Configuración EntraId - Gente, Autogestión y Portal Azure

Instructivo de configuración

Creación

21-05-2025

Versión

1.0.0

Plantilla

SS-IC-01-ES

Código

SAICO-IC-01-ES

Autor

Maurizio Quaroni

Índice

1 Introducción

El objetivo de este documento es brindar apoyo para la correcta configuración Gente y Autogestión para el correcto funcionamiento de EntraId en el sistema.

2 Propósito

Establecer las pautas necesarias para garantizar que todo lo que corresponda con EntraId se configure de manera uniforme y adecuada.

3 Audiencia

Este documento está dirigido a los equipos de las distintas áreas de SAICO que requieran comprender la configuración necesaria para el correcto funcionamiento de lo que abraca EntraId. También para aquellos clientes que necesiten configurar y/o visualizar la configuración de EntraId para su correcto funcionamiento en el sistema.

4 Términos y Acrónimos

Término	Definición o descripción
EntraId	Solución de administración de identidades y acceso de Microsoft que ayuda a las organizaciones a proteger y administrar identidades en entornos locales y en la nube.
Portal Azure	Portal donde se harán las configuraciones para generar el vínculo entre el login de Microsoft por entra id, con autogestión.

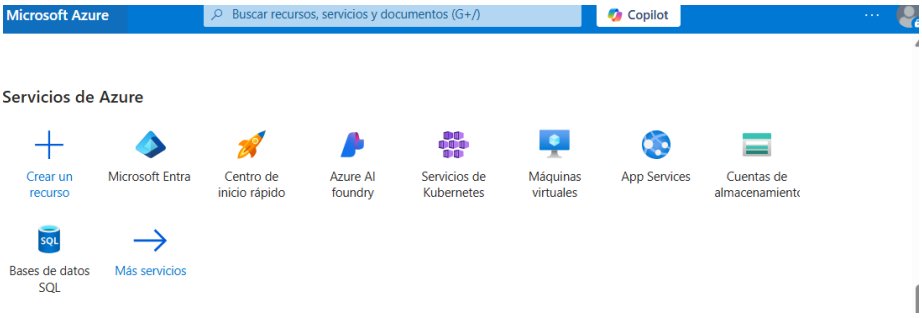
5 Pasos para la Configuración de EntraId en Gente-Autogestión y Portal Azure

5.1 Configuración en Portal Azure.

5.1.1 Ingresar al portal azure

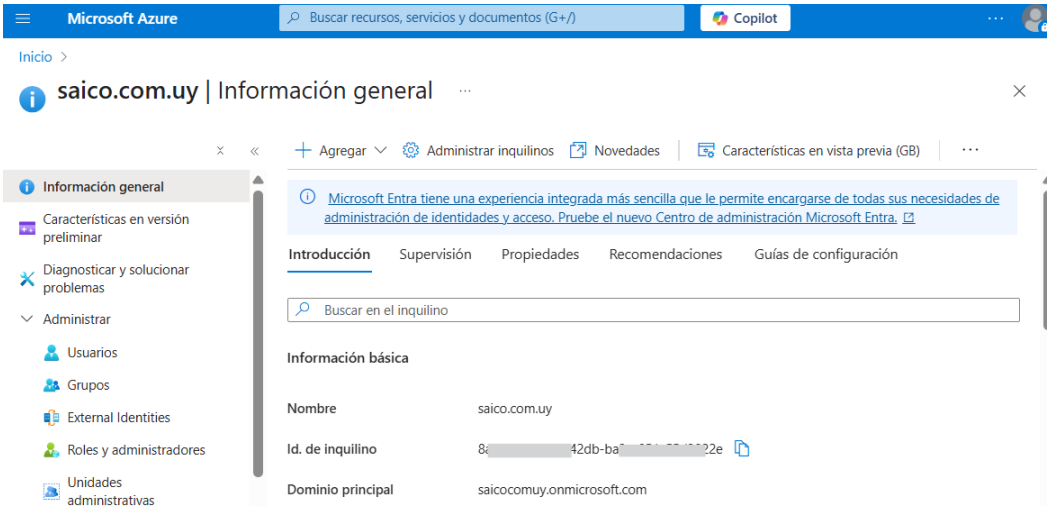
Dirigirse a: https://azure.microsoft.com/es-es/get-started/azure-portal/

Elegimos el servicio Microsoft Entra



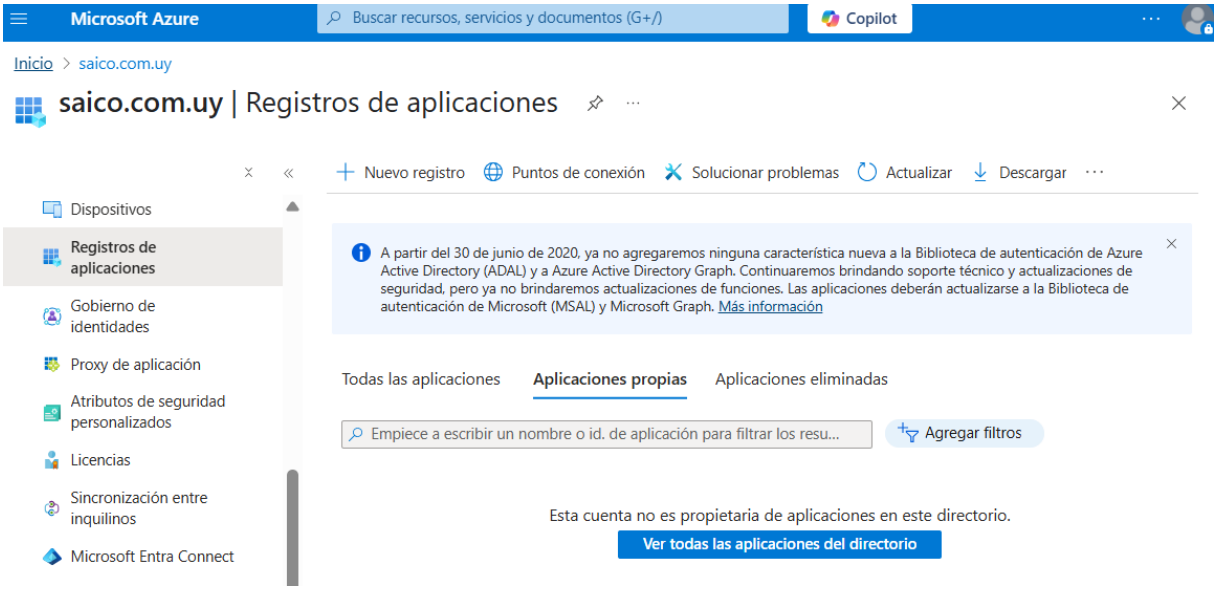
5.1.2 Obtener datos (Tenant Id)

Nos llevará a la pantalla principal, donde podremos obtener el dato del TenantId (o inquilino).



5.1.3 Registro de aplicación.

Como siguiente paso debemos crear la aplicación (si no se tiene una creada). Para ello hay que dirigirse dentro del menú principal, a la opción Registro de aplicaciones y presionar sobre + Nuevo Registro.

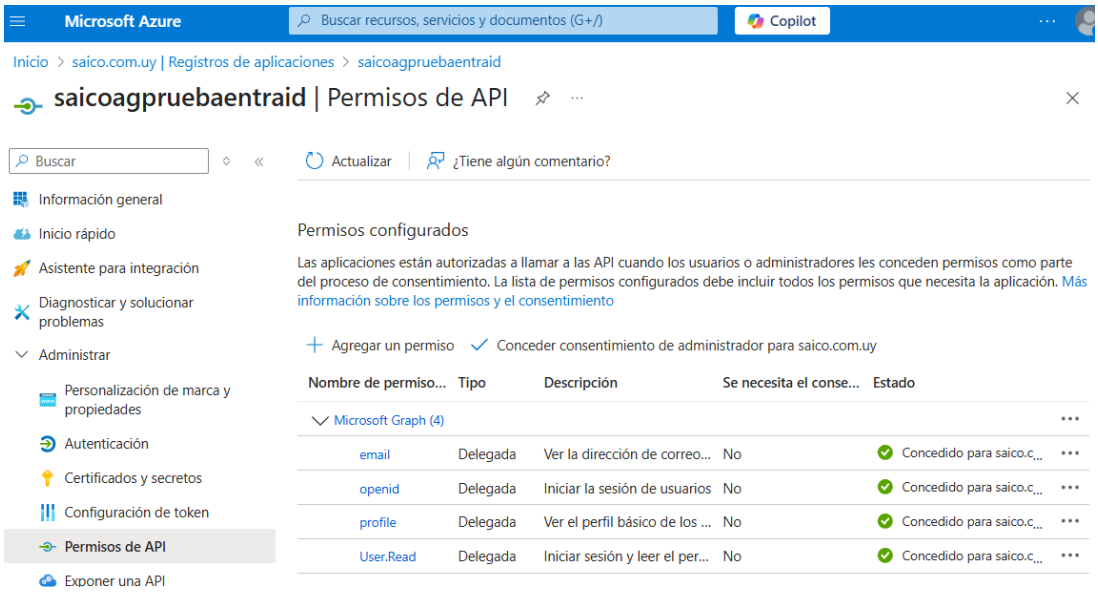


Configuramos el tipo de cuenta compatible y confirmamos

5.1.4 Permisos de Api.

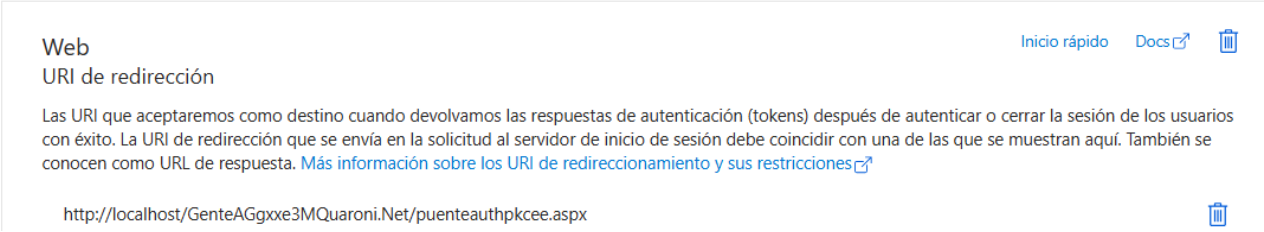
El siguiente paso sería, una vez creada la aplicación, ingresar en ella y seleccionar la opción de menú Permisos de Api.

Los permisos se asignan a partir del botón + Agregar un permiso → Microsoft Graph → Permisos Delegados y ahí marcamos las casillas de email, openid y profile.



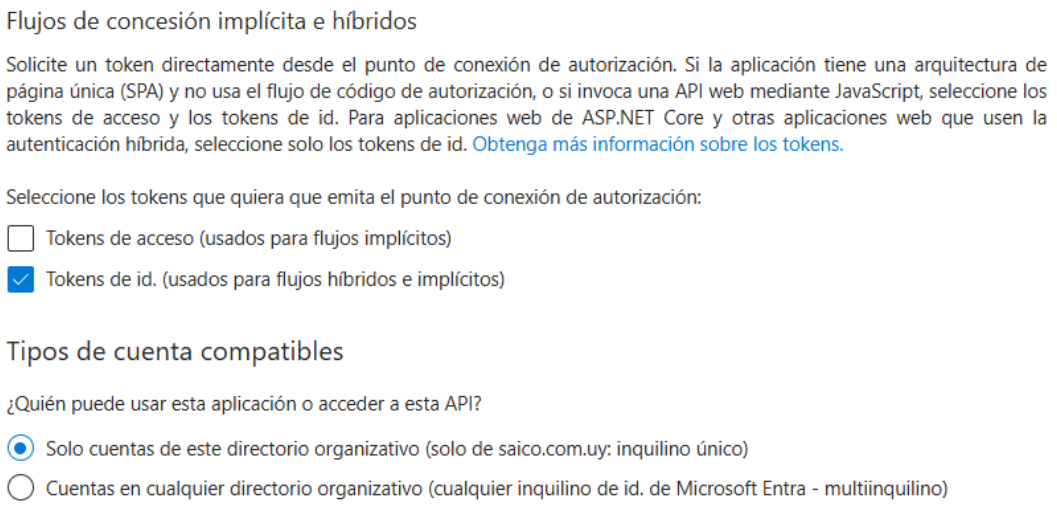
5.1.5 Autenticación

Aquí configuraremos la uri de redirección. Luego de autenticar o cerrar sesión, Microsoft debe tener en esta sección las url válidas a las que puede redirigir.



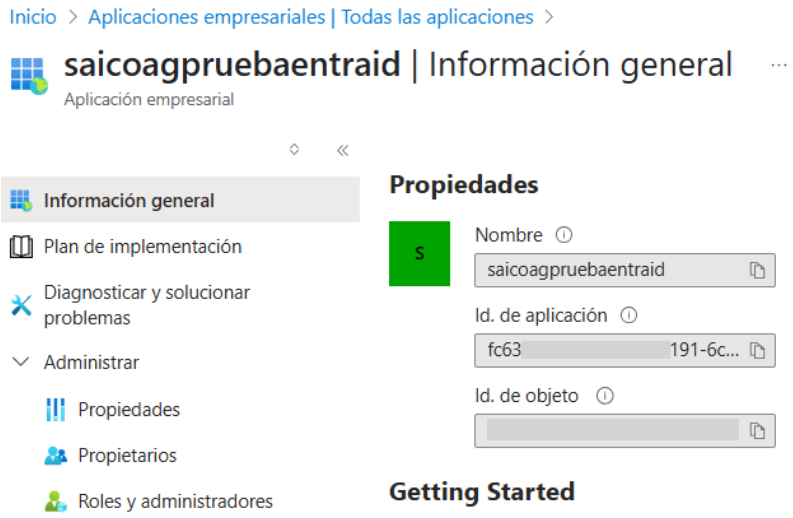
La otra configuración a tener en cuenta es la de flujos de concesión y tipos de cuenta compatibles.

Luego de cargada esa información se puede confirmar la autenticación.



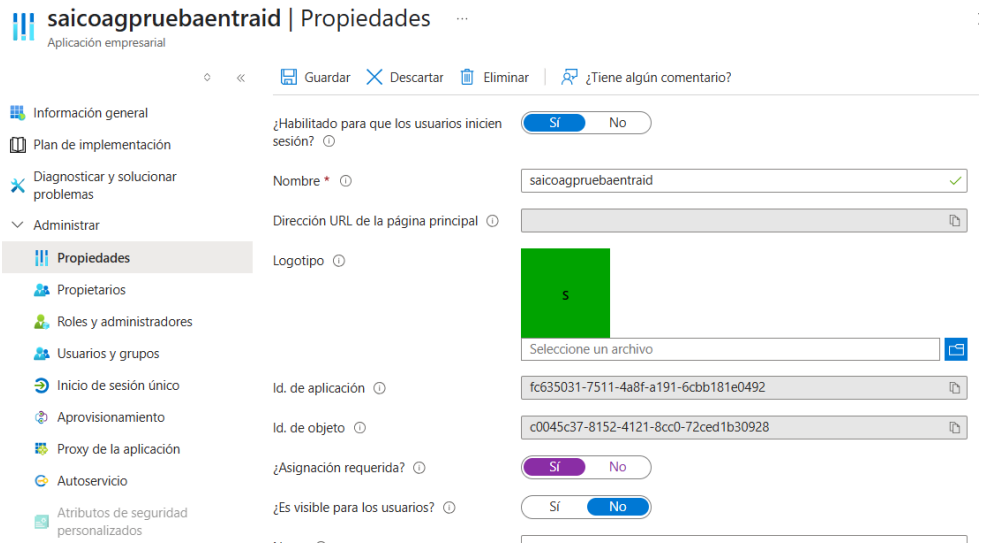
5.1.6 Información y propiedades de la aplicación

En Aplicaciones empresariales → nombre de la aplicación, donde dice Id. de aplicación obtendremos el otro valor necesario para la configuración del archivo creado desde Gente.

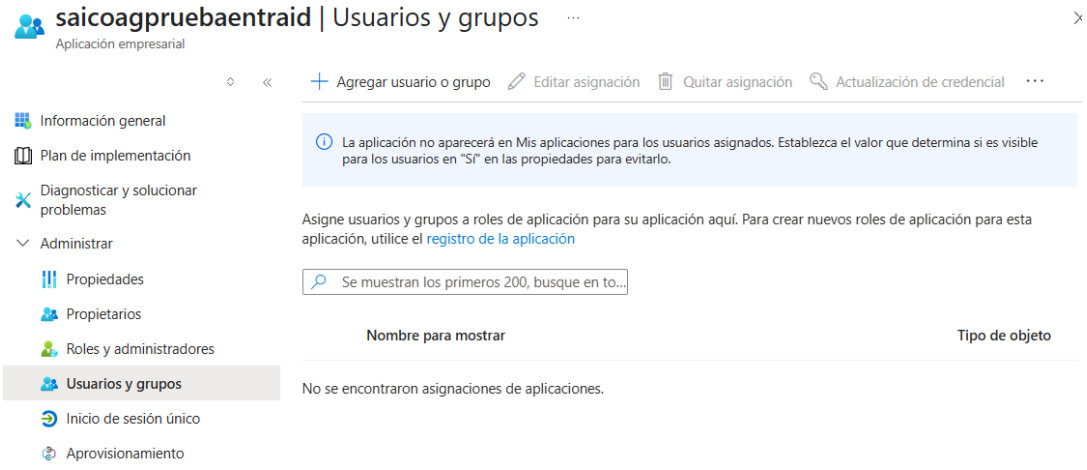


5.1.7 Asignación requerida

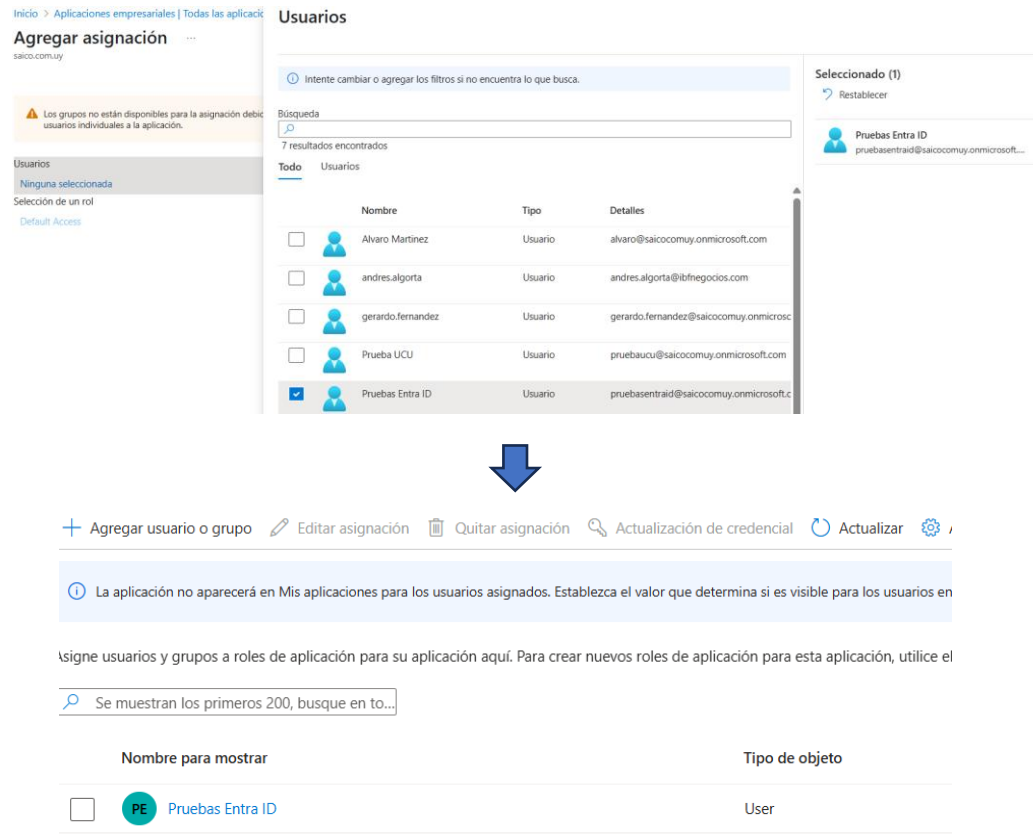
Ahora debemos dirigirnos a la opción de menú Propiedades para configurar (opcional), si para acceder a dicha aplicación se requiere estar asignado. También sirve para el escenario que por algún motivo un usuario (o grupo) no deba tener más acceso a la aplicación, quitándolo de la lista de asignados, al intentar acceder nuevamente a la aplicación ya no se le permitirá el acceso.



Menú Usuarios y grupos, botón + Agregar usuario o grupo

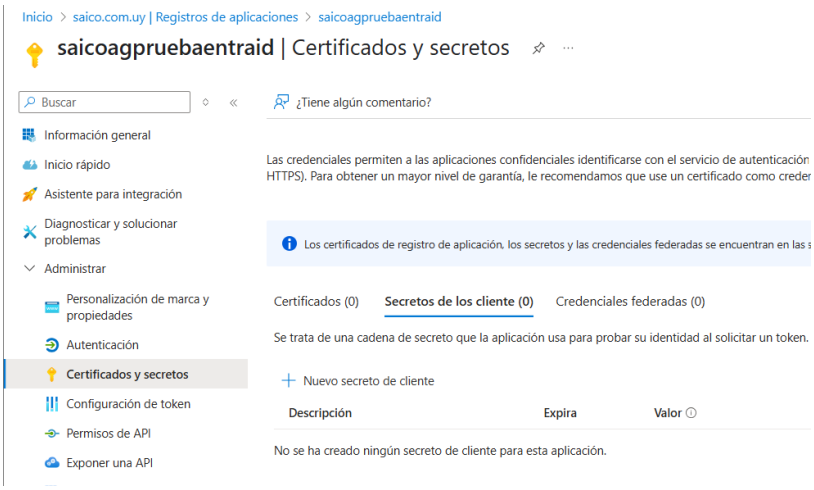


Seleccionar y asignar

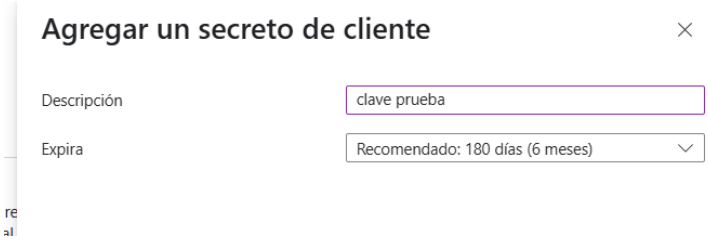


5.1.8 Certificados y secretos

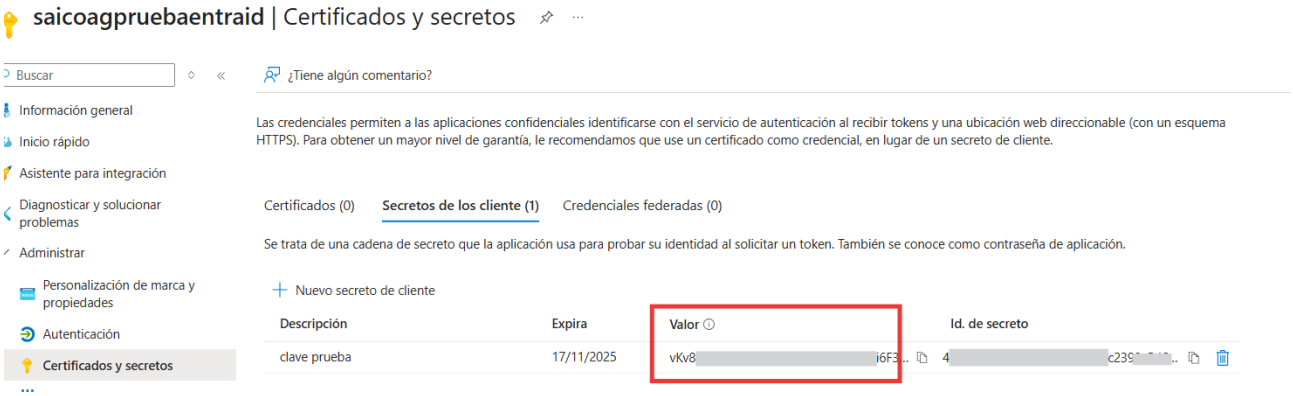
Por último, dentro de **Registro de aplicaciones → Certificados y secretos**, debemos crear una clave (secreto). Apenas se cree se tiene que guardar, ya que luego la aplicación la oculta y si se pierde se deberá generar una nueva. Este es el tercer y último ítem de los configurados en Gente para configurar el acceso a Entra Id.



+Nuevo secreto de cliente:



El valor será el dato a guardar de forma segura y a configurar en “configuración de JSON para Entra Id”



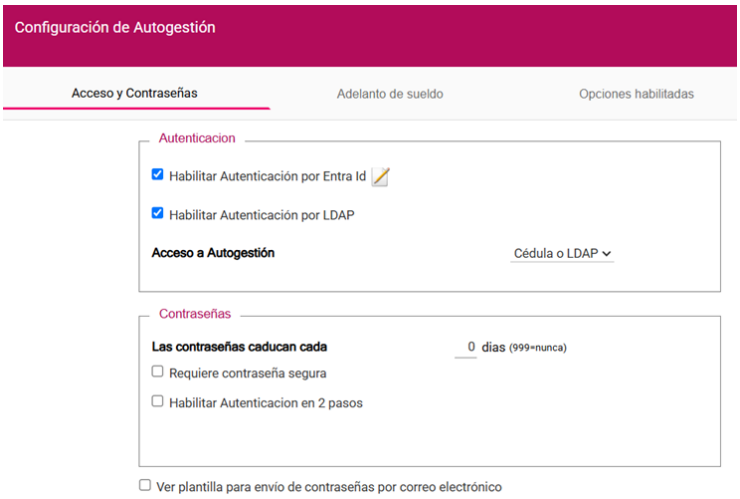
5.2 Configuración en Gente

5.2.1 Configuración Autogestión

Dirigirse al menú: Herramientas → Configuración → Opción Autogestión.

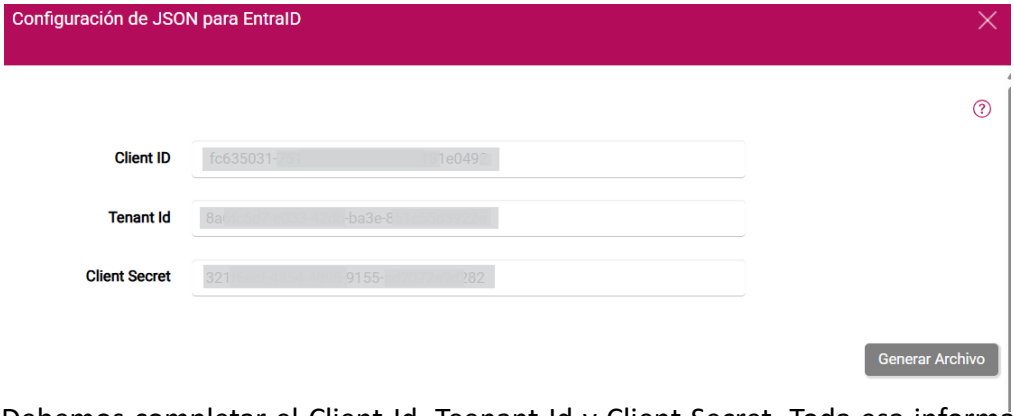
5.2.2 Pestaña Acceso y Contraseñas.

Se debe marcar el check de “Habilitar Autenticación por Entra Id”. Y eso habilitará el ícono que nos va a permitir agregar información necesaria para la conexión.



5.2.3 Configuración JSON con datos Azure

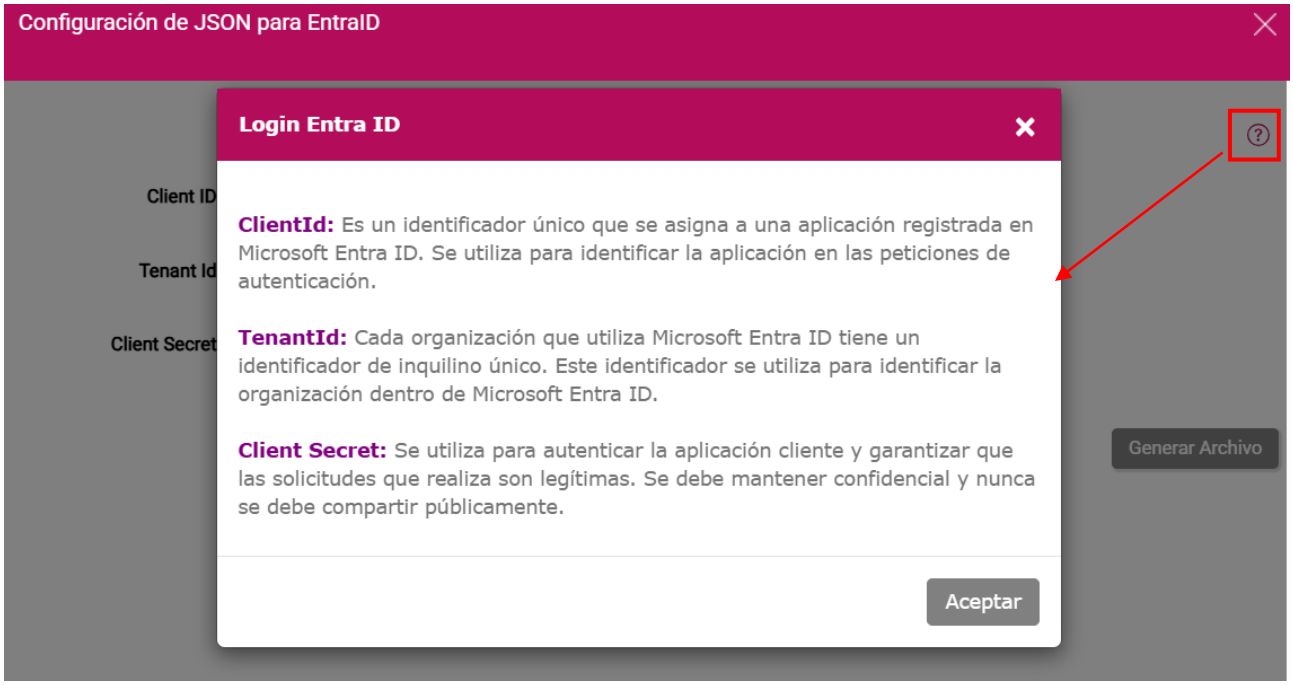
Hacer clic en el ícono de preferencias ( ) y nos abrirá el siguiente popup:



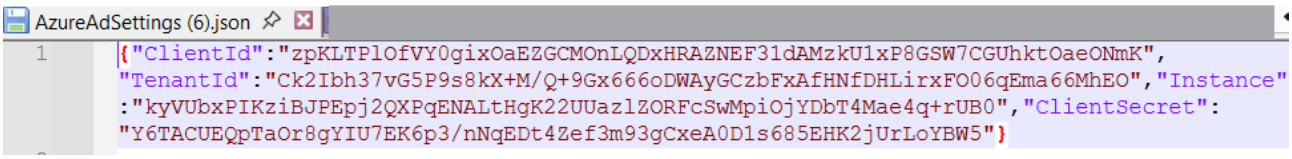
Debemos completar el Client Id, Teenant Id y Client Secret. Toda esa información la obtendremos del portal azure.

Al presionar sobre el icono '?' tendremos la definición de cada campo a completar.

Por último, luego de cargar los 3 valores, al cliquear sobre **Generar Archivo** se nos generará un archivo con extensión json con la información encriptada para luego configurar en autogestión (desarrollado más adelante).

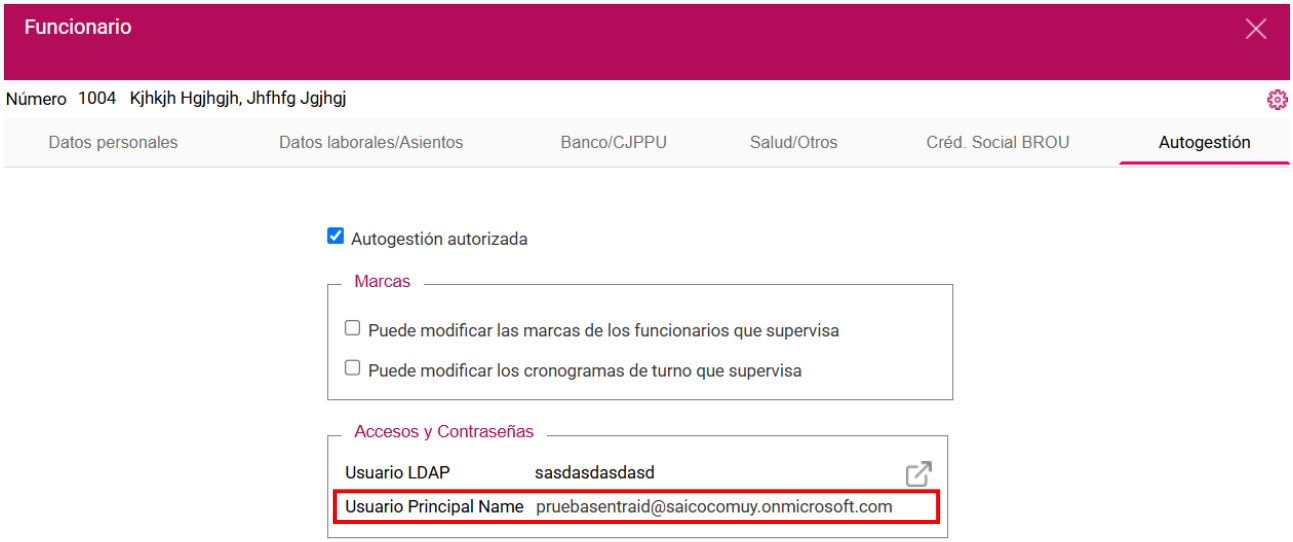


Archivo descargado ejemplo:



5.2.4 Configuración UPN.

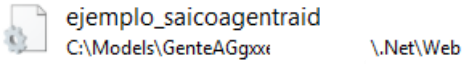
Como última configuración debemos agregar el upn (user principal name) en el funcionario. De esta forma se genera el vínculo a nivel de datos entre Gente/Autogestión y Entra Id.



5.3 Configuración para Autogestión:

5.3.1 Configuración saicoageentraid.ini

En dónde se encuentra instalada la aplicación de Autogestión, carpeta Web, podrán encontrar un archivo llamado ejemplo_saicoagentraid el cual se deberá copiar en la misma carpeta, pero sin el texto ejemplo_ (o simplemente renombrarlo) y ajustar la configuración.



De la siguiente manera podría quedar el archivo una vez configurado. Cada ítem explica cuales son sus opciones y como se comporta en cada caso. En este escenario, está habilitado el login con Entra Id, tiene una única empresa, se deja cargada la empresa en cuestión y por ultimo el nombre del archivo que se generó anteriormente desde Gente.

saicoagentraid.ini

```
habilitaEntraID=S
; Opcion S: Habilita login por EntraId, Opcion N: DesHabilita login por EntraId
unicaEmpresaEntraID=S
; En caso de tener una unica empresa marcar opcion S, si tiene mas de una empresa N
nombreEmpresaEntraID=genteDemoMQuaroni
; Se toma en cuenta cuando unicaEmpresaEntraID = S. Toma nombreEmpresaEntraID como base
nombreArchivoAzure=AzureAdSettings
; Nombre del archivo de configuracion de Azure para la conexion con EntraId
```

5.3.2 Copiar archivo generado.

Copiar el archivo generado en gente en el directorio Web dentro de la carpeta de instalación de Autogestión.

AzureAdSettings.json

```
{
    "ClientId":"mp5TlAg59j9xZ04aacxArjwJJXJAY07z2PvSjIBZjp78dTrG7CTleDB4O48lNgCd",
    "TenantId":"Ck2Ibh37vG5P9s8kX+M/Q+9Gx666oDWAyGCzbFxAfHNfDHLirxFO06qEma66MhEO",
    "Instance":"kyVUbxPIKziBJPEpj2QXPqENALtHgK22UUazlZORFcSwMpiOjYDbT4Mae4q+rUB0",
    "ClientSecret":"mmphvDJgP1T4RkdP9g5tJ4SE9khx6IKDm6FRwzPOYtTkZB5uIsaKmI1KHVa+7zsM"
}
```

5.3.3 Ajuste en web.config

Se debe agregar la política de seguridad hacia https://alcdn.msauth.ne porque Microsoft Entra Id utiliza ese dominio para cargar los scripts necesarios para el inicio de sesión. Si no se permite este dominio, el navegador bloquea esos scripts por política de seguridad, y el login no funciona correctamente.

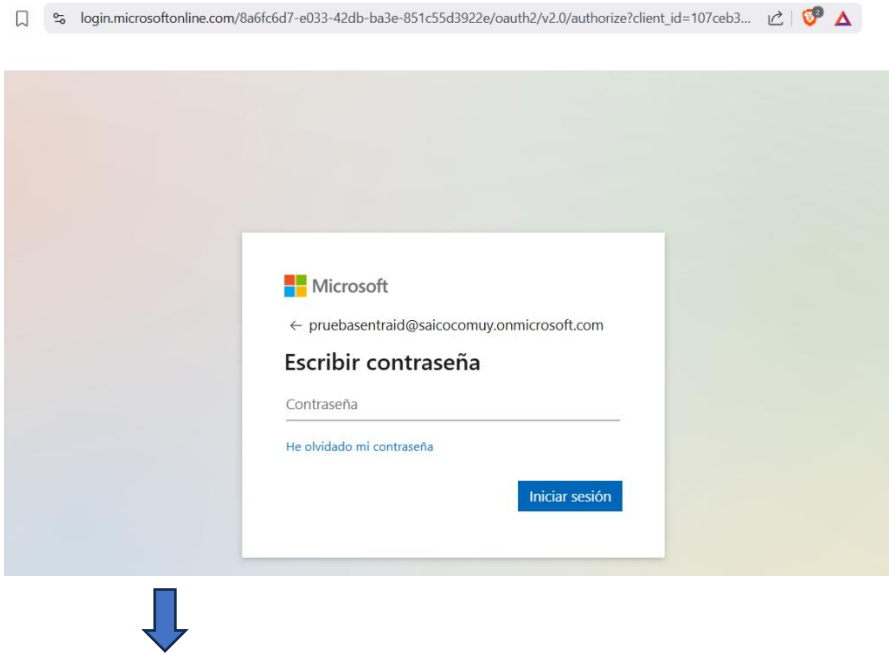
A continuación, adjunto un ejemplo de configuración del content security policy con la regla en negrita para entra id.

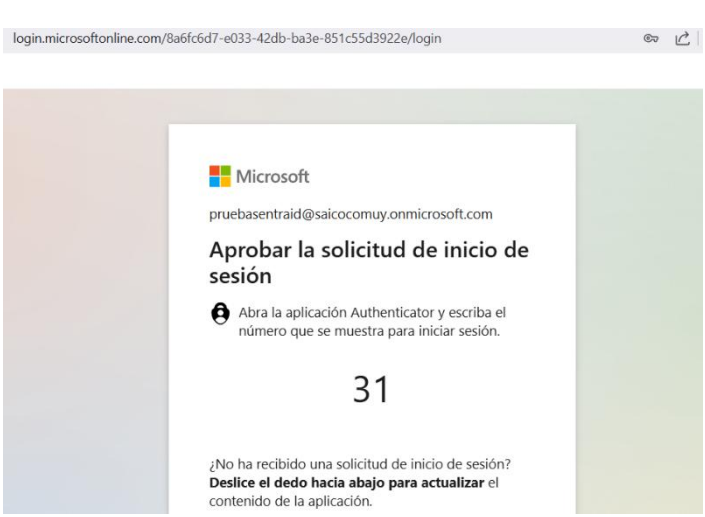
Ejemplo: <add name="Content-Security-Policy" value="default-src 'self'; frame-ancestors 'self'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; font-src 'self' https://fonts.gstatic.com; form-action 'self'; **script-src 'self' 'unsafe-inline' 'unsafe-eval' https://alcdn.msauth.net**; img-src 'self' data:;" />

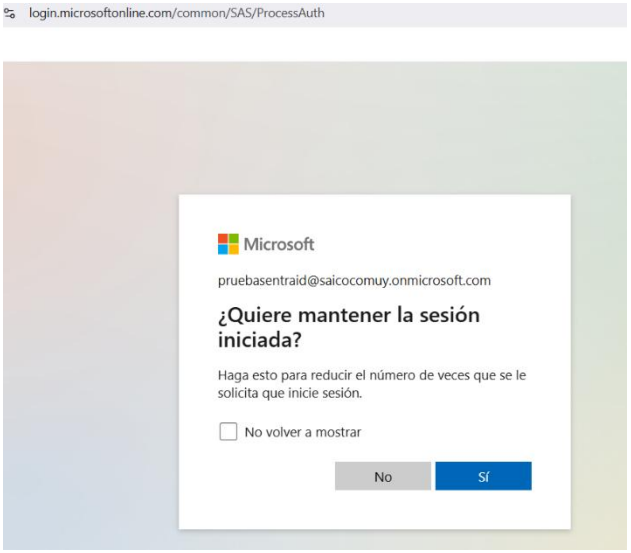
6 Verificación

1. Configurar un cliente con un email (upn) asignado a la aplicación.
2. Verificar que al dirigirse al link de login de Autogestión, automáticamente el sistema redirija al login de microsoft.
3. Ingresar las credenciales del usuario y confirmar que el acceso a la aplicación sea el correcto.

6.1 Login única empresa



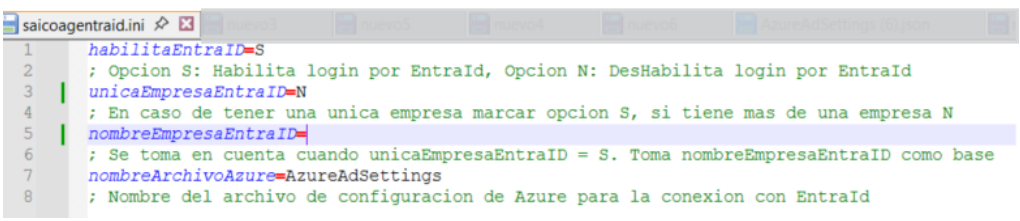




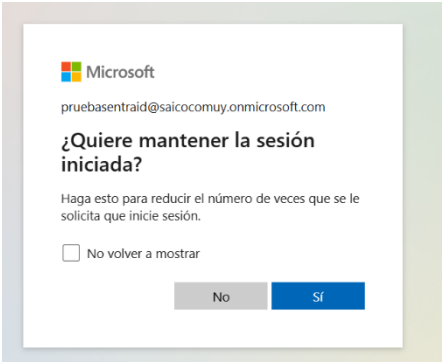
Login exitoso

6.2 Escenario Multi-Empresa

Configuramos el .ini para que inhabilite el unicaEmpresa

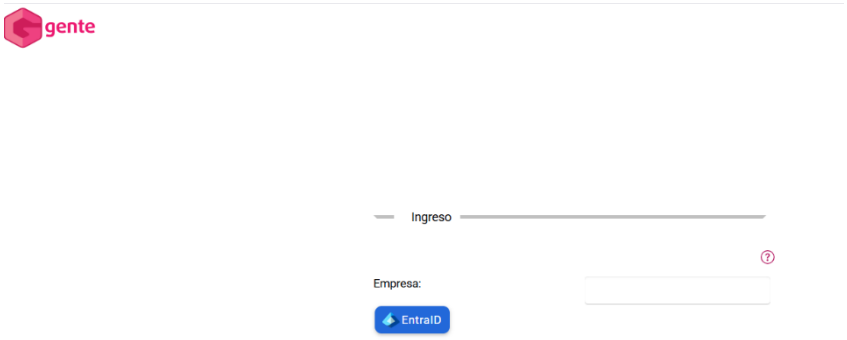


Mismo proceso de login indicando email, clave y segundo factor de autenticación.

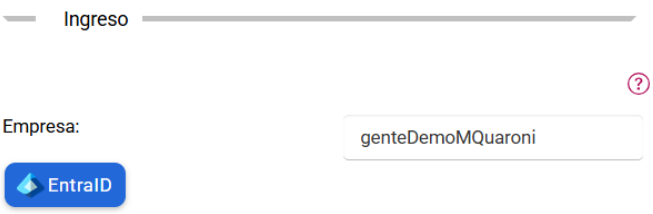


6.2.1 Pantalla de selección de empresa

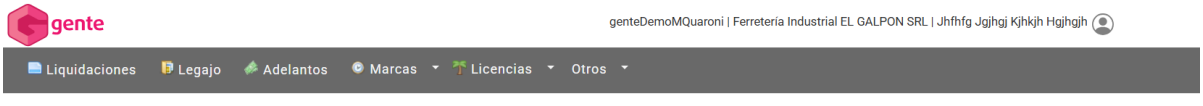
El login de microsoft nos redirigirá a una pantalla intermedia con el login para ingresar la empresa del usuario.



Ingresamos la empresa y presionamos sobre el botón EntraID



Login exitoso



Historial de cambios al documento

Versión	Fecha	Autor	Detalle
1.0.0	21-05-2025	Maurizio Quaroni	**Primera versión del documento**