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. Esta guía le presenta al cliente la configuración previa a tener en cuenta para la sincronización de usuarios del directorio activo desde Microsoft Entra ID.

Sincronización Microsoft Entra ID

Precondiciones

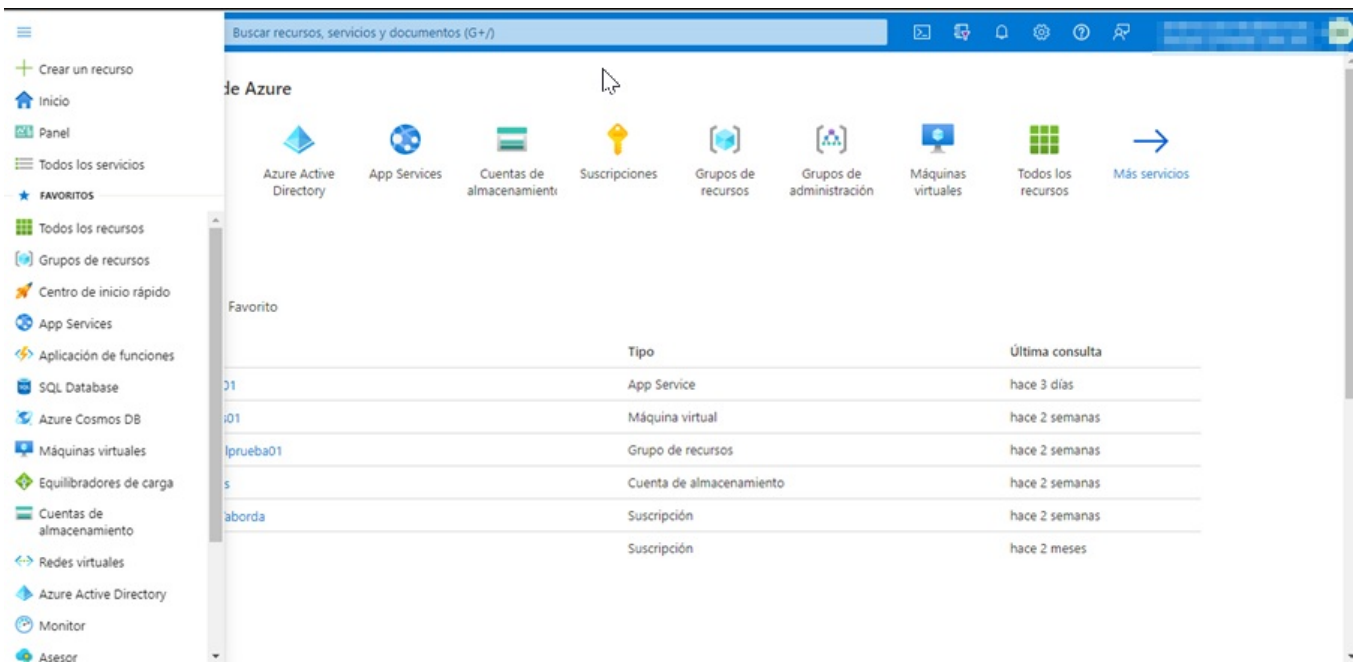
- Una cuenta de Azure con permisos para administrar aplicaciones en Microsoft Entra ID.
- Roles de Microsoft Entra ID con los permisos requeridos:

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

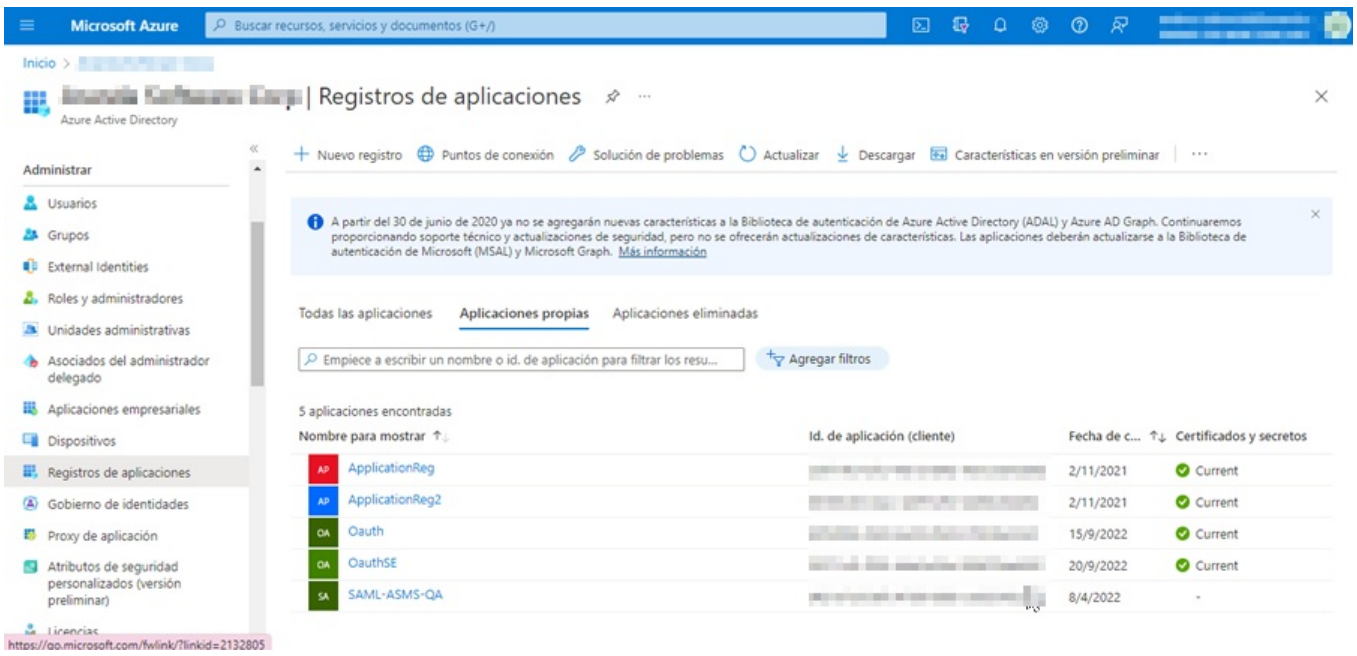
Creacion Aplicación en Azure

Cómo crear una aplicación en Azure

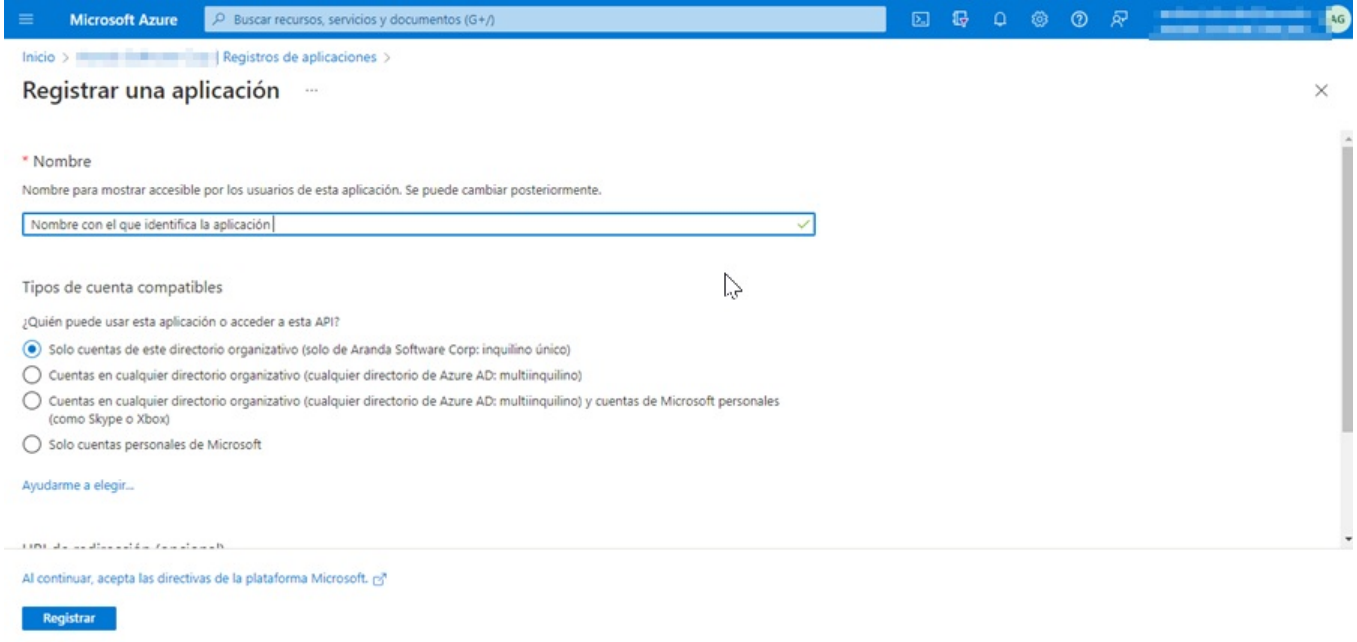
1. Se accede al portal de Azure Ver Microsoft Azure , busque y seleccione **Microsoft Entra ID**.



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



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

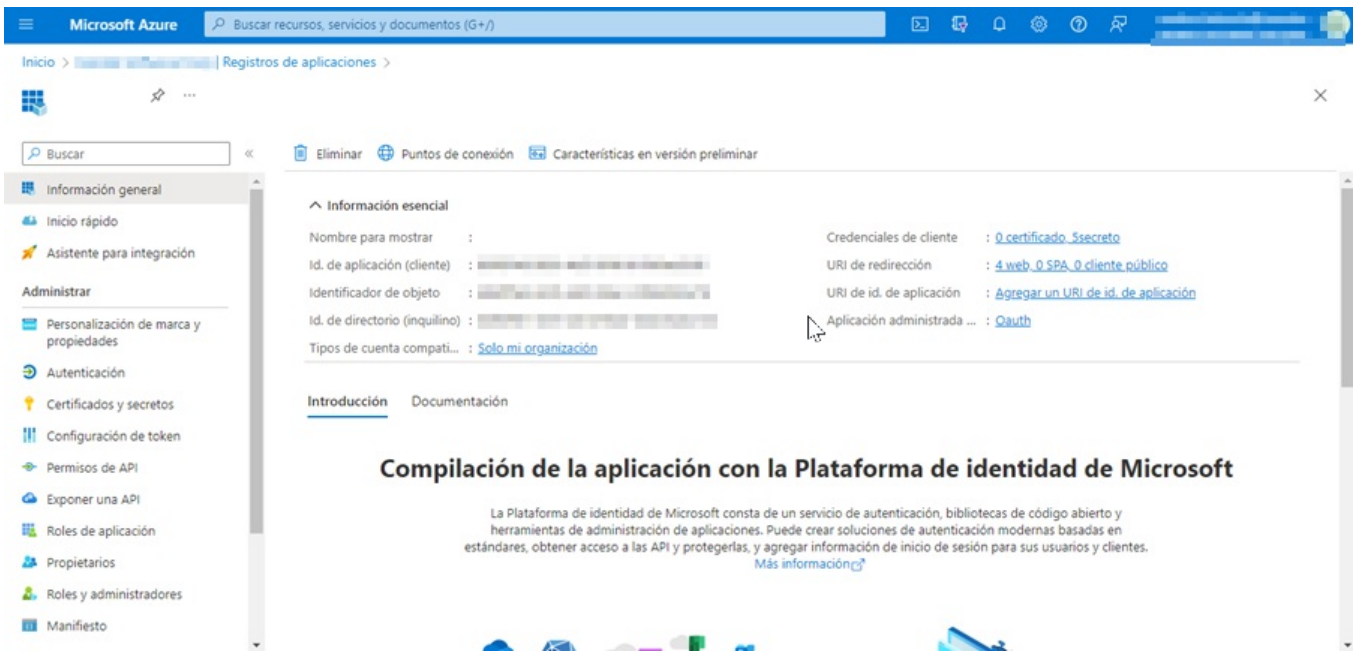


4.Cuando se tenga registrada la aplicación, guarde los siguientes datos que se requieren para la configuración en la sincronizacion de LDAP con Microsoft Entra ID.

- **Id. de directorio (inquilino)**=URL

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

- Id. de aplicación (cliente)= Cliente id



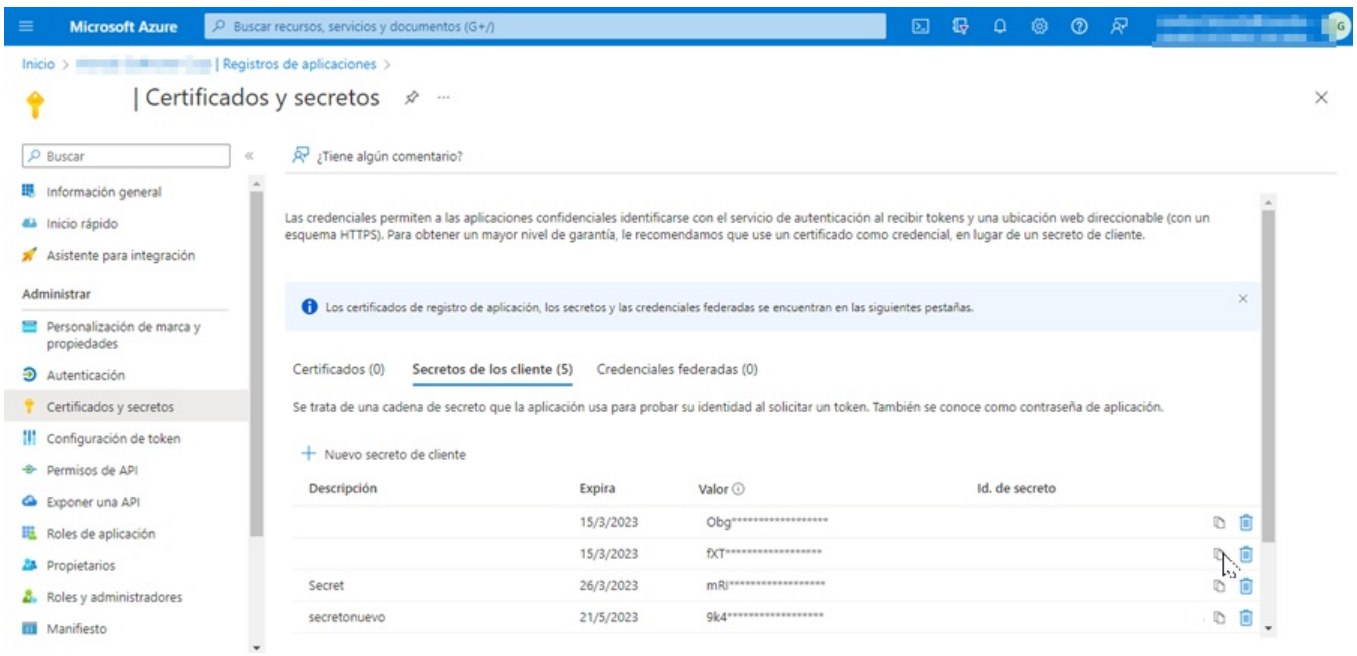
Configuración de la aplicación en el portal Azure

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

Creación del Secreto

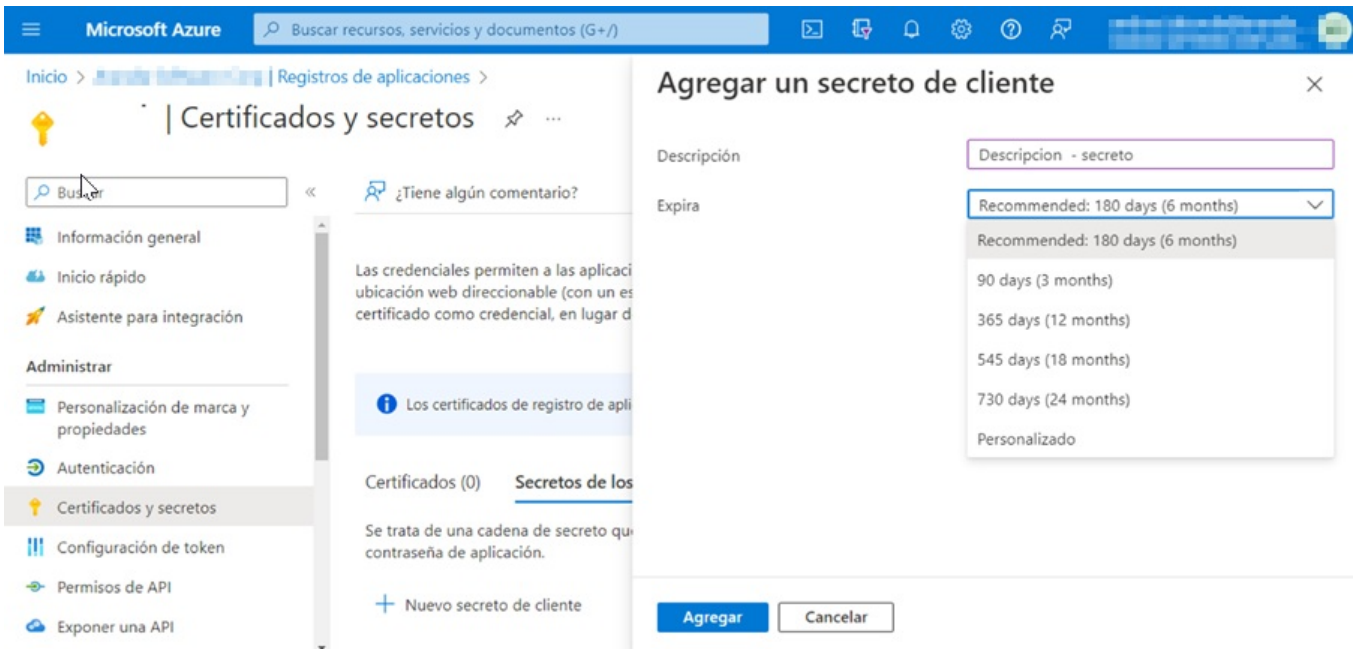
1. Para crear el secreto ingrese al portal de Azure > Menú > Microsoft Entra ID > Registros de aplicaciones > seleccione la aplicación creada del listado disponible.

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



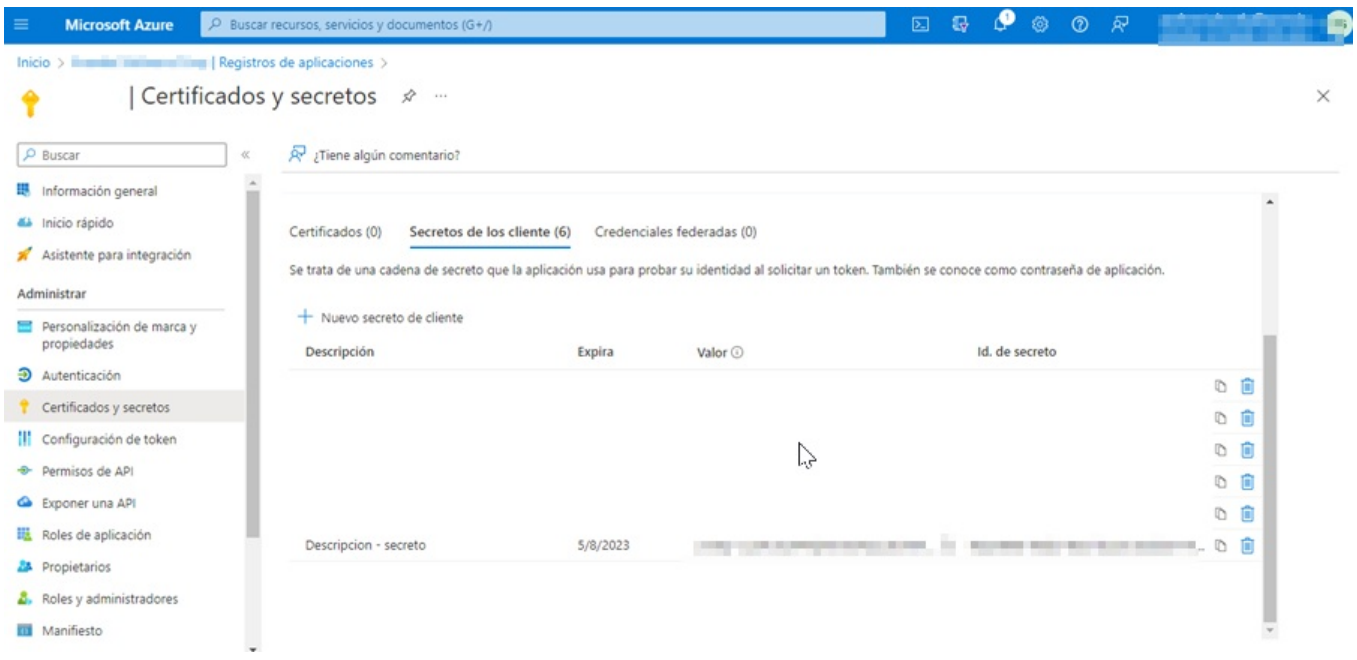
3. En la ventana **Agregar un secreto de cliente** diligencie el campo **Descripción**, defina la duración del secreto en el campo **Expira** y haga clic en el botón **Agregar**.

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



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

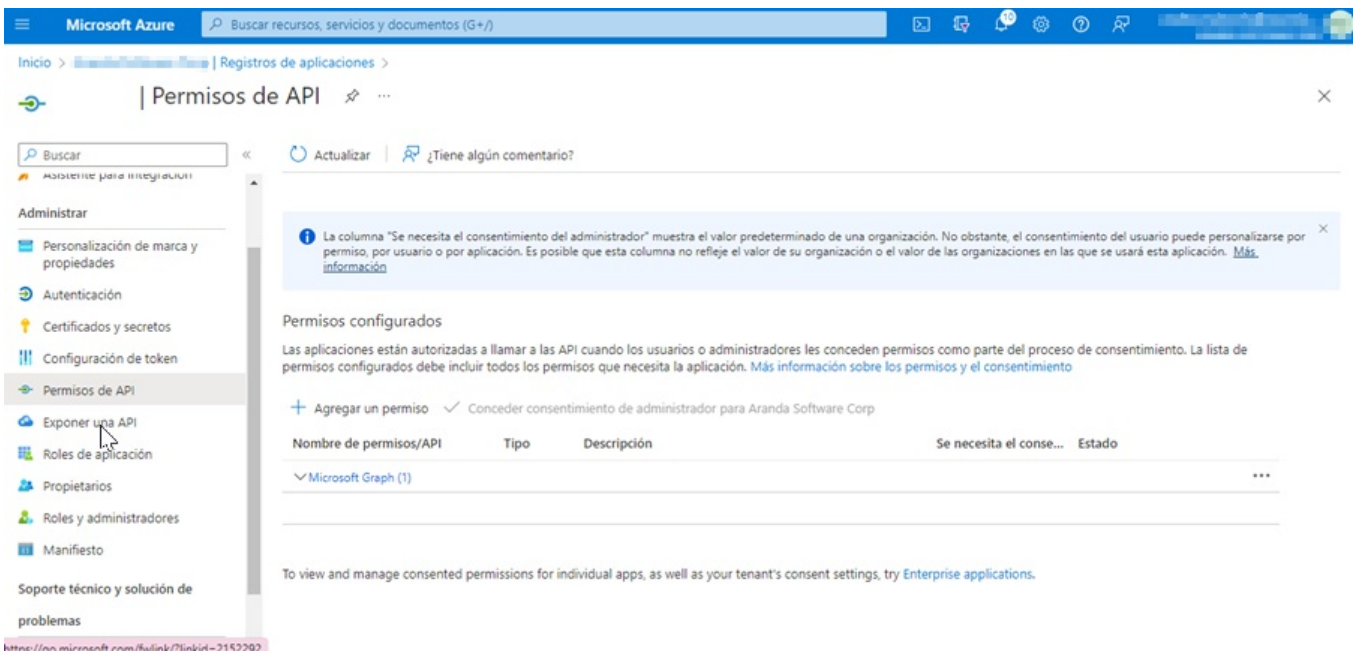
- Valor secreto de cliente = Cliente secreto.



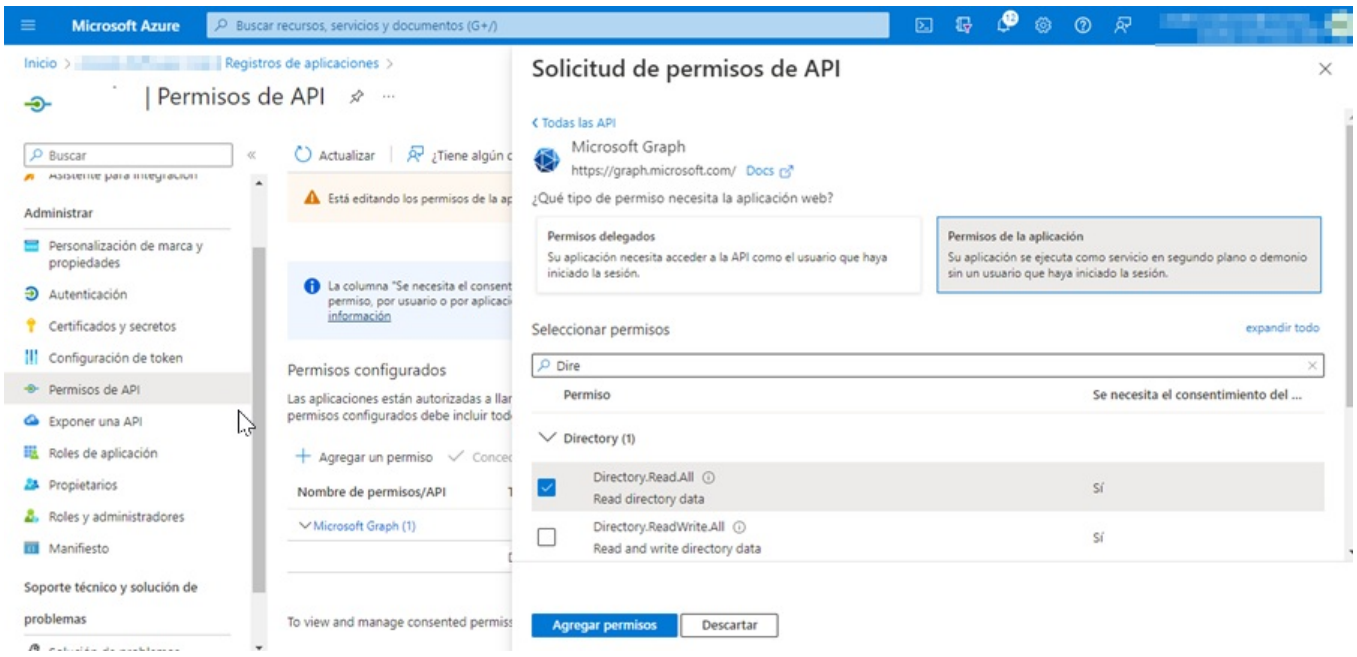
Configurar permisos de API

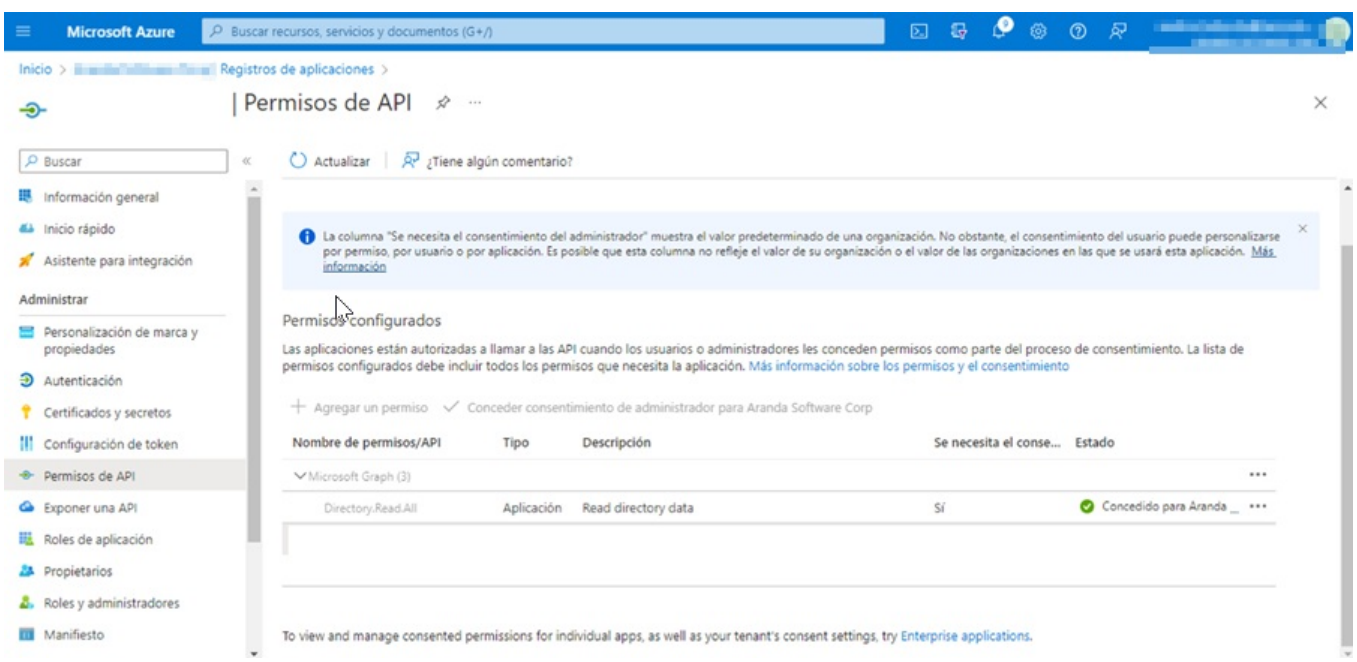
1. Para configurar los permisos de API se ingresa al portal de Azure > Menú > Microsoft Entra ID > Registros de aplicaciones > seleccione la aplicación creada del listado disponible.

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



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





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

Sincronización de ldap con Microsoft Entra ID en aplicaciones Aranda

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

- Ver Sincronización y configuracion Aranda Service Management ASMS