MANUAL DEL USUARIO · CENTRO DE AYUDA DE SIAC

Directorio Activo de Microsoft

Tu gente entra con su cuenta de Microsoft; quien sale de la empresa sale de SIAC. Conecta el Entra ID de tu empresa y tu gente entra a SIAC con su cuenta de Microsoft — en el panel, en Excel, en Chrome y en el escritorio. El directorio trae quién es cada persona y dónde está en la empresa; SIAC sigue gobernando qué puede hacer con la IA y cuánto puede gastar.

Dirigido a	Plataforma	Tiempo	Pantallas capturadas
Administradores	**SIAC v1.0.147**	**10 minutos**	**30 de septiembre de 2026**

Contenido

1 · Antes de empezar 3
2 · Cómo funciona 4
3 · La tarjeta Microsoft Entra ID 5
4 · Conectar el directorio 8
5 · Los tres modos 10
6 · Traer el organigrama 13
7 · Grupos → accesos 15
8 · Salidas automáticas (SCIM) 17
9 · Excel, Chrome y escritorio 19
10 · La bitácora de accesos 20
11 · Preguntas frecuentes 22

CAPÍTULO 1

Antes de empezar

PARA QUIÉN ES
Administradores de la organización que conectan el directorio de Microsoft 365 de su empresa a SIAC.

TIEMPO ESTIMADO
10 minutos

PANTALLAS DE
SIAC v1.0.147 · capturadas el 30 de septiembre de 2026

Lo que necesita

- Ser administrador de tu organización en SIAC (entras a **Seguridad** y ves la tarjeta «Microsoft Entra ID»).
- Un administrador global de tu Microsoft 365 disponible cinco minutos, para el consentimiento.
- ¿Prefieres ir directo al grano? La guía paso a paso te lleva en 6 pasos y unos 30 minutos.

Tabla 1. Permisos

Rol	Qué puede hacer aquí
Administrador de la organización	Conectar y desvincular el directorio (con su código de verificación si la organización lo exige), elegir el modo, traer el organigrama, mapear grupos y habilitar SCIM.
Usuario de la organización	Entrar con su cuenta de Microsoft en la web, Office, Chrome y el escritorio. No ve la tarjeta del directorio.

CAPÍTULO 2

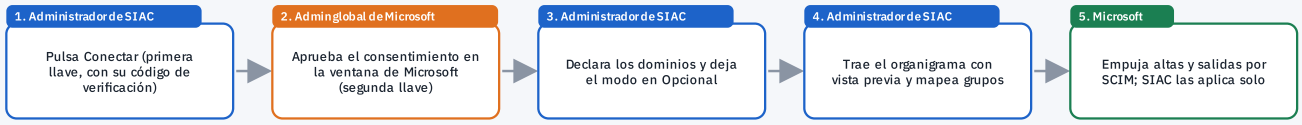
Cómo funciona

El directorio describe; SIAC gobierna

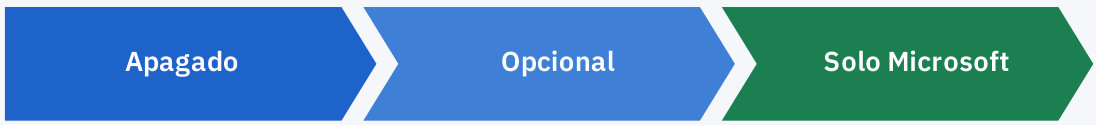
Microsoft prueba quién eres; SIAC decide qué puedes hacer. El directorio aporta quién es cada persona, dónde está (área, cargo, jefe) y si sigue en la empresa. SIAC conserva todo lo demás: roles, límites de consumo, presupuestos, accesos al conocimiento y la auditoría. La sesión que se emite siempre es de SIAC, nunca de Microsoft.

- **Entrar con Microsoft**: tu gente usa su cuenta corporativa, con la MFA que tu empresa ya exige en Microsoft. SIAC nunca ve esa contraseña.
- **Organigrama heredado**: áreas, cargos y jefes llegan del directorio, con vista previa antes de aplicar.
- **Salida en minutos**: quien es deshabilitado en Microsoft sale de SIAC entero: sesiones, Excel, Chrome y escritorio.
- **Lo que NO se hereda**: roles de administración, perfiles de consumo, presupuestos y accesos al conocimiento se deciden en SIAC, no en el directorio.

Entra una vez —y sale una vez— de la web, de Excel, de Chrome y del escritorio.



Quién hace qué para conectar el directorio



Los tres modos de entrada

CAPÍTULO 3

La tarjeta Microsoft Entra ID

Todo el directorio en un solo lugar

DÓNDE ESTÁ
Seguridad › Microsoft Entra ID

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
Administradores de la organización

CUÁNDO USARLA
Para saber si el directorio está conectado, en qué modo y quién entra por él.

La tarjeta vive en **Seguridad**, debajo de los roles. Con el directorio conectado dice **Directorio conectado** con el identificador (tenant) de tu Microsoft y la fecha del consentimiento 1, cuántas personas tienen su identidad enlazada 2 y abre la **Bitácora de accesos** 3. Debajo están el **modo** 4, las **opciones de entrada** 5, los **dominios** 6, la **estructura** del organigrama 7, los **grupos → accesos** 8, el **aprovisionamiento automático (SCIM)** 9 y **Desvincular directorio** 10.

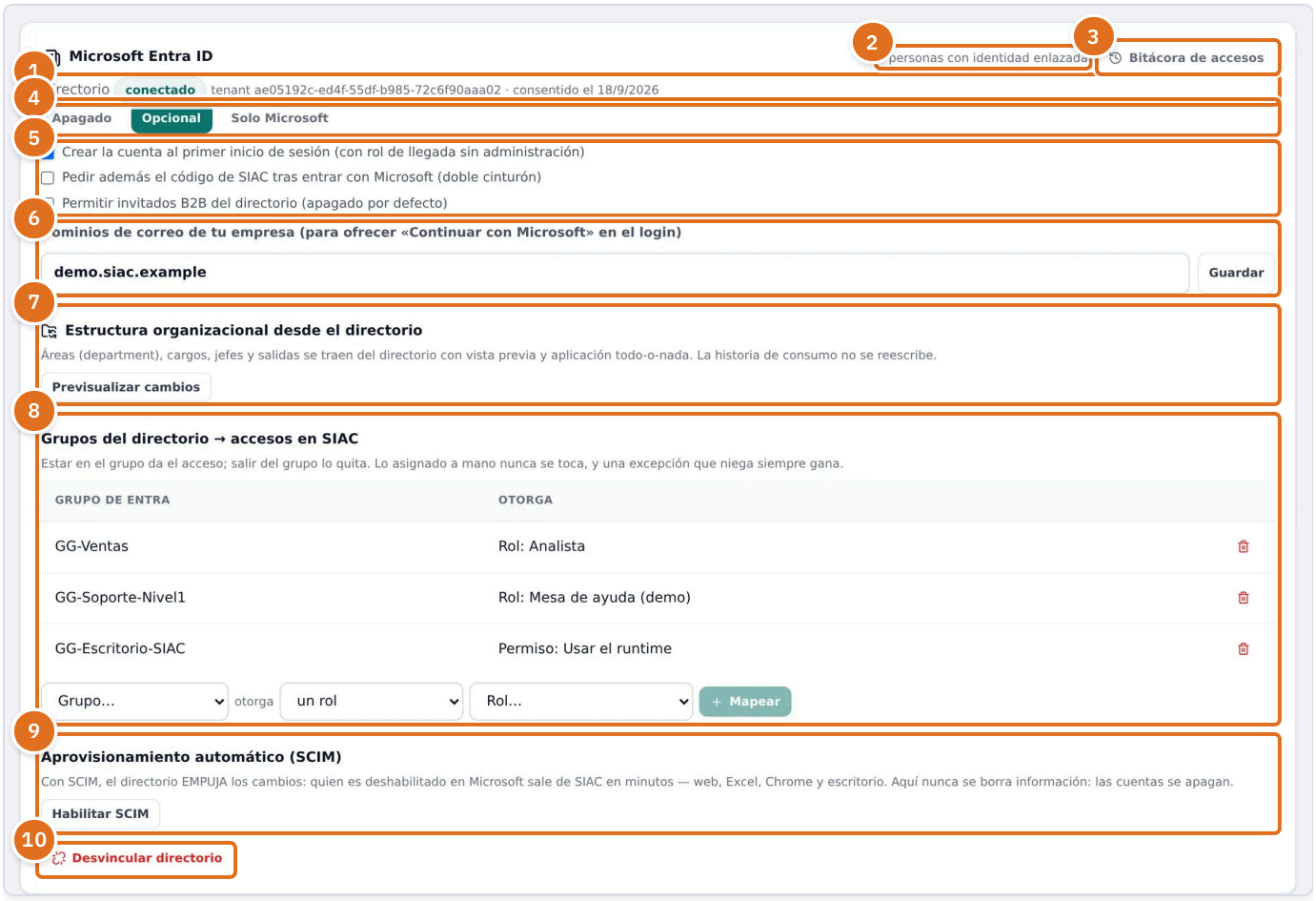


Figura 1. El directorio de Andina Demo, conectado en modo Opcional.

1. **Directorio conectado.** Confirma la vinculación: el identificador (tenant) de tu Microsoft y la fecha en que su administrador global dio el consentimiento.
2. **Personas con identidad enlazada.** Cuántas personas de tu organización ya tienen su cuenta de SIAC unida a su identidad de Microsoft (entraron alguna vez con ella o llegaron por el directorio).
3. **Bitácora de accesos.** Abre cada intento de entrar a tu organización: quién, cuándo, cómo (contraseña, Microsoft, Office, escritorio o SCIM), el resultado y la IP.
4. **Apagado · Opcional · Solo Microsoft.** El modo de entrada: Apagado (vinculado sin usarlo), Opcional (conviven Microsoft y la contraseña) o Solo Microsoft (la contraseña se apaga para la gente del directorio; exige un administrador local de emergencia).
5. **Opciones de entrada.** Crear la cuenta al primer inicio de sesión (con un rol de llegada sin administración), pedir además el código de SIAC tras entrar con Microsoft y permitir invitados B2B (apagado por defecto).
6. **Dominios de correo de tu empresa.** Los dominios que hacen aparecer «Continuar con Microsoft» en el inicio de sesión; escríbelos separados por comas.
7. **Estructura organizacional desde el directorio.** Trae del directorio las áreas, cargos, jefes y salidas, siempre con vista previa y aplicación todo-o-nada.
8. **Grupos del directorio → accesos en SIAC.** Convierte grupos de seguridad de Microsoft en roles o permisos de SIAC: estar en el grupo da el acceso y salir lo quita.
9. **Aprovisionamiento automático (SCIM).** Deja que tu Microsoft empuje altas, cambios y salidas: quien es deshabilitado allá sale de SIAC en minutos.
10. **Desvincular directorio.** Tras confirmar, nadie vuelve a entrar con Microsoft y el modo «Solo Microsoft» se apaga; las cuentas existentes no se tocan.

REGLA DEL SISTEMA

SIAC solo **lee** tu directorio. Jamás escribe, crea ni borra nada en tu Microsoft.

Tabla 2. Qué hace cada elemento de «La tarjeta Microsoft Entra ID» · los usan: Administradores de la organización

Elemento	Qué hace
Directorio conectado	Confirma la vinculación: el identificador (tenant) de tu Microsoft y la fecha en que su administrador global dio el consentimiento.
Personas con identidad enlazada	Cuántas personas de tu organización ya tienen su cuenta de SIAC unida a su identidad de Microsoft (entraron alguna vez con ella o llegaron por el directorio).
Bitácora de accesos	Abre cada intento de entrar a tu organización: quién, cuándo, cómo (contraseña, Microsoft, Office, escritorio o SCIM), el resultado y la IP.
Apagado · Opcional · Solo Microsoft	El modo de entrada: Apagado (vinculado sin usarlo), Opcional (conviven Microsoft y la contraseña) o Solo Microsoft (la contraseña se apaga para la gente del directorio; exige un administrador local de emergencia).
Opciones de entrada	Crear la cuenta al primer inicio de sesión (con un rol de llegada sin administración), pedir además el código de SIAC tras entrar con Microsoft y permitir invitados B2B (apagado por defecto).
Dominios de correo de tu empresa	Los dominios que hacen aparecer «Continuar con Microsoft» en el inicio de sesión; escríbelos separados por comas.
Estructura organizacional desde el directorio	Trae del directorio las áreas, cargos, jefes y salidas, siempre con vista previa y aplicación todo-o-nada.
Grupos del directorio → accesos en SIAC	Convierte grupos de seguridad de Microsoft en roles o permisos de SIAC: estar en el grupo da el acceso y salir lo quita.
Aprovisionamiento automático (SCIM)	Deja que tu Microsoft empuje altas, cambios y salidas: quien es deshabilitado allá sale de SIAC en minutos.
Desvincular directorio	Tras confirmar, nadie vuelve a entrar con Microsoft y el modo «Solo Microsoft» se apaga; las cuentas existentes no se tocan.

CAPÍTULO 4

Conectar el directorio

Dos aprobaciones, ninguna a solas

DÓNDE ESTÁ
Seguridad › Microsoft Entra ID › Conectar Microsoft Entra ID

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
Administradores de la organización

CUÁNDO USARLA
Una sola vez, cuando tu empresa decide que su gente entre con Microsoft.

En la tarjeta 1, pulsa **Conectar Microsoft Entra ID** 2. Se abre una ventana de Microsoft donde un **administrador global** de tu Microsoft 365 aprueba el consentimiento. Hacen falta las dos llaves: un administrador de SIAC inicia (con su código de verificación) y un administrador global de Microsoft consiente.

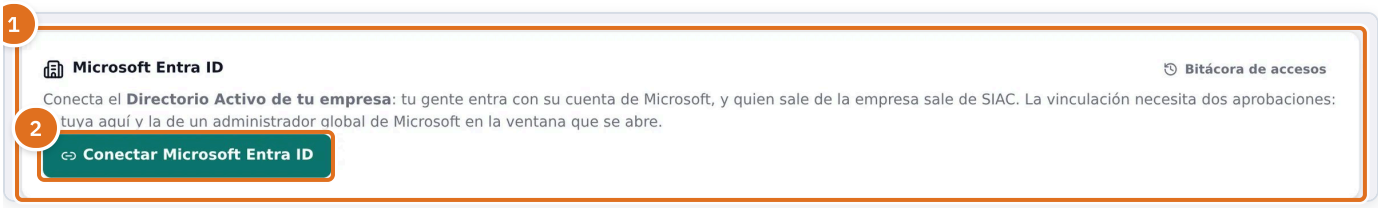


Figura 2. La tarjeta antes de conectar.

1. **Microsoft Entra ID.** Conecta el directorio de Microsoft de tu empresa para que la gente entre con su cuenta corporativa; muestra el estado, las opciones y la bitácora de accesos.
2. **Conectar Microsoft Entra ID.** Abre la ventana de Microsoft donde un administrador global aprueba la vinculación del directorio.

SI SIAC NO LO DEJA AVANZAR

Un directorio solo puede vincularse a **una** empresa en SIAC. Si al consentir aparece «ya está vinculado a otra empresa», contacta a soporte.

CUÁNDO USARLO

Si la tarjeta dice «la integración con Microsoft aún no está configurada en este servidor», pídele a tu asesor de SIAC que la active.

Tabla 3. Qué hace cada elemento de «Conectar el directorio» · los usan: Administradores de la organización

Elemento	Qué hace
Microsoft Entra ID	Conecta el directorio de Microsoft de tu empresa para que la gente entre con su cuenta corporativa; muestra el estado, las opciones y la bitácora de accesos.
Conectar Microsoft Entra ID	Abre la ventana de Microsoft donde un administrador global aprueba la vinculación del directorio.

CAPÍTULO 5

Los tres modos

De convivencia a «solo Microsoft»

DÓNDE ESTÁ
Seguridad › Microsoft Entra ID

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
Administradores de la organización

CUÁNDO USARLA
Al conectar (Opcional) y, cuando todo funcione, si quieres apagar la contraseña (Solo Microsoft).

El modo 1 decide cómo entra tu gente:

- **Apagado**: vinculado pero sin iniciar sesión con Microsoft (útil para preparar).
- **Opcional** (recomendado al empezar): conviven «Continuar con Microsoft» y la contraseña de siempre.
- **Solo Microsoft**: la contraseña se apaga para la gente del directorio. SIAC exige que quede al menos un **administrador local de emergencia** (con contraseña y sin identidad de Entra): es la puerta si el directorio falla. Sin ella, este modo no se puede activar.

Las opciones 2 completan el modo: **crear la cuenta al primer inicio de sesión** (alguien nuevo del directorio entra y su cuenta nace sola, con un rol de llegada que nunca es de administración), **pedir además el código de SIAC** tras entrar con Microsoft (doble cinturón) y **permitir invitados B2B** (apagado por defecto). Los **dominios** 3 son los que hacen aparecer «Continuar con Microsoft» en el inicio de sesión; **Guardar** 4 los fija.

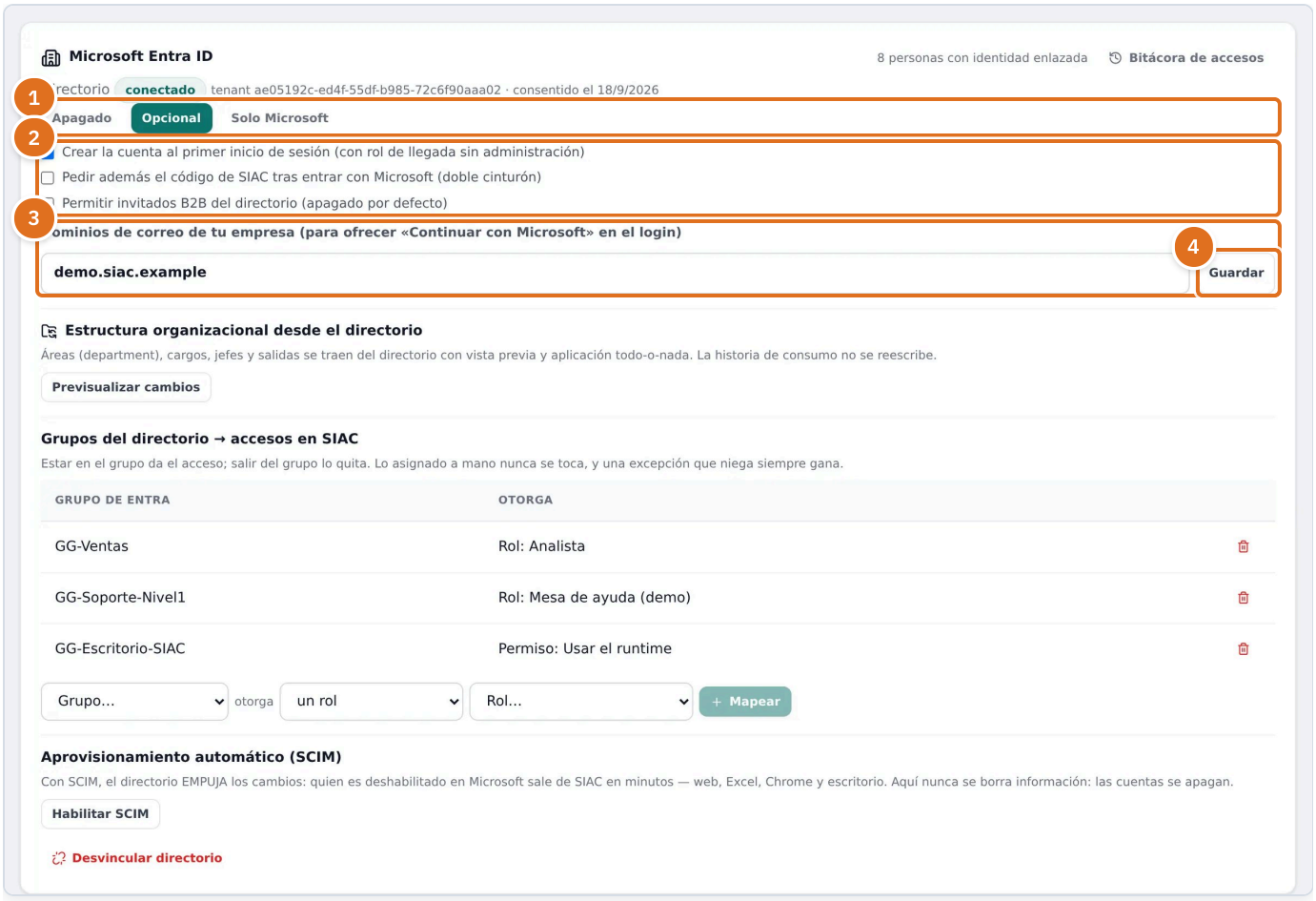


Figura 3. Modo Opcional, cuentas al primer inicio de sesión y el dominio de la empresa.

1. **Apagado · Opcional · Solo Microsoft.** El modo de entrada: Apagado (vinculado sin usarlo), Opcional (conviven Microsoft y la contraseña) o Solo Microsoft (la contraseña se apaga para la gente del directorio; exige un administrador local de emergencia).
2. **Opciones de entrada.** Crear la cuenta al primer inicio de sesión (con un rol de llegada sin administración), pedir además el código de SIAC tras entrar con Microsoft y permitir invitados B2B (apagado por defecto).
3. **Dominios de correo de tu empresa.** Los dominios que hacen aparecer «Continuar con Microsoft» en el inicio de sesión; escríbelos separados por comas.
4. **Guardar.** Guarda los dominios de correo escritos al lado.

REGLA DEL SISTEMA

En modo **Solo Microsoft**, si no queda ningún administrador local de emergencia, la tarjeta lo dice en rojo: «No queda ningún administrador local de emergencia... Crea uno: es la puerta si el directorio falla».

Tabla 4. Qué hace cada elemento de «Los tres modos» · los usan: Administradores de la organización

Elemento	Qué hace
Apagado · Opcional · Solo Microsoft	El modo de entrada: Apagado (vinculado sin usarlo), Opcional (conviven Microsoft y la contraseña) o Solo Microsoft (la contraseña se apaga para la gente del directorio; exige un administrador local de emergencia).
Opciones de entrada	Crear la cuenta al primer inicio de sesión (con un rol de llegada sin administración), pedir además el código de SIAC tras entrar con Microsoft y permitir invitados B2B (apagado por defecto).
Dominios de correo de tu empresa	Los dominios que hacen aparecer «Continuar con Microsoft» en el inicio de sesión; escríbelos separados por comas.
Guardar	Guarda los dominios de correo escritos al lado.

CAPÍTULO 6

Traer el organigrama

Vista previa siempre; nunca un sync silencioso

DÓNDE ESTÁ
Seguridad › Microsoft Entra ID › Estructura organizacional

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
Administradores de la organización

CUÁNDO USARLA
Después de conectar, y cada vez que en tu empresa cambien áreas, cargos o personas.

Previsualizar cambios 1 muestra el diff completo 2: áreas nuevas, personas por mover, cargos, salidas y regresos, y cuántas personas del directorio aún no tienen cuenta en SIAC. **Aplicar** 3 lo ejecuta **todo o nada**.



Figura 4. La vista previa: dos áreas nuevas, tres movimientos, cuatro cargos y una salida.

1. **Previsualizar cambios.** Pide al directorio el diff completo (áreas nuevas, movimientos, cargos, salidas y regresos) sin tocar nada.
2. **El diff haría.** El resumen de la vista previa: unidades nuevas, movimientos, cargos, salidas (en rojo si las hay), regresos y personas del directorio sin cuenta en SIAC.
3. **Aplicar.** Aplica el diff de la vista previa, todo o nada; si quedó bloqueado por el tope de cordura, solo se habilita al marcar la casilla de forzar.

PASO A PASO

1. Si el diff desactivaría a demasiada gente (más del **20 %** de las personas enlazadas, por defecto), queda **bloqueado** esperando tu decisión explícita: un error de alcance en Entra se ve en la vista previa, no en producción.

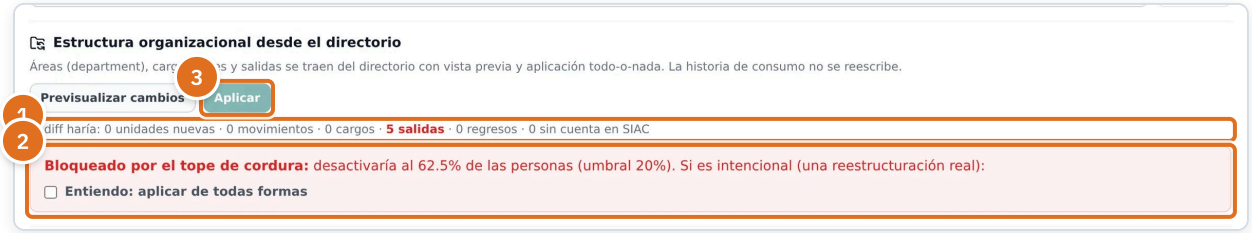


Figura 5. Un diff bloqueado por el tope de cordura.

1. **El diff haría.** El resumen de la vista previa: unidades nuevas, movimientos, cargos, salidas (en rojo si las hay), regresos y personas del directorio sin cuenta en SIAC.
2. **Bloqueado por el tope de cordura.** El diff desactivaría a más personas que el umbral (20 % por defecto); solo se aplica si marcas «Entiendo: aplicar de todas formas».
3. **Aplicar.** Aplica el diff de la vista previa, todo o nada; si quedó bloqueado por el tope de cordura, solo se habilita al marcar la casilla de forzar.

REGLA DEL SISTEMA

La historia no se reescribe: el consumo pasado queda contabilizado en el área donde ocurrió, aunque la persona cambie de área hoy.

Tabla 5. Qué hace cada elemento de «Traer el organigrama» · los usan: Administradores de la organización

Elemento	Qué hace
Previsualizar cambios	Pide al directorio el diff completo (áreas nuevas, movimientos, cargos, salidas y regresos) sin tocar nada.
El diff haría	El resumen de la vista previa: unidades nuevas, movimientos, cargos, salidas (en rojo si las hay), regresos y personas del directorio sin cuenta en SIAC.
Aplicar	Aplica el diff de la vista previa, todo o nada; si quedó bloqueado por el tope de cordura, solo se habilita al marcar la casilla de forzar.
Bloqueado por el tope de cordura	El diff desactivaría a más personas que el umbral (20 % por defecto); solo se aplica si marcas «Entiendo: aplicar de todas formas».

CAPÍTULO 7

Grupos → accesos

Estar en el grupo da el acceso; salir lo quita

DÓNDE ESTÁ
Seguridad › Microsoft Entra ID › Grupos del directorio

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
Administradores de la organización

CUÁNDO USARLA
Si tu empresa ya organiza permisos con grupos de seguridad de Microsoft.

Mapea un **grupo de seguridad** de tu directorio a un **rol** o a un **permiso** de SIAC. La tabla 1 muestra los mapeos vigentes; para uno nuevo eliges el grupo 2, qué otorga y cuál 3, y pulsas **Mapear** 4. En cada inicio de sesión, SIAC ajusta los accesos según los grupos actuales de la persona.

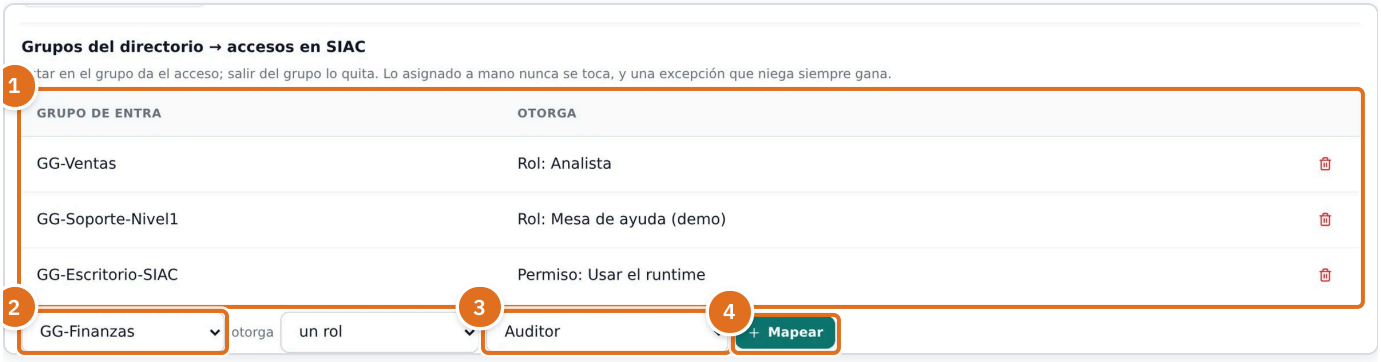


Figura 6. Tres mapeos vigentes y uno nuevo: GG-Finanzas → Auditor.

1. **Grupo de Entra · Otorga.** Los mapeos vigentes: qué grupo da qué rol o permiso; la papelera borra el mapeo y lo que vino por él se retira en el próximo inicio de sesión.
2. **Grupo…** El grupo de seguridad de tu Microsoft que dará el acceso; la lista sale del directorio.
3. **Rol…** El rol de SIAC que recibirá quien esté en ese grupo (o el permiso puntual, si elegiste «un permiso puntual»).
4. **Mapear.** Crea el mapeo; solo puedes mapear hacia accesos que tú mismo posees.

REGLA DEL SISTEMA

Tres garantías: lo asignado a mano **nunca** lo toca el sync; una excepción que **niega** siempre gana; y solo puedes mapear hacia accesos que **tú mismo posees**. Si los accesos de alguien se reducen, sus sesiones se renuevan al instante.

Tabla 6. Qué hace cada elemento de «Grupos → accesos» · los usan: Administradores de la organización

Elemento	Qué hace
Grupo de Entra · Otorga	Los mapeos vigentes: qué grupo da qué rol o permiso; la papelera borra el mapeo y lo que vino por él se retira en el próximo inicio de sesión.
Grupo…	El grupo de seguridad de tu Microsoft que dará el acceso; la lista sale del directorio.
Rol…	El rol de SIAC que recibirá quien esté en ese grupo (o el permiso puntual, si elegiste «un permiso puntual»).
Mapear	Crea el mapeo; solo puedes mapear hacia accesos que tú mismo posees.

CAPÍTULO 8

Salidas automáticas (SCIM)

El directorio empuja los cambios

DÓNDE ESTÁ
Seguridad › Microsoft Entra ID › Aprovisionamiento automático

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
Administradores de la organización

CUÁNDO USARLA
Cuando quieres que las salidas de la empresa lleguen solas a SIAC, sin esperar a que nadie entre.

Habilitar SCIM 1 genera el endpoint y el token 2 —el token se muestra **una sola vez**— que copias en Entra › Aprovisionamiento. Desde ahí, deshabilitar a alguien en Microsoft lo saca de SIAC en minutos: cuenta apagada, sesiones cerradas y equipos de escritorio revocados.

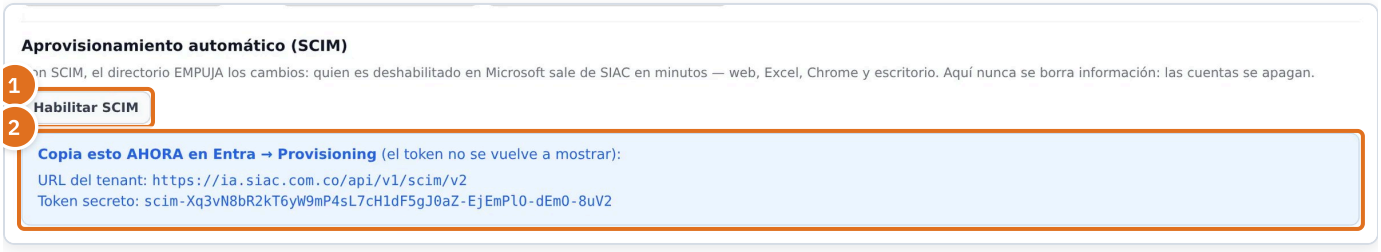


Figura 7. La credencial de SCIM recién generada.

1. **Habilitar SCIM.** Genera la URL y el token secreto para Entra → Aprovisionamiento; si ya está habilitado dice «Rotar credencial» y el token anterior deja de servir.
2. **Copia esto AHORA en Entra → Provisioning.** La URL del tenant y el token secreto: el token se muestra una sola vez, así que cópialo ya.

REGLA DEL SISTEMA

En SIAC nunca se borra información: las cuentas se **apagan** y su historial queda.

CONSEJO

Si pierdes el token, el mismo botón dice **Rotar credencial**: genera uno nuevo y el anterior deja de servir al instante.

Tabla 7. Qué hace cada elemento de «Salidas automáticas (SCIM)» · los usan: Administradores de la organización

Elemento	Qué hace
Habilitar SCIM	Genera la URL y el token secreto para Entra → Aprovisionamiento; si ya está habilitado dice «Rotar credencial» y el token anterior deja de servir.
Copia esto AHORA en Entra → Provisioning	La URL del tenant y el token secreto: el token se muestra una sola vez, así que cópialo ya.

CAPÍTULO 9

Excel, Chrome y escritorio

Cero login donde más se trabaja

- **Complementos de Office**: con el directorio conectado, abrir Excel, Word, PowerPoint u Outlook es entrar: el complemento reconoce tu sesión de Microsoft sin teclear nada.
- **Extensión de Chrome y app de escritorio**: «Continuar con Microsoft» abre tu navegador (con tu sesión corporativa ya iniciada) y vuelve solo.
- En todos los casos, **la sesión que se emite es de SIAC**: Microsoft prueba quién eres; SIAC decide qué puedes hacer.

CAPÍTULO 10

La bitácora de accesos

Cada intento, con su método y su motivo

DÓNDE ESTÁ
Seguridad › Microsoft Entra ID › Bitácora de accesos

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
Administradores de la organización

CUÁNDO USARLA
Para auditar quién entra, por dónde, y por qué se rechazó un intento.

La bitácora 1 muestra cada intento de entrar a tu organización: cuándo, quién, **cómo** (contraseña, Microsoft, Office o escritorio), el **resultado** —«entró» o «rechazado» con su motivo— y la IP. Los frenados por el freno de fuerza bruta aparecen como «bloqueado».

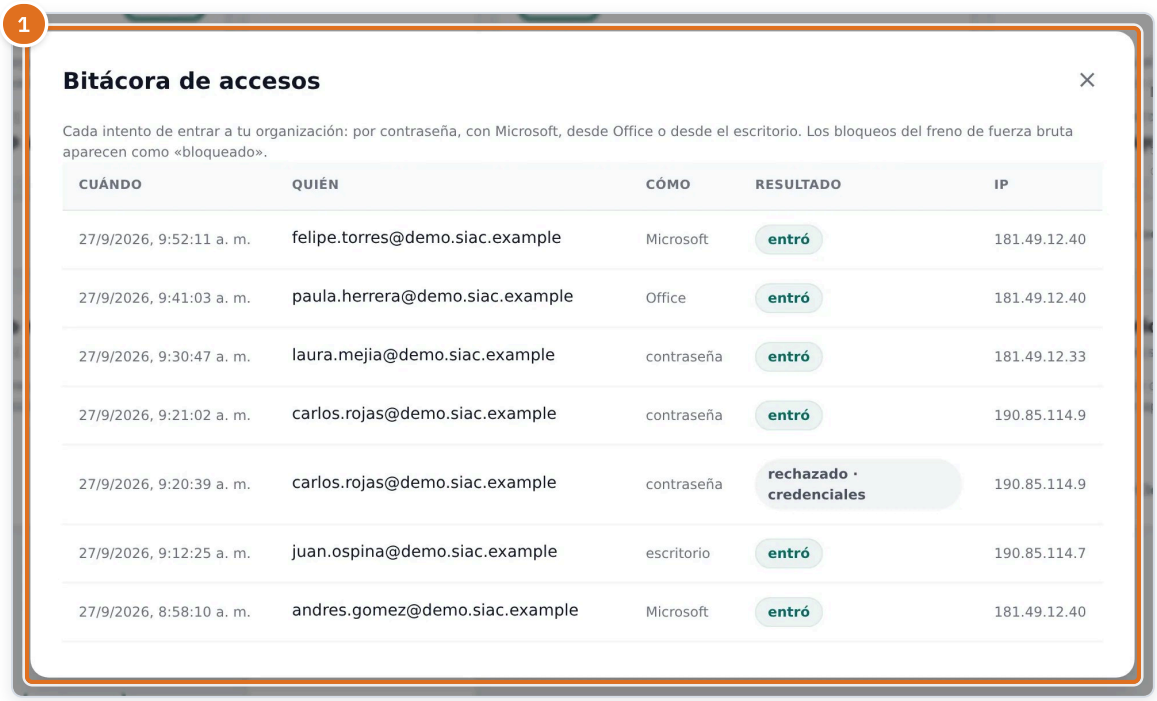


Figura 8. La bitácora de accesos, con entradas por Microsoft, Office, escritorio y contraseña.

1 **Bitácora de accesos.** La tabla de intentos de acceso; los rechazados dicen el motivo y los frenados por fuerza bruta aparecen como «bloqueado».

Tabla 8. Qué hace cada elemento de «La bitácora de accesos» · los usan: Administradores de la organización

Elemento	Qué hace
Bitácora de accesos	La tabla de intentos de acceso; los rechazados dicen el motivo y los frenados por fuerza bruta aparecen como «bloqueado».

CAPÍTULO 11

Preguntas frecuentes

¿SIAC guarda contraseñas de Microsoft?

No. Nunca las ve: la autenticación ocurre en Microsoft y a SIAC llega solo una prueba de identidad firmada, que se valida y se descarta.

¿Un token de otro directorio sirve?

No. Cada empresa acepta únicamente tokens de SU directorio vinculado; cualquier otro se rechaza y queda en la bitácora (motivo «tid_ajeno»).

¿Y si Entra se cae?

En modo Opcional, la contraseña sigue. En modo Solo Microsoft, el administrador local de emergencia entra con contraseña y baja el modo.

¿Quién vigila los intentos?

La **Bitácora de accesos** (en la misma tarjeta) muestra cada intento: método, resultado y motivo. El freno de fuerza bruta bloquea y avisa al titular.

¿Los invitados externos (B2B) entran?

No, salvo que lo actives explícitamente en las opciones de la tarjeta.

¿Qué pasa si desvinculo el directorio?

Nadie vuelve a entrar con Microsoft y el modo «Solo Microsoft» se apaga. Las cuentas existentes no se tocan.