

Cómo autorizar a Cloner 365 en su tenant de Microsoft 365

Cloner 365 se conecta mediante una aplicación registrada en su tenant, con permisos de Microsoft Graph. Estos pasos los realiza un administrador de su organización; no se instala nada en los equipos.

Antes de empezar

- ✓ Un administrador con permisos para **registrar aplicaciones** en Microsoft Entra ID (antes Azure Active Directory) y para **conceder consentimiento de administrador**.

Lo que obtendrá

- ✓ El **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.
- ✓ Un **secreto de cliente** vigente.
- ✓ Con esos datos, nuestro equipo vincula las cuentas con Cloner 365.

Registrar la aplicación

1 Crear un nuevo registro

En Microsoft Entra ID, entre a **Registros de aplicaciones** → **Nuevo registro**. Use un nombre que identifique su uso, por ejemplo "Cloner 365"; el nombre no tiene relevancia técnica.

2 Guardar la información esencial

Al abrir la aplicación creada, anote los datos de la sección **Información esencial**: el ID de aplicación (cliente) y el ID de directorio (inquilino).

3 Crear un secreto de cliente

En **Certificados y secretos** → **Nuevo secreto de cliente**, use un nombre alusivo y la caducidad máxima (2 años). Azure muestra el valor **solo una vez**: cópielo y guárdelo en un lugar seguro. Antes de que caduque habrá que generar uno nuevo.

4 Agregar los permisos

En **Permisos de API** → **Agregar un permiso** → **Microsoft Graph** → **Permisos de la aplicación**, agregue los permisos de los cinco grupos de la página siguiente.

5 Conceder el consentimiento

Con todos los permisos agregados, elija **Conceder consentimiento de administrador** para su dominio. Todos deben quedar en estado "Concedido".

6 Vincular las cuentas con Cloner

Por último, se vinculan las cuentas del dominio con Cloner 365. Recomendamos hacerlo con la asistencia de uno de nuestros técnicos de soporte.

Permisos de Microsoft Graph

Cloner 365 necesita **permisos de aplicación** de Microsoft Graph en cinco grupos. Permiten acceder a los usuarios, a los sitios de SharePoint, a OneDrive y a Outlook, leer los archivos y correos para respaldarlos, y escribir en esos mismos espacios cuando se hace una restauración.

Grupo	Qué cubre	Para qué
Directory	Directorio de la organización	Identificar a los usuarios y recursos que se respaldan.
Files	Archivos de OneDrive y SharePoint	Leer los archivos para respaldarlos, y escribirlos al restaurar.
Mail	Buzones de Outlook (Exchange Online)	Leer los correos para respaldarlos, y devolverlos a su carpeta de origen al restaurar.
Sites	Sitios y bibliotecas de SharePoint	Leer su contenido para respaldarlo, y restaurarlo.
User	Usuarios de la organización	Identificar las cuentas cuyos datos se respaldan.

Dentro de cada grupo se elige el nivel de acceso: lectura para respaldar y escritura para restaurar. **Nuestro técnico de soporte le confirma el nivel exacto de cada grupo** durante la configuración, antes de conceder el consentimiento.

Cómo usa Cloner este acceso

- ✓ La conexión con Microsoft se hace por la Graph API, con las medidas de seguridad que define Microsoft.
- ✓ La copia queda cifrada en la infraestructura de Cloner, y solo se accede a ella con aprobación escrita de un administrador registrado en el contrato.
- ✓ Puede revocar el acceso en cualquier momento, eliminando la aplicación o su secreto en Microsoft Entra ID.

¿Dudas o necesita ayuda?

Nuestro equipo puede acompañarlo en todo el proceso. Escribanos a **soporte@cloner.cl** o llámenos al **+56 2 2492 0162**, de lunes a viernes, de 9:00 a 18:00.