MANUAL DEL USUARIO · CENTRO DE AYUDA DE SIAC

Conecta tu Directorio Activo en 6 pasos

Del clic en Conectar a que tu gente entre a SIAC con su cuenta de Microsoft, y quien salga de la empresa salga solo. Cada paso dice quién lo hace, cuánto tarda, cómo se ve en pantalla y cómo verificar que quedó bien. Media hora, una sola vez — y queda para siempre.

Dirigido a	Plataforma	Tiempo	Pantallas capturadas
Administradores · 2 personas	**SIAC v1.0.147**	**30 minutos**	**30 de septiembre de 2026**

Contenido

1 · Antes de empezar 3
2 · Cómo funciona 4
3 · El porqué 5
4 · El paraqué 6
5 · 1 · Conecta el directorio (las dos llaves) 7
6 · 2 · Declara tus dominios y deja el modo en «Opcional» 9
7 · 3 · Pruébalo tú mismo: «Continuar con Microsoft» 11
8 · 4 · Trae el organigrama — con vista previa, siempre 13
9 · 5 · Mapea grupos → accesos (opcional, recomendado) 15
10 · 6 · Activa las salidas automáticas (SCIM) 17
11 · El modo «Solo Microsoft» — y su puerta de emergencia 19
12 · Checklist final 21
13 · Preguntas frecuentes 22

CAPÍTULO 1

Antes de empezar

PARA QUIÉN ES
El administrador de SIAC de tu organización, con el administrador global de tu Microsoft 365 a mano.

TIEMPO ESTIMADO
30 minutos

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

Lo que necesita

- **Tú** necesitas ser administrador de tu empresa en SIAC (entras a **Seguridad** y ves la tarjeta «Microsoft Entra ID»). Si tu organización usa código de verificación, ten tu WhatsApp o correo a mano.
- Necesitas a un **administrador global de tu Microsoft 365** disponible 5 minutos (suele ser quien administra los correos de la empresa). Si eres la misma persona, mejor todavía.
- Nada más. SIAC nunca pide contraseñas de Microsoft ni escribe en tu directorio: todo lo que sigue es de lectura y con tu aprobación explícita.
- ¿Primero el concepto? Lee el manual del Directorio Activo.

Tabla 1. Permisos

Rol	Qué puede hacer aquí
Administrador de la organización	«👤 Tú, en SIAC»: ejecuta los pasos 1 a 6 en la tarjeta Microsoft Entra ID.

Cada paso de esta guía lleva una etiqueta de quién lo ejecuta. Son tres actores, y solo tres: 👤 **Tú, en SIAC**, 🏢 **Admin global de tu Microsoft** y ⚙️ **Automático**.

¿La tarjeta dice «la integración con Microsoft aún no está configurada en este servidor»? Ese es el único caso en que el primer movimiento no es tuyo: pídele a tu asesor de SIAC que active la integración con Microsoft y vuelve a esta guía.

CAPÍTULO 2

Cómo funciona

Los 6 pasos

1. **Conectar el directorio** — 5 min.
2. **Dominios y modo** — 3 min.
3. **Probar la entrada** — 2 min.
4. **Traer el organigrama** — 5 min.
5. **Grupos → accesos** — 5 min.
6. **Salidas automáticas** — 10 min.

Unos 30 minutos en total, dos personas y sin tocar tu Microsoft.



Quién hace cada paso

CAPÍTULO 3

El porqué

La misma historia, con dos finales

Ana, de Comercial, sale de la empresa un viernes. Mira qué pasa con su acceso a la IA de tu organización en cada escenario: esta es la razón entera de esta guía.

😵 **Sin el directorio conectado** — cada sistema es una isla; el offboarding depende de que alguien se acuerde:

1. 📋 RR. HH. deshabilita a Ana en Microsoft. *Viernes 5:00 p. m.*
2. 📧 Alguien debería avisar al admin de SIAC… El correo se envía el lunes. O no se envía.
3. 🔓 La cuenta de Ana en SIAC sigue viva: chat, documentos, conocimiento de la empresa. Y su sesión de Excel y del escritorio siguen abiertas.

Resultado: días (o semanas) con un acceso que ya no debería existir.

😌 **Con el directorio conectado** — un solo lugar manda: tu Microsoft. SIAC obedece solo:

1. 📋 RR. HH. deshabilita a Ana en Microsoft. *Viernes 5:00 p. m.* — lo mismo de siempre, nada nuevo que recordar.
2. ⚡ Microsoft se lo empuja a SIAC (paso 6 de esta guía). Automático.
3. 🔒 Cuenta apagada, sesiones cerradas, Excel y escritorio revocados. Y queda en la bitácora. *Viernes 5:0x p. m.* — minutos.

Entra una vez, y sale una vez. Sin depender de la memoria de nadie. Y el mismo beneficio al revés: quien entra a la empresa entra a SIAC con la cuenta que RR. HH. ya le creó — sin invitaciones, sin otra contraseña que olvidar, con la MFA que tu empresa ya exige en Microsoft.

CAPÍTULO 4

El paraqué

Qué decide Microsoft y qué sigue decidiendo SIAC

Conectar el directorio **no le entrega el control de tu IA a Microsoft**. El reparto es este, y es la clave para leer todos los pasos que siguen:

- **Tu Microsoft** (Entra ID · el Directorio Activo) decide **QUIÉN** es cada persona, **DÓNDE** está (área, cargo, jefe) y **SI** sigue en la empresa — más su contraseña y su MFA, que SIAC nunca ve. Le envía a SIAC una **prueba de identidad**.
- **SIAC** (gobierna y emite la sesión) decide **QUÉ** puede hacer con la IA, **CUÁNTO** puede gastar y **QUÉ** conocimiento ve: roles, límites y auditoría.
- **La sesión SIEMPRE la emite SIAC — nunca Microsoft**, en las cuatro superficies: 🌐 panel web, 📊 Excel · Word · Outlook, 🧭 extensión de Chrome y 💻 SIAC Desktop.

Microsoft prueba quién eres; SIAC decide qué puedes hacer. Por eso conectar el directorio no cambia roles, límites ni permisos: solo cambia la puerta de entrada — en las cuatro superficies a la vez.

- 🔑 **Entrar una vez**: una sola cuenta —la de Microsoft— abre el panel, Excel, Chrome y el escritorio. Sin otra contraseña que crear, olvidar o phishear.
- 🌳 **Organigrama vivo**: áreas, cargos y jefes se traen del directorio con vista previa. El consumo de IA se reporta por área, solo.
- 🚪 **Salir una vez**: deshabilitar en Microsoft = salir de SIAC en minutos. El offboarding deja de ser una lista de sistemas.
- 👁️ **Verlo todo**: cada intento de entrada —por contraseña, Microsoft, Office o escritorio— queda en la Bitácora de accesos.

CAPÍTULO 5

1 · Conecta el directorio (las dos llaves)

👤 Tú, en SIAC · 🏢 Admin de Microsoft · ⏱ 5 min

DÓNDE ESTÁ
Seguridad › Microsoft Entra ID

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
👤 Tú (administrador de SIAC) y 🏢 el administrador global de tu Microsoft.

CUÁNDO USARLA
Una sola vez, al empezar.

La conexión exige **dos aprobaciones distintas** — así ni un admin de SIAC a solas, ni uno de Microsoft a solas, pueden vincular nada. Así se ve la tarjeta 1 antes de conectar, con el botón **Conectar Microsoft Entra ID** 2.

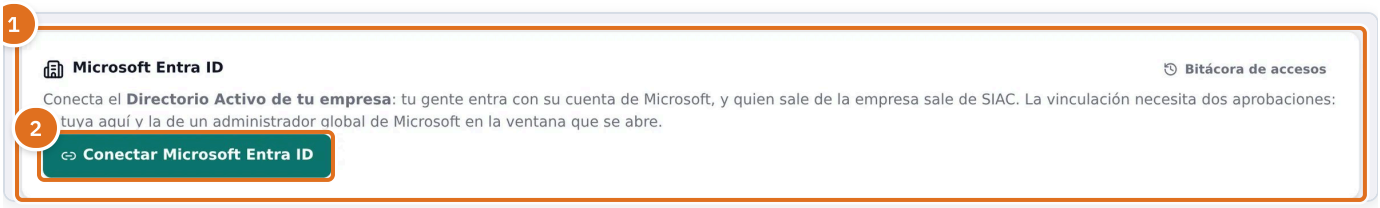

Figura 1. La tarjeta antes de conectar. Tras el consentimiento muestra «conectado» y tu tenant.

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.

PASO A PASO

1. 👤 **Tú.** Entra a Seguridad y baja hasta la tarjeta **Microsoft Entra ID** 1.
2. 👤 **Tú.** Pulsa **Conectar Microsoft Entra ID** 2 — primera llave: la tuya, con tu código de verificación si aplica.
3. 🏢 **Admin de Microsoft.** Se abre una ventana de Microsoft pidiendo consentimiento de administrador: ahí entra tu admin global de Microsoft con SU cuenta y pulsa **Aceptar** — segunda llave. La pantalla lista exactamente qué se autoriza: iniciar sesión y leer usuarios y grupos.
4. **Quedó bien si:** la tarjeta cambia a **Directorio conectado** con el identificador de tu tenant de Microsoft y la fecha del consentimiento 1.

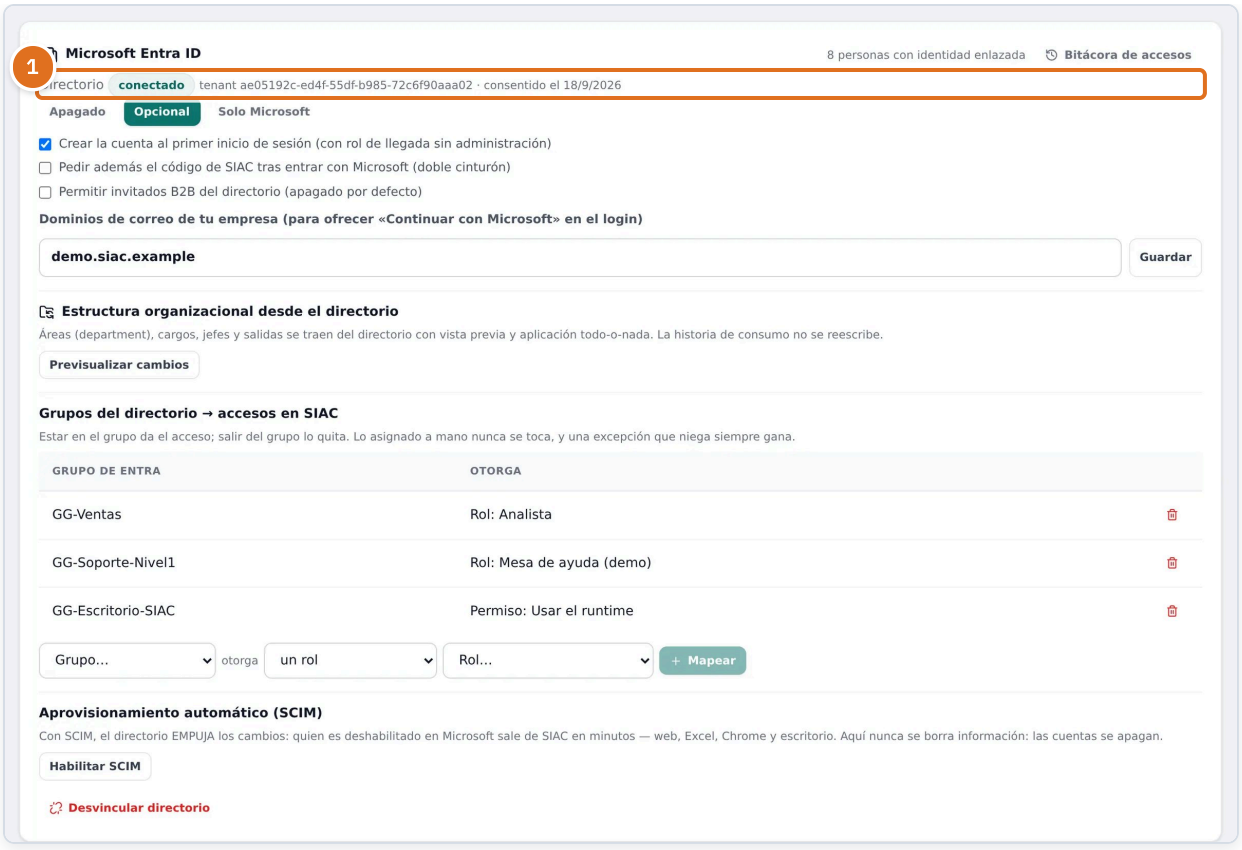

Figura 2. Directorio conectado: el tenant y la fecha del consentimiento.

1 **Directorio conectado.** Confirma la vinculación: el identificador (tenant) de tu Microsoft y la fecha en que su administrador global dio el consentimiento.

SI SIAC NO LO DEJA AVANZAR

Si al consentir aparece «Ese directorio de Microsoft ya está vinculado a otra empresa», contacta a soporte: un directorio solo puede vincularse a una empresa en SIAC.

Tabla 2. Qué hace cada elemento de «1 · Conecta el directorio (las dos llaves)» · 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.
Directorio conectado	Confirma la vinculación: el identificador (tenant) de tu Microsoft y la fecha en que su administrador global dio el consentimiento.

CAPÍTULO 6

2 · Declara tus dominios y deja el modo en «Opcional»

👤 Tú, en SIAC · ⏱ 3 min

DÓNDE ESTÁ	DIRECCIÓN
Seguridad › Microsoft Entra ID	/seguridad
QUIÉN LA USA	**CUÁNDO USARLA**
👤 Tú.	Justo después de conectar.

En la misma tarjeta está el modo 1, las opciones de entrada 2 y los dominios de correo de tu empresa 3, que se guardan con **Guardar** 4. Tres modos: **Apagado**, **Opcional** y **Solo Microsoft**. «Solo Microsoft» es para después (última sección) — no hoy.

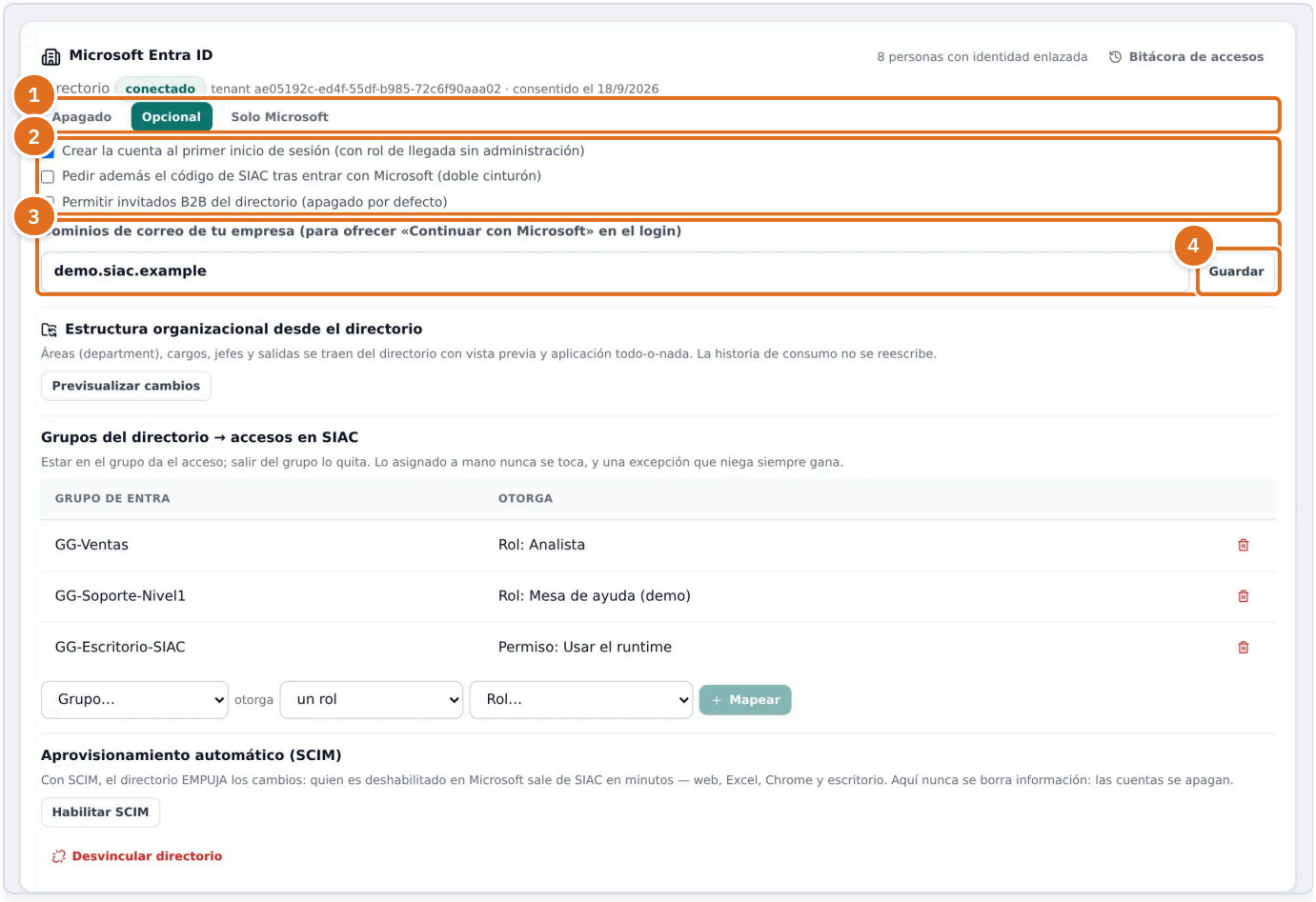

Figura 3. Modo Opcional, cuenta al primer inicio de sesión y el dominio guardado.

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.

PASO A PASO

1. Escribe los dominios de correo de tu empresa 3 —por ejemplo `tuempresa.com, filial.com`— y pulsa **Guardar** 4. Son los que harán aparecer el botón «Continuar con Microsoft» en el inicio de sesión.
2. Verifica que el modo 1 esté en **Opcional**: conviven la contraseña de siempre y Microsoft. Es el modo correcto para empezar — nadie queda fuera mientras pruebas.
3. Deja activo **Crear la cuenta al primer inicio de sesión** 2: alguien nuevo del directorio entra y su cuenta nace sola, con un rol de llegada básico que nunca es de administración. Tú decides después si le das más.
4. **Quedó bien si:** la tarjeta muestra tus dominios guardados y el modo en **Opcional**.

Tabla 3. Qué hace cada elemento de «2 · Declara tus dominios y deja el modo en «Opcional»» · 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 7

3 · Pruébalo tú mismo: «Continuar con Microsoft»

👤 Tú, en SIAC · ⏱ 2 min

DÓNDE ESTÁ	DIRECCIÓN
Seguridad › Microsoft Entra ID › Bitácora de accesos	/seguridad
QUIÉN LA USA	**CUÁNDO USARLA**
👤 Tú.	En cuanto guardes los dominios.

Pruébalo con tu propia cuenta antes de anunciarlo a nadie. El botón «Continuar con Microsoft» aparece en el inicio de sesión **solo** cuando el dominio del correo tiene el directorio conectado. Después, confírmalo en la **Bitácora de accesos** 1.

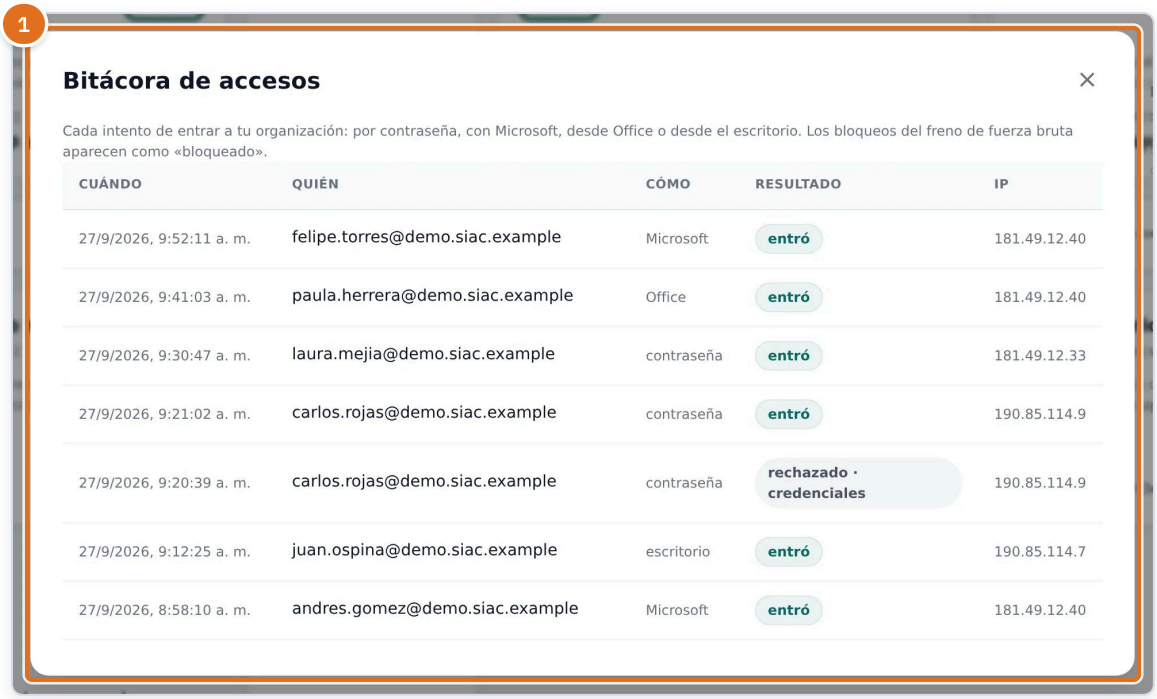

Figura 4. La bitácora: entradas por Microsoft, Office, escritorio y contraseña, y un intento rechazado.

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

PASO A PASO

1. Abre una ventana de incógnito en `ia.siac.com.co/login` y escribe tu correo corporativo (por ejemplo `ana@tuempresa.com`): al reconocer tu dominio aparece el botón **Continuar con Microsoft**.

2. Púlsalo: el viaje ocurre en una ventana de Microsoft (con la MFA de tu empresa) y vuelve solo al panel, ya adentro.
3. Desde este momento, en Excel, Word, PowerPoint y Outlook los complementos reconocen la sesión de Microsoft del equipo y entran sin teclear nada; en la extensión de Chrome y en SIAC Desktop, el mismo botón abre el navegador y vuelve solo.
4. **Quedó bien si:** entraste sin escribir contraseña de SIAC — y tu intento aparece en la **Bitácora de accesos** 1 de la tarjeta como **Microsoft · entró**.

Tabla 4. Qué hace cada elemento de «3 · Pruébalo tú mismo: «Continuar con Microsoft»» · 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 8

4 · Trae el organigrama — con vista previa, siempre

👤 Tú, en SIAC · ⏱ 5 min

DÓNDE ESTÁ
Seguridad › Microsoft Entra ID › Estructura organizacional

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
👤 Tú.

CUÁNDO USARLA
Cuando la entrada funciona; y después, cada vez que tu empresa cambie.

Tu directorio ya sabe el **área** (department), el **cargo** y el **jefe** de cada persona. SIAC los usa para reportar el consumo de IA por área y avisar a quien corresponde. **Previsualizar cambios** 1 trae el resumen 2 y **Aplicar** 3 lo ejecuta. Primero el diff completo; aplicar es todo-o-nada. Un sync silencioso no existe aquí.



Figura 5. La vista previa del sync, antes de aplicar.

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. En la tarjeta, sección **Estructura organizacional desde el directorio**, pulsa **Previsualizar cambios** 1.
2. Lee el resumen 2: áreas nuevas, personas por mover, cargos, salidas y regresos. Nada se ha tocado todavía.
3. Si cuadra con tu realidad, pulsa **Aplicar** 3. Todo entra junto, o nada.
4. 🛡️ **El tope de cordura te cuida:** si la vista previa desactivaría a más del **20 %** de tu gente (típico de un filtro mal hecho en Microsoft), el diff llega **bloqueado** y no se aplica — salvo que tú marques la casilla **Entiendo: aplicar de todas formas**, a conciencia.

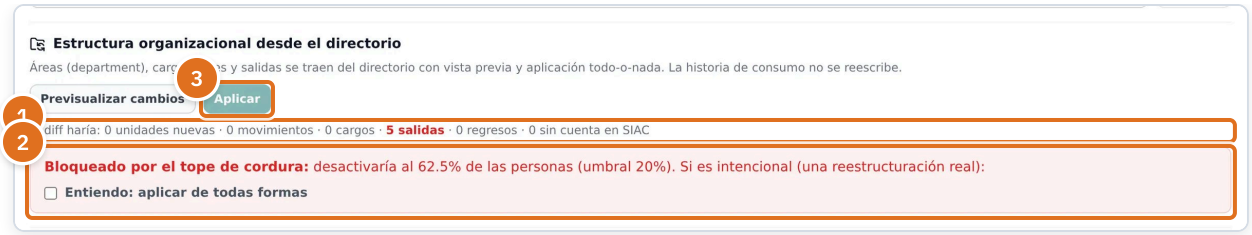

Figura 6. Un diff bloqueado: desactivaría al 62,5 % de las personas.

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.

5 **Quedó bien si:** en Gobernanza ves el árbol con tus áreas reales y cada persona en la suya.

REGLA DEL SISTEMA

La historia no se reescribe: el consumo pasado queda contado en el área donde ocurrió.

Tabla 5. Qué hace cada elemento de «4 · Trae el organigrama — con vista previa, siempre» · 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 9

5 · Mapea grupos → accesos (opcional, recomendado)

👤 Tú, en SIAC · ⏱ 5 min

DÓNDE ESTÁ
Seguridad › Microsoft Entra ID › Grupos del directorio

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
👤 Tú.

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

Si tu empresa ya organiza permisos con grupos de seguridad de Microsoft (por ejemplo **GG-Ventas**), puedes convertirlos en accesos de SIAC: **estar en el grupo da el acceso; salir del grupo lo quita** — en el siguiente inicio de sesión. La tabla 1 muestra los mapeos; eliges el grupo 2 y el rol 3 y pulsas **Mapear** 4.

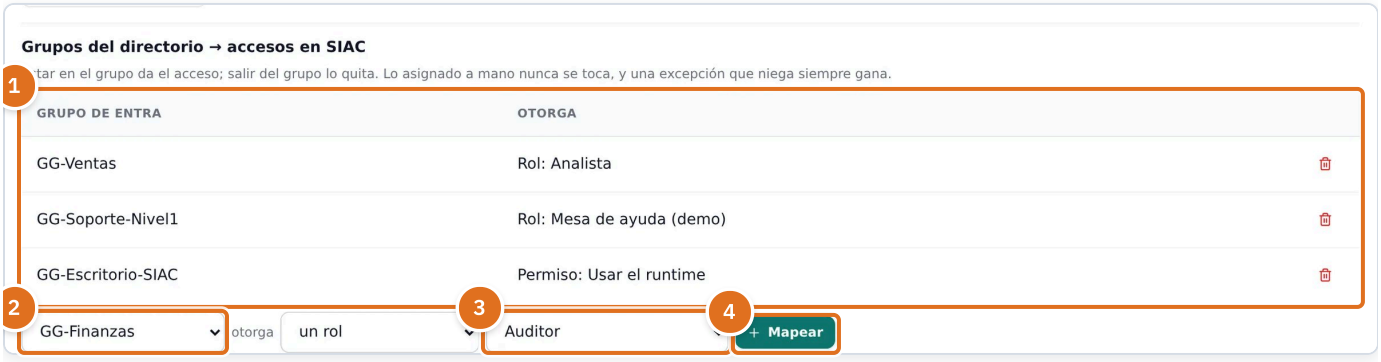

Figura 7. GG-Ventas → Rol: Analista, y un mapeo nuevo a punto de crearse.

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.

PASO A PASO

1. En la sección **Grupos del directorio → accesos en SIAC**, elige el grupo 2, qué otorga (**un rol** o **un permiso puntual**) y cuál 3, y pulsa **Mapear** 4.
2. **Quedó bien si:** en la tabla de mapeos 1 aparece la fila «GG-Ventas → Rol: Analista» — y quien entre estando en ese grupo lo recibe solo.

REGLA DEL SISTEMA

Tres garantías: ✋ lo que asignaste a mano **nunca** lo toca el sync; ⛔ una excepción que niega (un «negar» del admin) **siempre gana** sobre cualquier grupo; y solo puedes mapear hacia accesos que **tú mismo posees**. ✓ Entra al grupo → recibe el rol solo; ↩ sale del grupo → el rol se retira solo. El grupo manda la membresía; SIAC sigue mandando qué significa el rol.

Tabla 6. Qué hace cada elemento de «5 · Mapea grupos → accesos (opcional, recomendado)» · 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 10

6 · Activa las salidas automáticas (SCIM)

👤 Tú, en SIAC · 🏢 Admin de Microsoft · ⏱ 10 min

DÓNDE ESTÁ
Seguridad › Microsoft Entra ID › Aprovisionamiento automático

DIRECCIÓN
/seguridad

QUIÉN LA USA
👤 Tú y 🏢 el administrador de Microsoft.

CUÁNDO USARLA
Para cerrar: es el paso que compra la promesa del principio.

Es el paso que compra la promesa del principio: que Microsoft **EMPUJE** los cambios, sin esperar a que nadie entre. Habilitar SCIM 1 te muestra una URL y un token 2: cópialos ya, el token se enseña **una sola vez**.

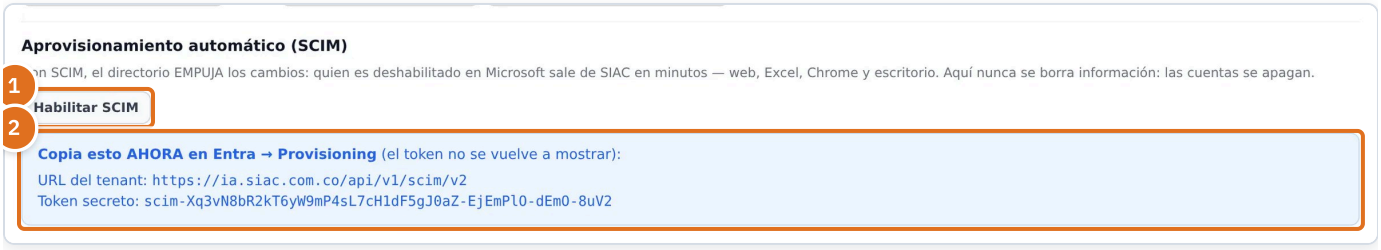

Figura 8. La URL y el token de SCIM, para pegar en Entra.

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.

PASO A PASO

1. 👤 **TÚ.** En la tarjeta, sección **Aprovisionamiento automático (SCIM)**, pulsa Habilitar SCIM 1. Copia la URL y el token 2.
2. 🏢 **ADMIN MS.** En el portal de Entra: **Aplicaciones empresariales → SIAC → Aprovisionamiento →** modo **Automático →** pega la URL en **URL de inquilino** y el token en **Token secreto → Probar conexión → Guardar → Iniciar aprovisionamiento**.
3. ⚙️ **AUTO.** Desde ahí, altas, cambios y —sobre todo— deshabilitaciones viajan solas a SIAC: 🔒 cuenta apagada (nunca borrada), 🚫 sesiones web y de complementos cerradas, 💻 equipos de escritorio revocados al instante, 📖 y el evento queda en la bitácora.
4. **Quedó bien si:** «Probar conexión» en Entra da verde — y al deshabilitar un usuario de prueba en Microsoft, en minutos aparece apagado en SIAC y el evento en la bitácora.

REGLA DEL SISTEMA

En SIAC nunca se borra información por una salida: la cuenta se apaga y su historial queda para auditoría. Si la persona regresa, se reactiva — pero sus equipos de escritorio revocados exigen enrolarse de nuevo, a propósito.

CONSEJO

Offboarding: de «lista de sistemas» a «un solo clic en RR. HH.». Si pierdes el token, el mismo botón dice **Rotar credencial** y el anterior deja de servir.

Tabla 7. Qué hace cada elemento de «6 · Activa las 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 11

El modo «Solo Microsoft» — y su puerta de emergencia

Cuando ya todo funcione

DÓNDE ESTÁ	DIRECCIÓN
Seguridad › Microsoft Entra ID	`/seguridad`
QUIÉN LA USA	**CUÁNDO USARLA**
👤 Tú.	Tras unos días en Opcional sin sorpresas.

Tras unos días en Opcional sin sorpresas, puedes subir a **Solo Microsoft** 1: la contraseña de SIAC se apaga para la gente del directorio (menos contraseñas = menos phishing) y la política de acceso queda 100 % en manos de tu Microsoft (MFA, acceso condicional, horarios).

La regla que SIAC te exige antes de permitirlo: 🏢 todos entran por Microsoft (la puerta normal) **+** 🗝️ un **administrador local de emergencia**, con contraseña y SIN identidad de Entra **=** 🛡️ nunca quedas fuera: si Microsoft falla, él entra y baja el modo.

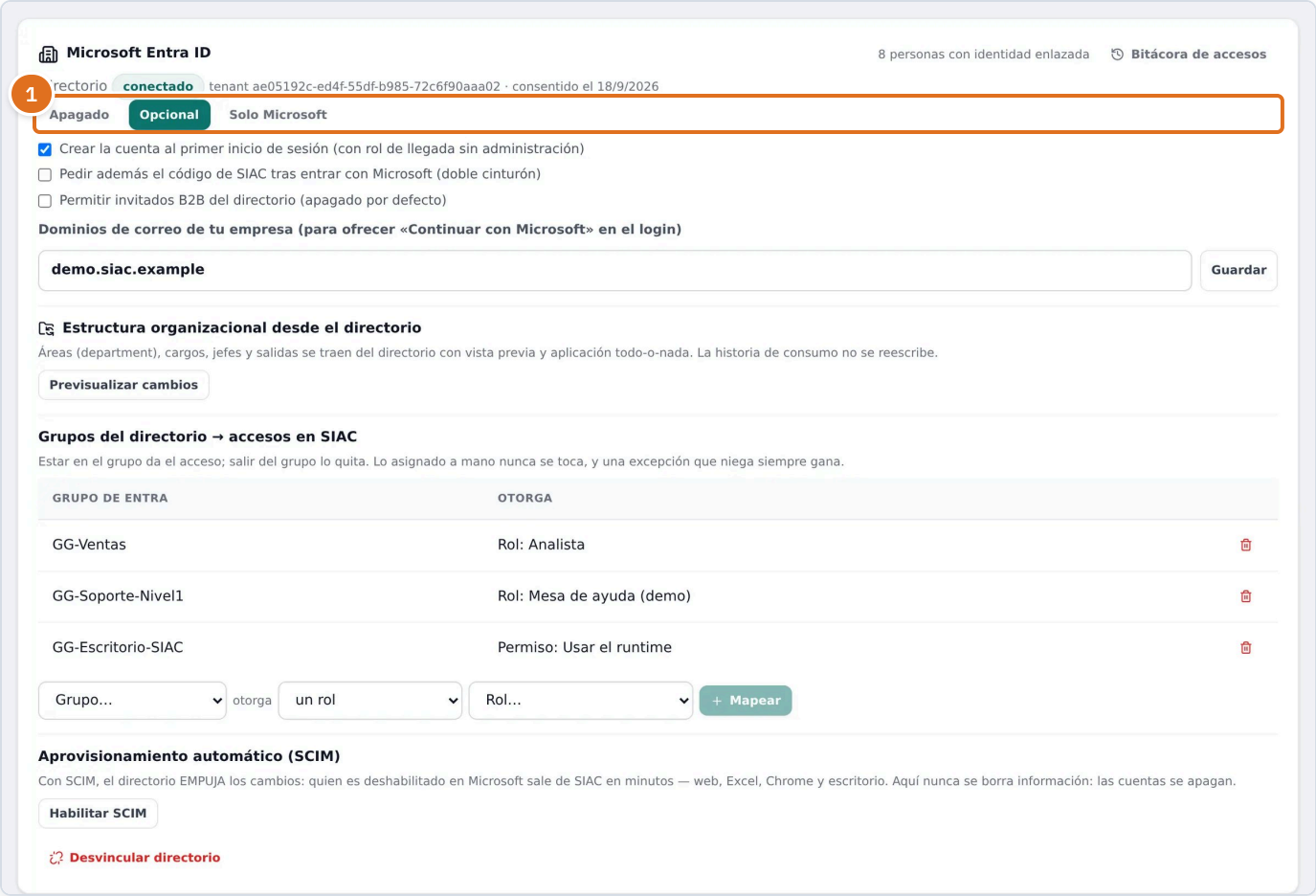

Figura 9. Los tres modos; «Solo Microsoft» exige el administrador de emergencia.

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).

SI SIAC NO LO DEJA AVANZAR

Sin ese administrador de emergencia, SIAC se niega a activar el modo «Solo Microsoft» — y la propia tarjeta te lo dice en rojo: «No queda ningún administrador local de emergencia». No es un capricho: es tu seguro contra un día malo de Microsoft o una app mal tocada en Entra.

Tabla 8. Qué hace cada elemento de «El modo «Solo Microsoft» — y su puerta de emergencia» · 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).

CAPÍTULO 12

Checklist final

¿Quedó todo? Repásalo en un minuto

- **Directorio conectado** — dónde: **Seguridad** › tarjeta Entra ID — se ve: «conectado» + tu tenant + fecha.
- **Botón en el login** — dónde: `/login` con un correo de tu dominio — se ve: «Continuar con Microsoft» visible.
- **Entrada sin contraseña** — dónde: Bitácora de accesos — se ve: «Microsoft · entró» con tu correo.
- **Organigrama vivo** — dónde: **Gobernanza** — se ve: tus áreas reales, cada quien en la suya.
- **Grupos → accesos** — dónde: tarjeta › tabla de mapeos — se ve: tus filas grupo → rol/permiso.
- **Salidas automáticas** — dónde: Entra › Aprovisionamiento — se ve: «Probar conexión» en verde, ciclo activo.
- **Puerta de emergencia** — dónde: tarjeta, al elegir «Solo Microsoft» — se ve: sin aviso rojo de admin local faltante.

CAPÍTULO 13

Preguntas frecuentes

¿Puedo hacer los 6 pasos yo solo?

Sí, si también eres administrador global de tu Microsoft 365. Si no, solo necesitas a esa persona 5 minutos en el paso 1 y unos minutos en el paso 6.

¿Qué pasa con la gente mientras pruebo?

Nada: en modo Opcional la contraseña de siempre sigue funcionando. Nadie queda fuera.