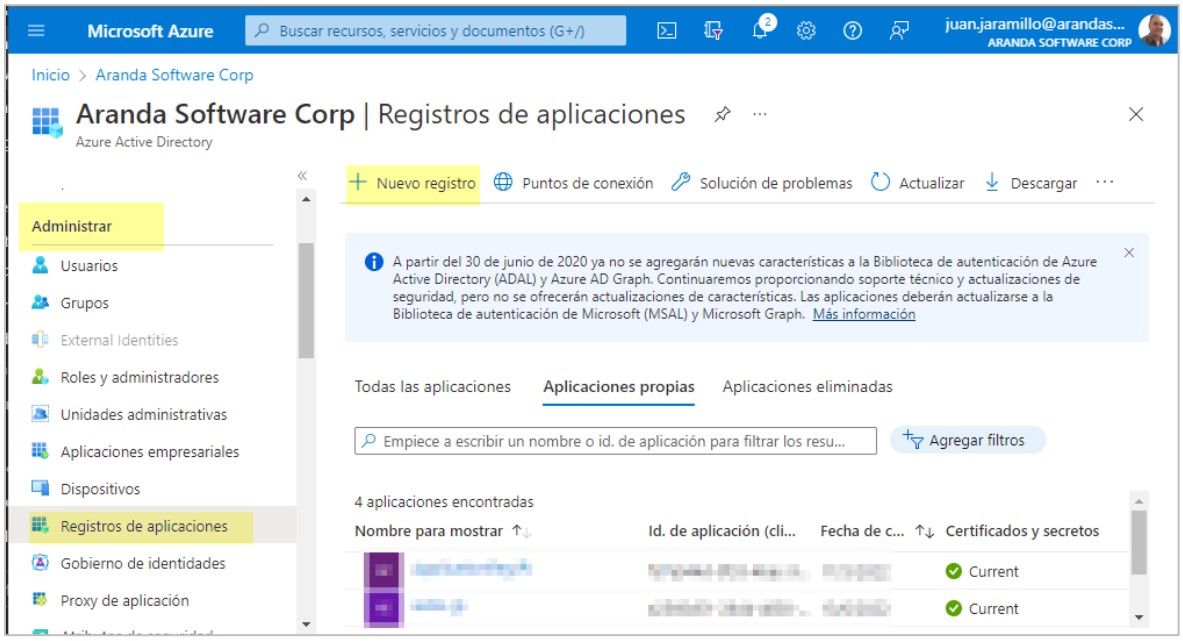
- Aplicación POSTMAN para la solicitud del refresh_token.

Crear Aplicación en portal Azure y captura de datos.

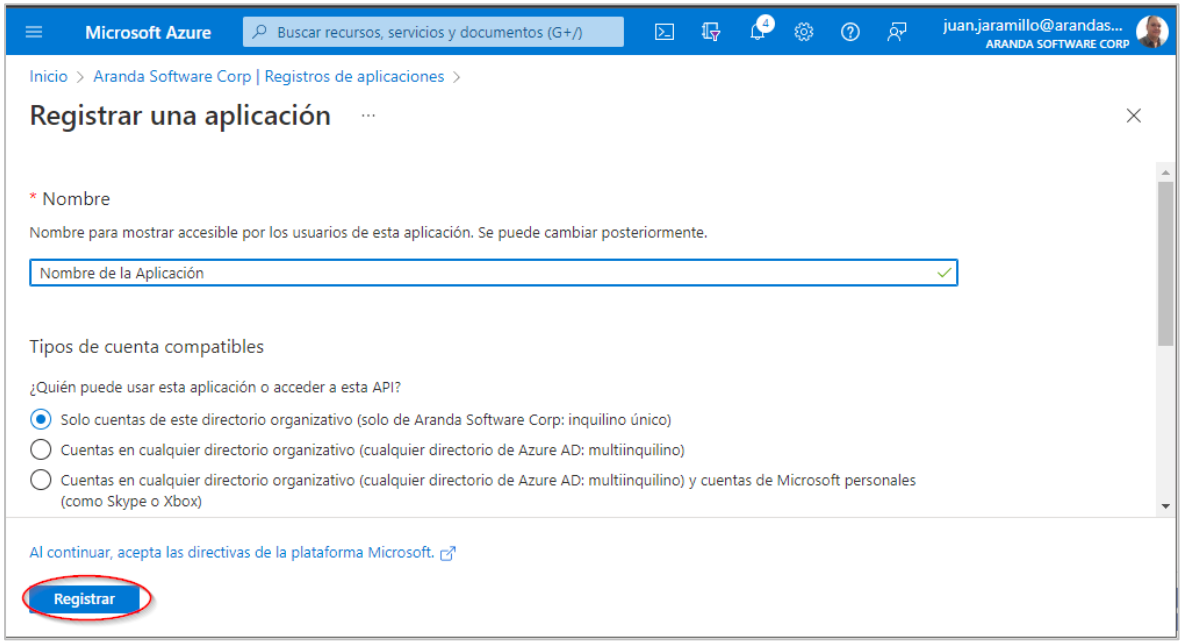
1. Se accede al portal de Azure link , busque y seleccione **Azure Active Directory.**



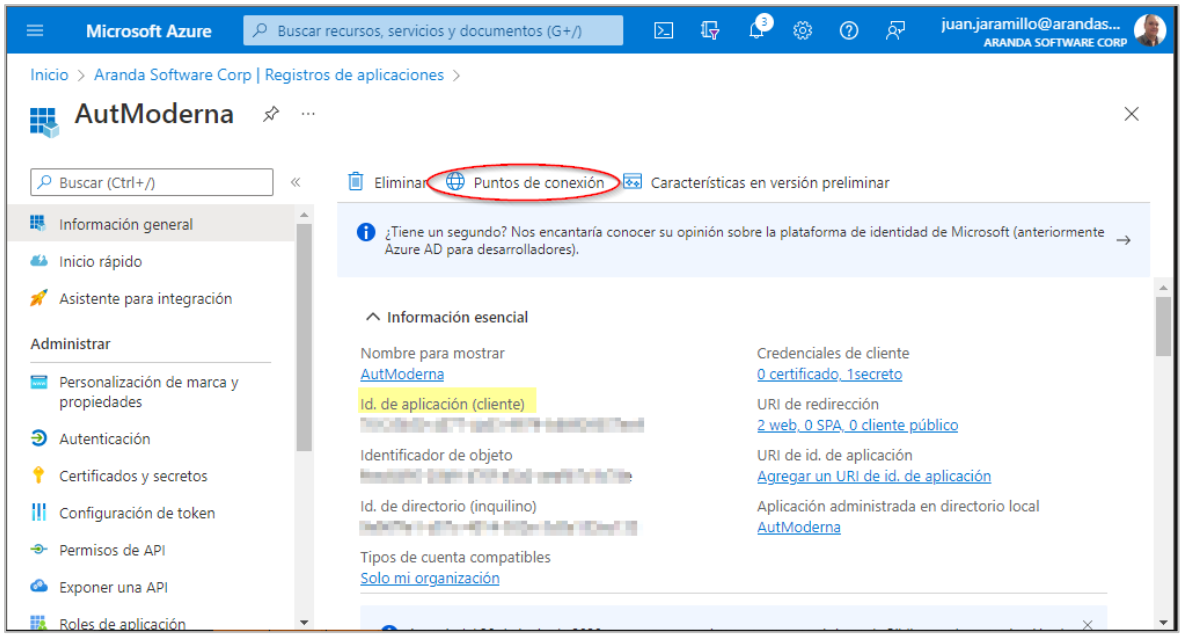
2. En la sección **Administrar** busque y seleccione **Registros de aplicaciones**, haga clic en **Nuevo registro.**

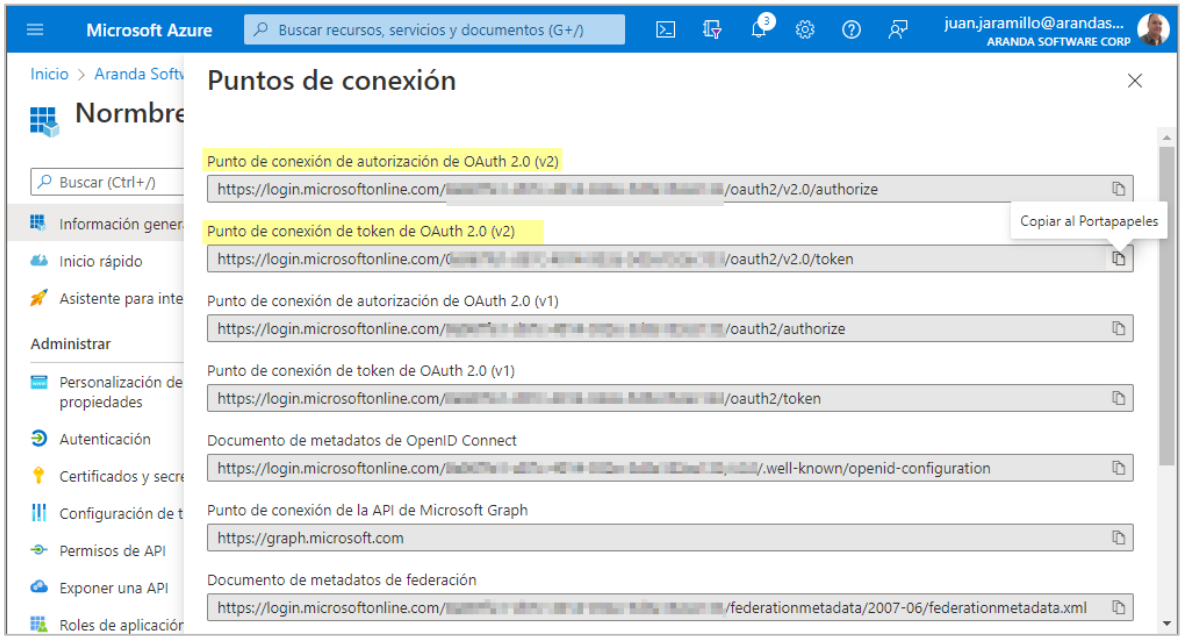


3. Se diligencia el campo del nombre y se selecciona la opción deseada en (Tipos de cuenta compatibles), clic en **Registrar**.



4. Cuando ya se tenga registrada la aplicación se deben guardar tres datos que se utilizaran más adelante.
   - **Id. de aplicación (cliente)**
     Clic en la opción (Puntos de conexión).
   - **Punto de conexión de autorización de OAuth 2.0 (v2).**
   - **Punto de conexión de token de OAuth 2.0 (v2)**.





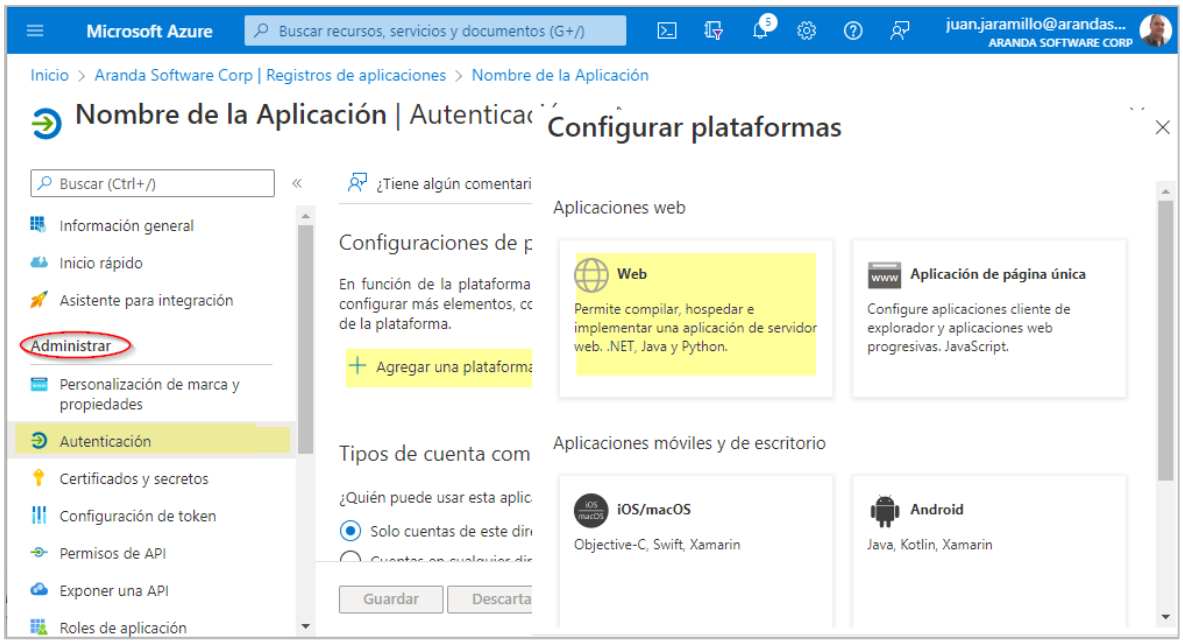
Configuración de la Aplicación en el portal Azure

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

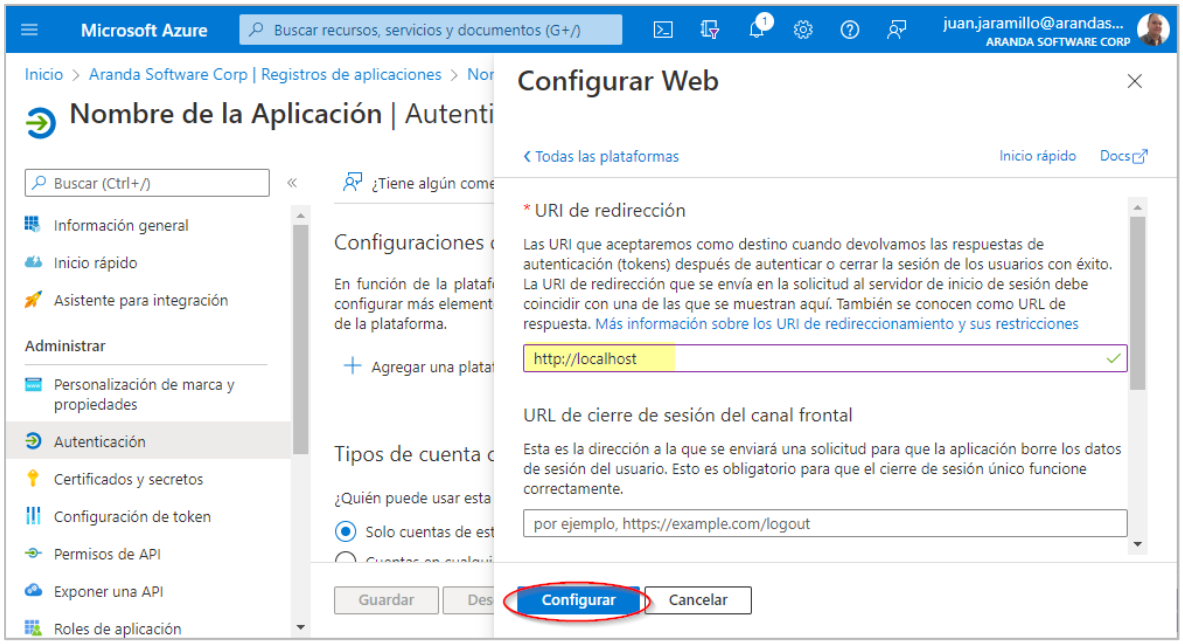
Configurar la Autenticación

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** finalmente seleccionamos **WEB**.



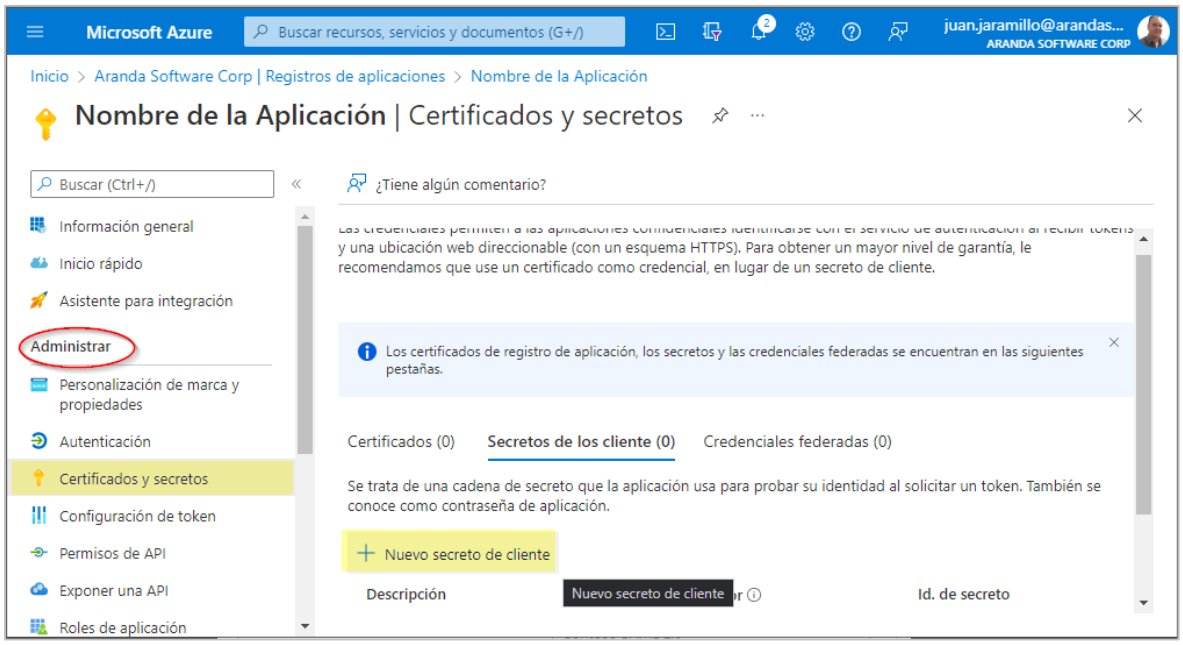
3. En el campo **URI de redirección** agregamos el siguiente valor **http://localhost**, y luego seleccionamos **Configurar.**



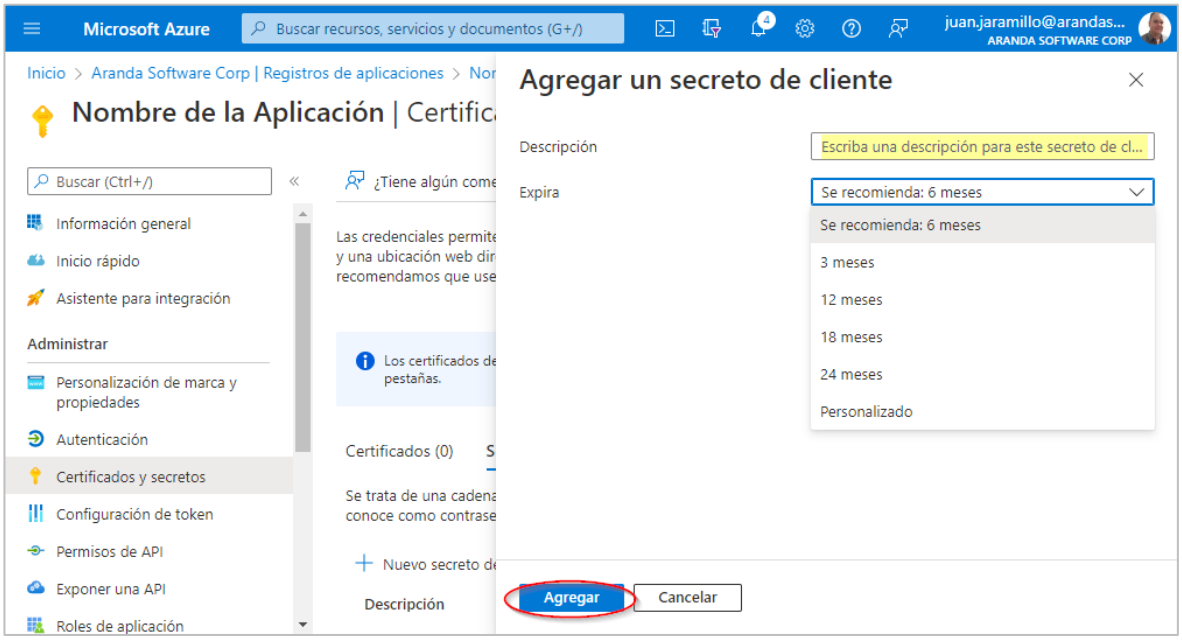
Creación del Secreto

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.

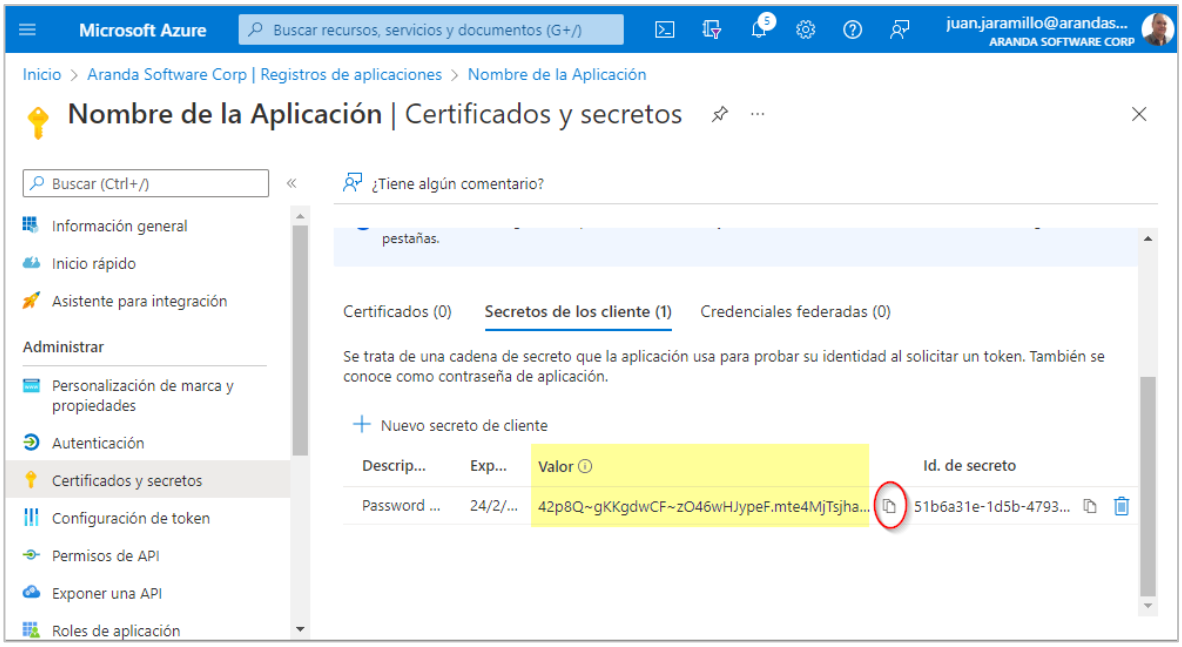
2. En la sección **Administrar** busque y seleccione **Certificados y secretos** > luego en **Nuevo secreto de cliente**.



3. En la vista **Agregar un secreto de cliente** debes diligenciar el campo **Descripción** y configurar el campo **Expira** que es la duración del secreto y luego selecciona **Agregar** (Es importante siempre tener presente esta duración dado que, a su vencimiento, si no se actualiza, fallará la autenticación).



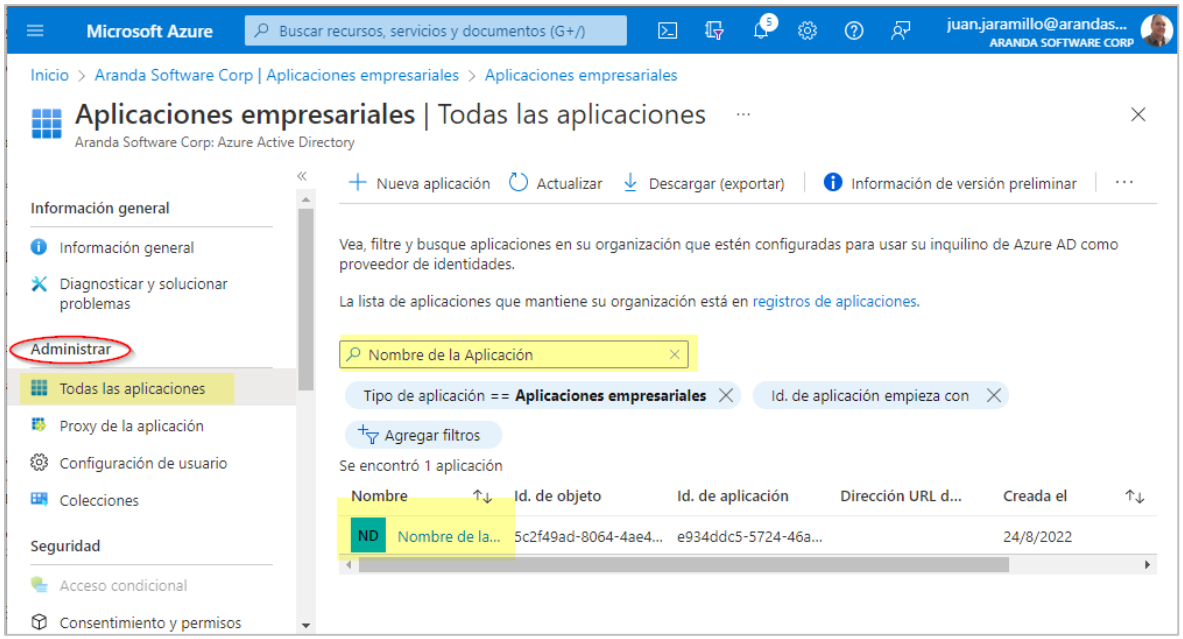
4. El valor del secreto solo es visible cuando se crea por lo que se debe guardar para usarlo más adelante y conservarlo para las configuraciones que se requieran en los productos de Aranda.
   - **Valor secreto de cliente**



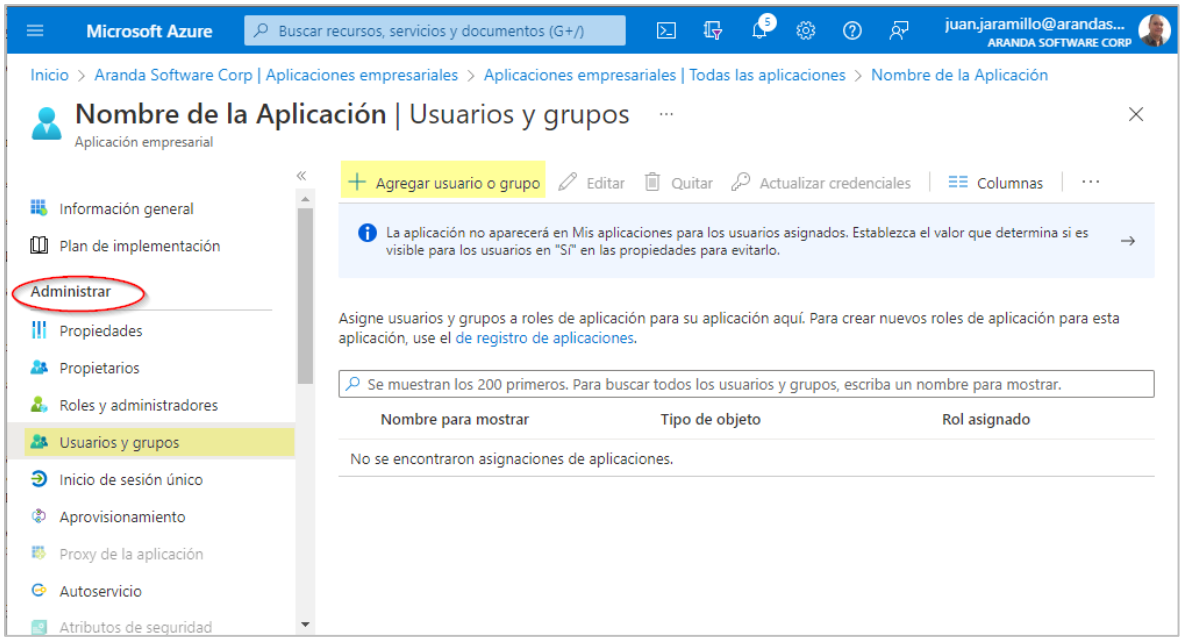
Configuración de usuarios y grupos

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

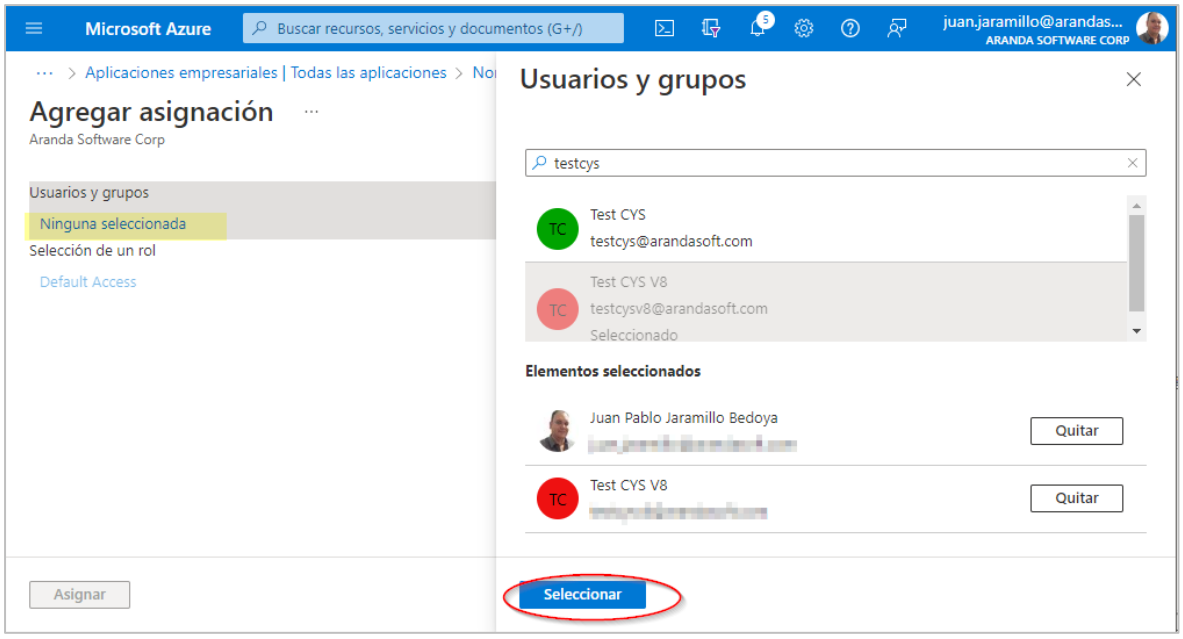
1. Se ingresa al portal de Azure> Menú> Azure Active Directory> Aplicaciones empresariales> seleccionar la aplicación creada del listado que aparece en la vista.



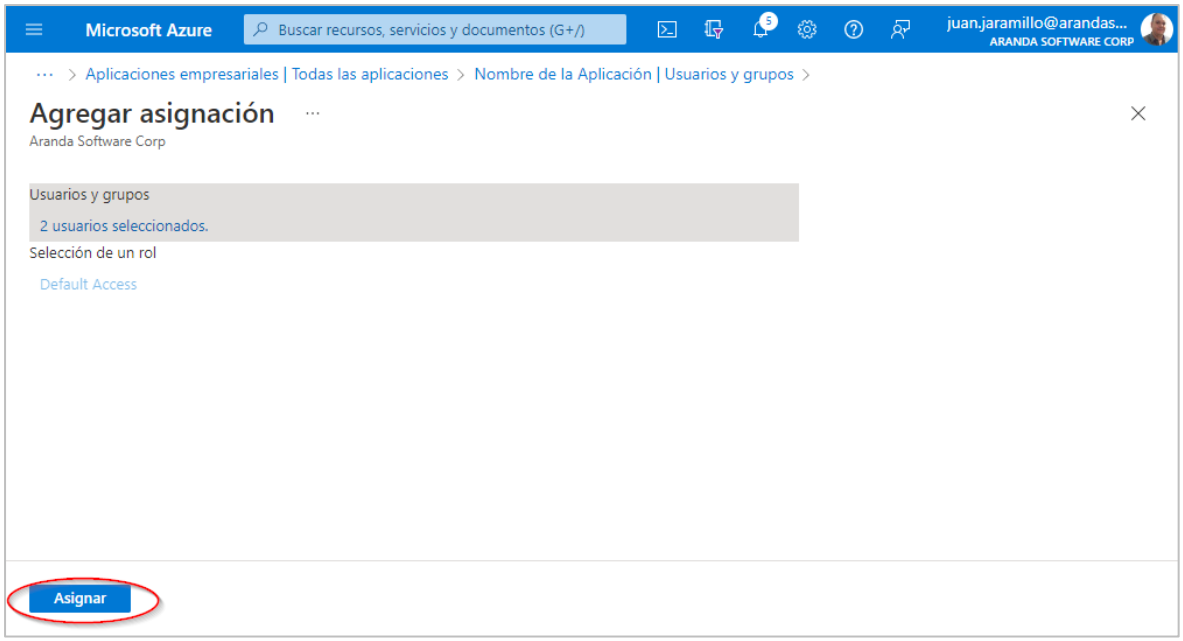
2. En la sección **Administrar** busque y seleccione **Usuarios y grupos**> y luego **Agregar usuario o grupo**.



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**.



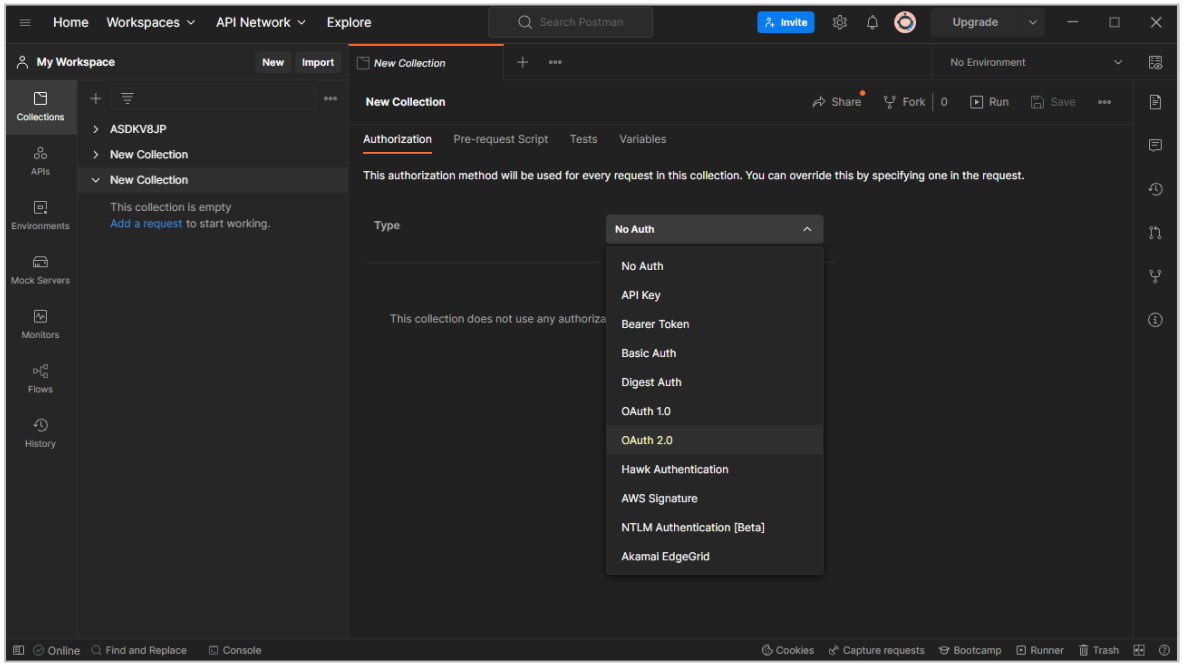
4. Finalmente seleccione Asignar



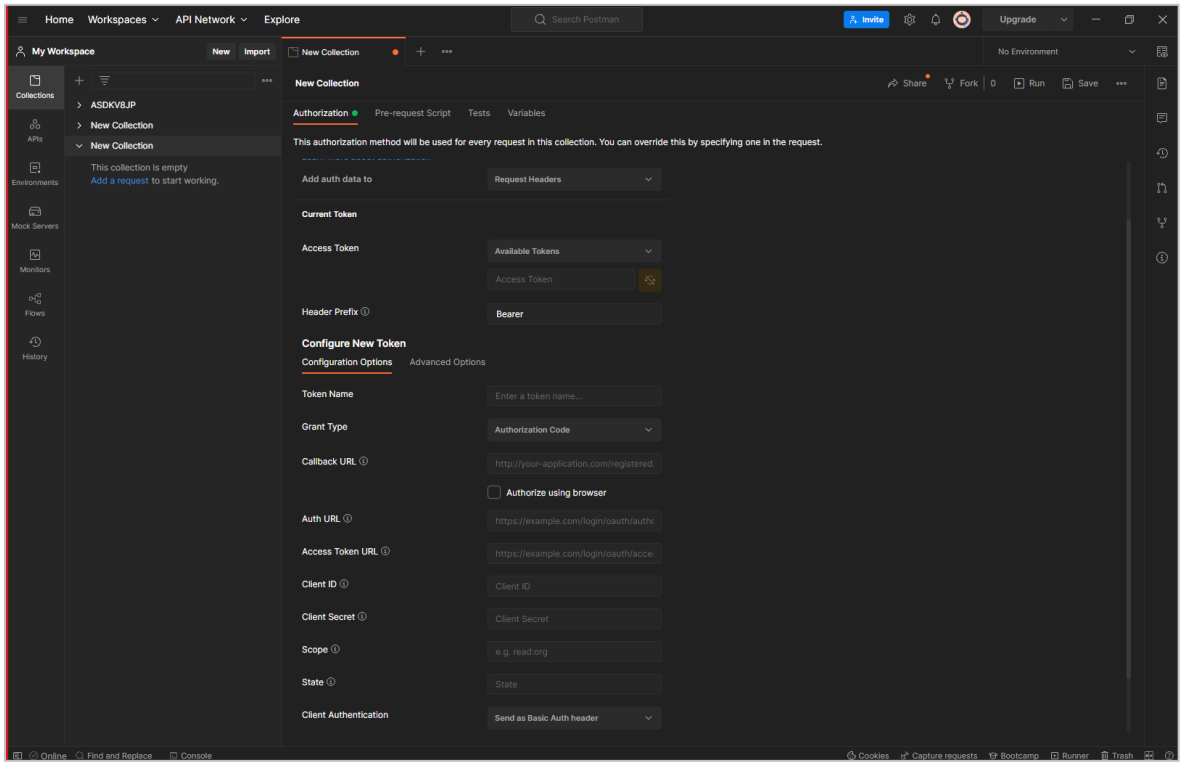
Solicitud del Refresh_Token

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

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



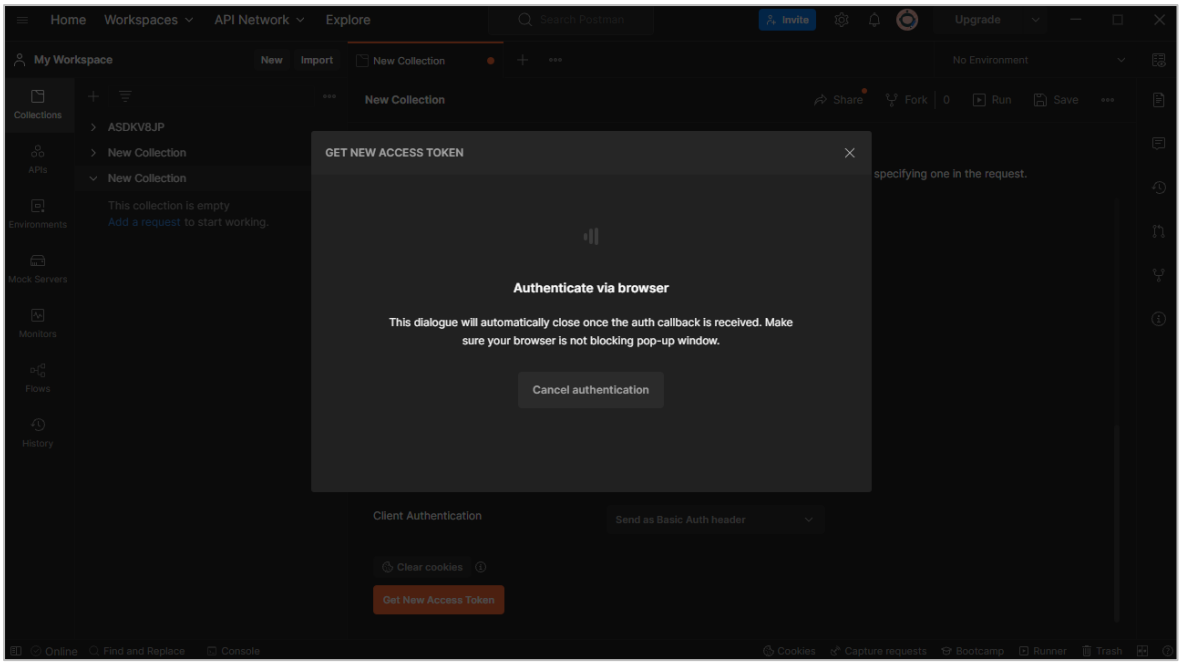
2. En la vista se debe diligenciar los campos de la siguiente manera:

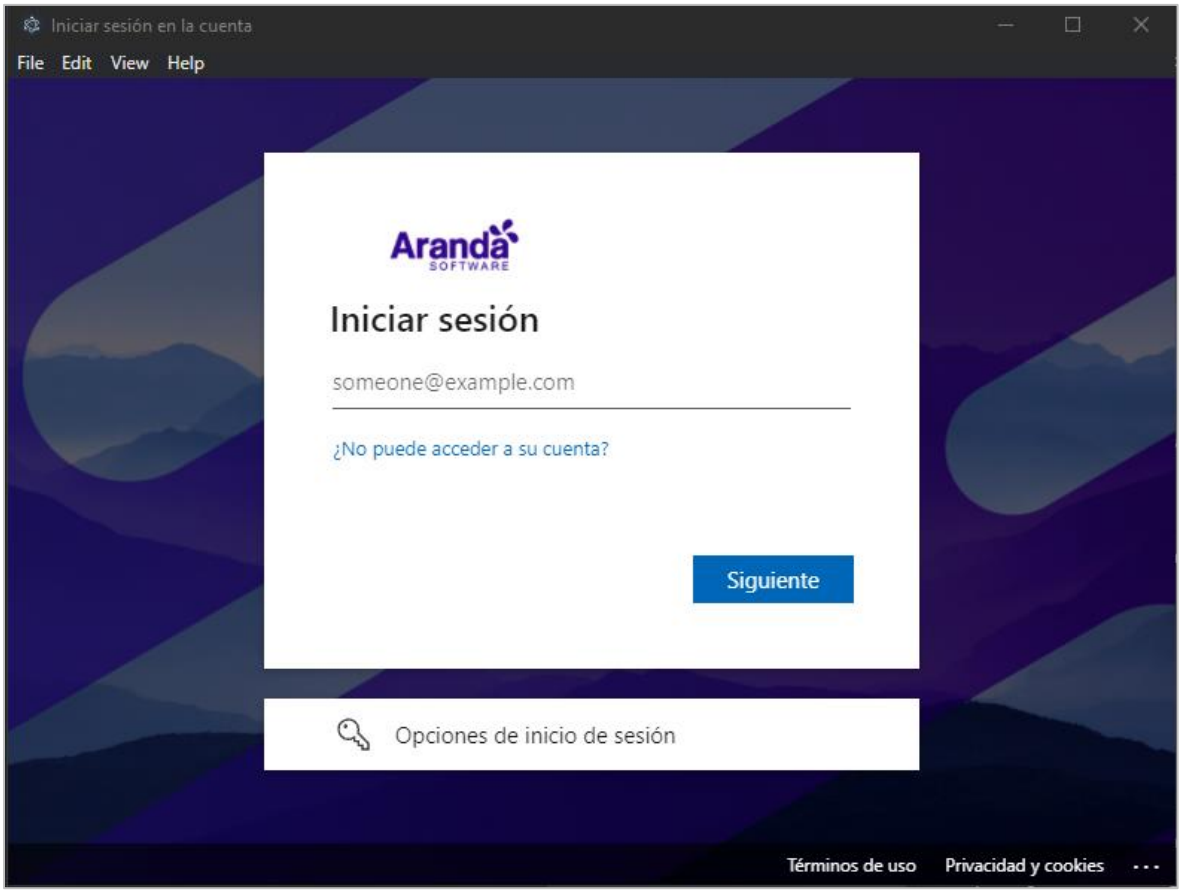


Type = OAuth 2.0
Add auth data to = Request Headers
Acces Token = Availabe Token
Header Prefix = Bearer
Token Name = Nombre que desee para la colección
Gran Type = Autorization Code
Callback URL = http://localhost
Auth URL= Debe ingresar el valor de Punto de conexión de autorización de OAuth 2.0 (v2).
Access Token URL = Debe ingresar el valor de Punto de conexión de token de OAuth 2.0 (v2).
Client ID = Debe ingresar el valor de Id. de aplicación (cliente).
Client Secret = Debe ingresar 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.

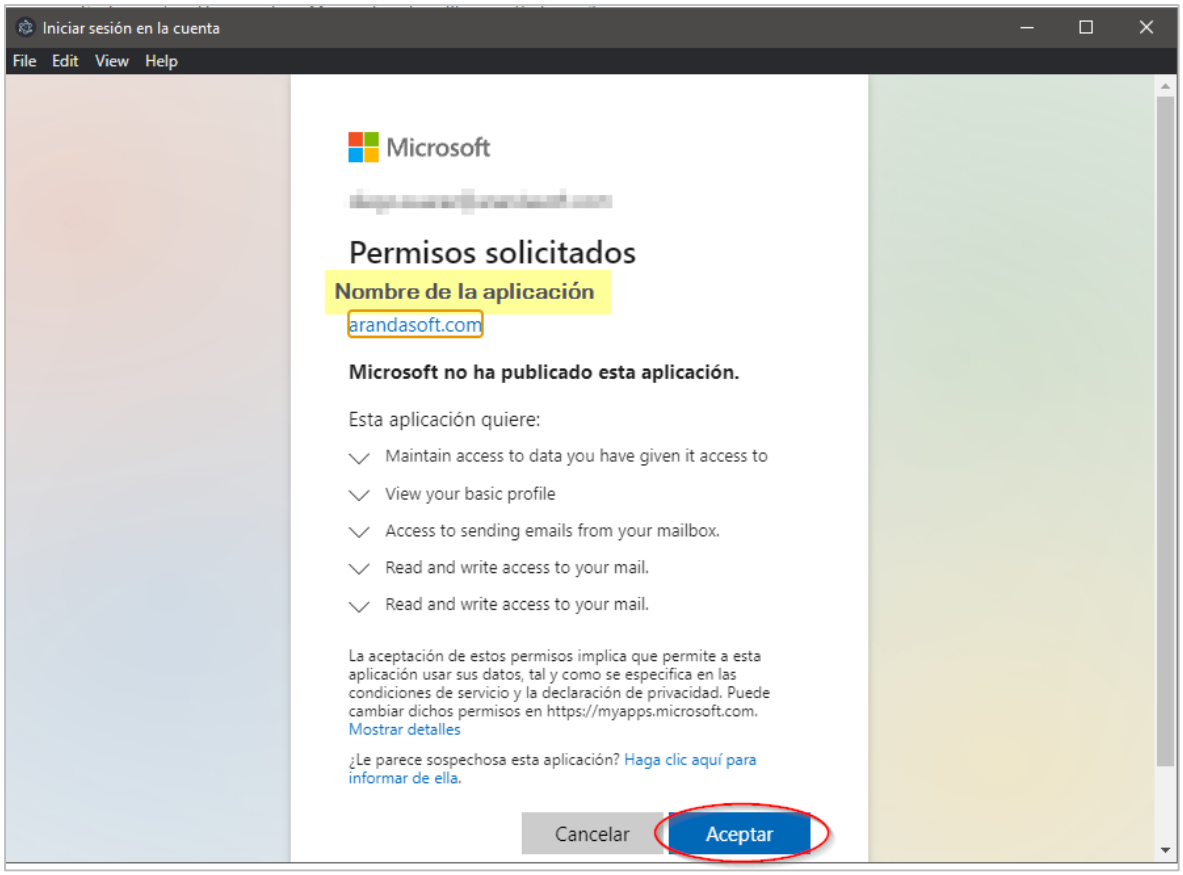
Cuando si diligencia toda la información seleccionamos **Get New Access Token.**

3. Se deben abrir dos ventanas, una ventana donde se deben ingresar las credenciales de acceso y la otra donde se visualiza el proceso de solicitud del Token.





4. 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.