MANUAL DEL USUARIO · CENTRO DE AYUDA DE SIAC

Seguridad y cumplimiento

Qué protege a la información de tu empresa dentro de SIAC, quién puede ver qué, cómo se administran los accesos y qué cambia cuando tu operación vive en una instancia dedicada.

Dirigido a	Plataforma	Tiempo	Pantallas capturadas
Administradores y áreas de riesgos	**SIAC v1.0.147**	**20 minutos**	**30 de septiembre de 2026**

Contenido

1 · Antes de empezar 3
2 · Cómo funciona 4
3 · Compartido vs. dedicado 5
4 · El viaje de un dato 6
5 · Quién entra, y hasta dónde llega 7
6 · Accesos y roles: la pantalla 8
7 · Crear o clonar un rol 11
8 · Los accesos de una persona 13
9 · Quién usa SIAC Desktop 15
10 · Cifrado y custodia de llaves 17
11 · Aislamiento y contención 18
12 · El rastro que no se puede alterar 19
13 · El equipo del usuario 20
14 · Continuidad y respaldo 21
15 · Retención y borrado 22
16 · Cuándo puede entrar SIAC 23
17 · Lo que no hacemos 24
18 · Reportar una vulnerabilidad 25
19 · Preguntas frecuentes 26

CAPÍTULO 1

Antes de empezar

PARA QUIÉN ES
Administradores de la organización y áreas de riesgos, seguridad y cumplimiento que evalúan o gobiernan SIAC.

TIEMPO ESTIMADO
20 minutos

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

Lo que necesita

- Para leer el modelo de seguridad, nada. Para administrar los accesos, ser administrador de tu organización.

Tabla 1. Permisos

Rol	Qué puede hacer aquí
Administrador de la organización	Crear, clonar y asignar roles de acceso, conceder o denegar permisos puntuales, revisar la auditoría de accesos y decidir quién usa SIAC Desktop.
Operador de la plataforma	Lo mismo en todas las organizaciones de la plataforma.

Esta página describe el **modelo de seguridad**: qué garantiza la plataforma y qué queda en manos de tu organización. El detalle técnico —inventario de controles, evidencias y respuestas al cuestionario de tu área de riesgos— se entrega bajo acuerdo de confidencialidad; lo pides en `bercontsoft@bercont.com`.

- **Argon2id.** Las contraseñas nunca se guardan; solo su huella, con el algoritmo que hoy recomienda la industria.
- **Llave propia.** Cada instancia dedicada cifra con una llave que es solo suya. Ninguna otra puede leer sus secretos.
- **Cadena firmada.** La actividad se encadena por hash: alterar un registro rompe todos los siguientes y se nota.
- **Sin salida.** El código que la IA genera para fabricar documentos corre en una red sin acceso a internet.

CAPÍTULO 2

Cómo funciona

Punto de partida: la frontera de responsabilidad

La pregunta que ordena todo lo demás no es «¿es seguro SIAC?» sino «¿de qué responde cada uno?». Una plataforma puede estar impecablemente construida y aun así filtrar información si alguien concede permisos de más. Al revés también: la disciplina más estricta de permisos no sirve si la plataforma guarda las contraseñas en claro. Por eso el modelo tiene dos mitades, y las dos tienen que sostenerse.

SIAC responde de la plataforma

- Cifrado en tránsito y en reposo, y la custodia de las llaves.
- Aislamiento entre organizaciones y entre instancias.
- Que el rastro de actividad sea completo y no se pueda alterar.
- Respaldo, continuidad y el tiempo de recuperación pactado.
- Que una capacidad nueva nazca cerrada y haya que abrirla a propósito.
- Actualizar la plataforma y el ciclo de vida de los modelos.

Va en el contrato: no lo presupuestas ni lo operas tú.

Tu empresa responde del uso

1. Quién tiene cuenta, y qué permisos lleva cada rol.
2. Qué carpetas y qué conexiones puede tocar un agente.
3. Qué información se sube a los espacios de conocimiento.
4. Los límites de gasto por área y por persona.
5. Revisar la auditoría: la plataforma la produce, alguien la lee.
6. Dar de baja a quien se va, el mismo día.

Aquí es donde se pierde o se gana de verdad. **Ninguna de las dos mitades cubre a la otra.** SIAC hace imposible lo que debe ser imposible; tu organización decide lo que debe ser posible.

Consecuencia práctica: casi todos los incidentes reales de plataformas como esta empiezan en la segunda mitad —una cuenta que no se dio de baja, un permiso amplio «por rapidez», un espacio de conocimiento con un archivo que no debía estar—. Por eso SIAC empuja a que todo permiso sea explícito y quede registrado: para que esa mitad sea revisable, no una creencia.

CAPÍTULO 3

Compartido vs. dedicado

Qué cambia cuando tu operación tiene su propio servidor

SIAC funciona en dos modalidades. En el **plano compartido**, tu organización convive con otras en la misma infraestructura, separada por identificador en cada dato y en cada consulta. En una **instancia dedicada**, tu operación tiene servidor, base de datos, llave de cifrado y región propios: no comparte nada con nadie.

La diferencia no es de tamaño. Es de superficie: en una instancia dedicada, un fallo de aislamiento en otra organización no puede alcanzarte, porque no hay un «otra organización» del otro lado. El mismo código corre en las dos modalidades —permisos, auditoría encadenada, cifrado en tránsito y política del escritorio son idénticos—: es el mismo producto; la instancia dedicada cambia dónde vive, no cómo se gobierna. Lo que añade es soledad: servidor, base, llave y región propios.

Punto por punto

- **Base de datos.** Compartido: común; cada dato lleva marcada su organización y toda consulta filtra por ella. Dedicado: propia; no hay datos de terceros que separar.
- **Llave de cifrado.** Compartido: de la plataforma, con rotación programada; protege los secretos de todas las organizaciones. Dedicado: generada al crear tu instancia y usada solo por ella. Al migrar desde el plano compartido, tus secretos se vuelven a cifrar con ella en el traslado.
- **Servidor.** Compartido: el de SIAC, que lo opera y actualiza. Dedicado: tu servidor, solo con tu organización; también lo opera y actualiza SIAC.
- **Región de los datos.** Compartido: la que opera SIAC. Dedicado: la eliges del catálogo habilitado (México, Chile, Brasil), y la de respaldo puede ser otra distinta.
- **Actualizaciones.** Compartido: continuas, cuando SIAC despliega. Dedicado: por versiones publicadas; tu instancia se actualiza cuando tú lo aceptas, y hay vuelta atrás.
- **Continuidad.** Compartido: respaldo de la plataforma. Dedicado: nivel contratable, con un objetivo de pérdida y de recuperación pactado (más abajo).
- **Qué ve SIAC.** Compartido: opera la plataforma completa. Dedicado: del funcionamiento de tu instancia solo recibe agregados —cuántas personas la usan, cuánto costó la IA, qué versión corre y si está sana—. Nunca contenido, nunca el detalle de una persona.
- **Si otra empresa tiene un problema.** Compartido: el aislamiento por organización lo contiene. Dedicado: no te alcanza; no comparten nada.

Sobre la migración: pasar del plano compartido a una instancia dedicada mueve tus datos completos —incluidos los que no cuelgan de una tabla, como los archivos y las referencias a catálogos—, vuelve a cifrar tus secretos con tu llave nueva y verifica al final que lo que llegó coincide con lo que salió. Si algo no cuadra, el traslado se detiene en vez de continuar a medias.

CAPÍTULO 4

El viaje de un dato

Por dónde pasa lo que escribes, y dónde se queda cada cosa



Recorrido de una petición desde el equipo del usuario hasta el modelo de IA y de vuelta

La pregunta que más se repite en una revisión de riesgos es simple: «¿por dónde pasa lo que escribo, y qué queda guardado?». Este es el recorrido completo de una petición. Cada tramo viaja cifrado (TLS).

Queda guardado, para tu auditoría: quién y cuándo, qué modelo usó, cuánto costó y qué herramienta tocó qué archivo.

Tres cosas que NO ocurren en este recorrido

- Tu contenido no se usa para entrenar modelos, ni propios ni del proveedor.
- El equipo no envía nada que la política de tu organización no haya autorizado a leer.
- Ningún otro cliente de SIAC puede consultar tu actividad ni tu consumo.

Lo que se conserva es el **metadato** —quién, cuándo, con qué modelo, cuánto costó, qué archivo tocó—, porque es lo que hace auditable el uso de la IA. El contenido de la conversación se conserva solo donde tú lo pides: en el historial de tu chat y en los espacios de conocimiento que tu organización crea.

CAPÍTULO 5

Quién entra, y hasta dónde llega

Identidad y acceso

- **Contraseñas: nunca se guardan.** Se almacena una huella calculada con Argon2id, el algoritmo que hoy recomienda la industria frente a ataques con hardware dedicado. Ni SIAC ni nadie puede recuperar tu contraseña: solo comprobar si la que escribes coincide.
- **Sesiones de vida corta.** La credencial que viaja en cada petición caduca en minutos y se renueva sola mientras trabajas. Si alguien la interceptara, le serviría durante muy poco tiempo.
- **Segundo factor: código de un solo uso.** Para entrar y para acciones sensibles, según lo que tu organización active. El código caduca en minutos, admite pocos intentos y de él se guarda solo su huella.
- **Recuperación sin revelar quién existe.** Pedir recuperar una contraseña responde igual exista o no la cuenta. Es lo que impide usar ese formulario para averiguar quién trabaja en tu empresa.
- **Identidad corporativa: entra con la cuenta de tu empresa.** SIAC se integra con el directorio de Microsoft: la persona entra con su cuenta corporativa, se crea sola la primera vez y se sincroniza después. Quien deja la empresa pierde el acceso donde ya lo pierde todo, sin depender de que alguien se acuerde. Ver Directorio Activo.
- **Permisos: lo no concedido, no se puede.** Cada acción exige un permiso concreto. Los roles agrupan permisos y se pueden afinar persona a persona. Una capacidad nueva nace cerrada: hay que abrirla a propósito, y queda registrado quién la abrió.

La estructura de tu organización manda

Los permisos no viven en una lista plana: cuelgan de tus áreas. Un jefe de área ve y administra lo suyo —su gente, su consumo, su presupuesto— y no lo de al lado. Eso permite delegar la administración sin repartir llaves maestras, que es la forma más común de perder el control sin darse cuenta. Las secciones siguientes muestran dónde se administra todo esto en SIAC.

CAPÍTULO 6

Accesos y roles: la pantalla

A qué módulos y funciones entra cada persona, al estilo de un ERP

DÓNDE ESTÁ
Administración › Accesos y roles

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
Administradores de la organización

CUÁNDO USARLA
Cuando necesitas dar a un grupo de personas acceso a unos módulos y no a otros, o revisar quién puede qué.

Desde **Accesos y roles** controlas a qué módulos entra cada persona y qué funciones puede usar dentro de cada uno. **Nuevo rol** 1 crea un rol marcando módulos y funciones en la matriz, y **Auditoría** 2 muestra todo cambio de roles y permisos: qué se hizo, quién y cuándo. Arriba ves cuántos roles hay, cuántos son de sistema y cuántas asignaciones tienen 3.

Cada tarjeta es un rol reutilizable 4 con su número de permisos y de usuarios. Las plantillas (**Solo productividad**, **Analista**, **Supervisor de área**, **Auditor**) sirven de punto de partida: **Clonar** 5 crea una copia editable. En un rol propio, **Editar** 6 cambia sus permisos.

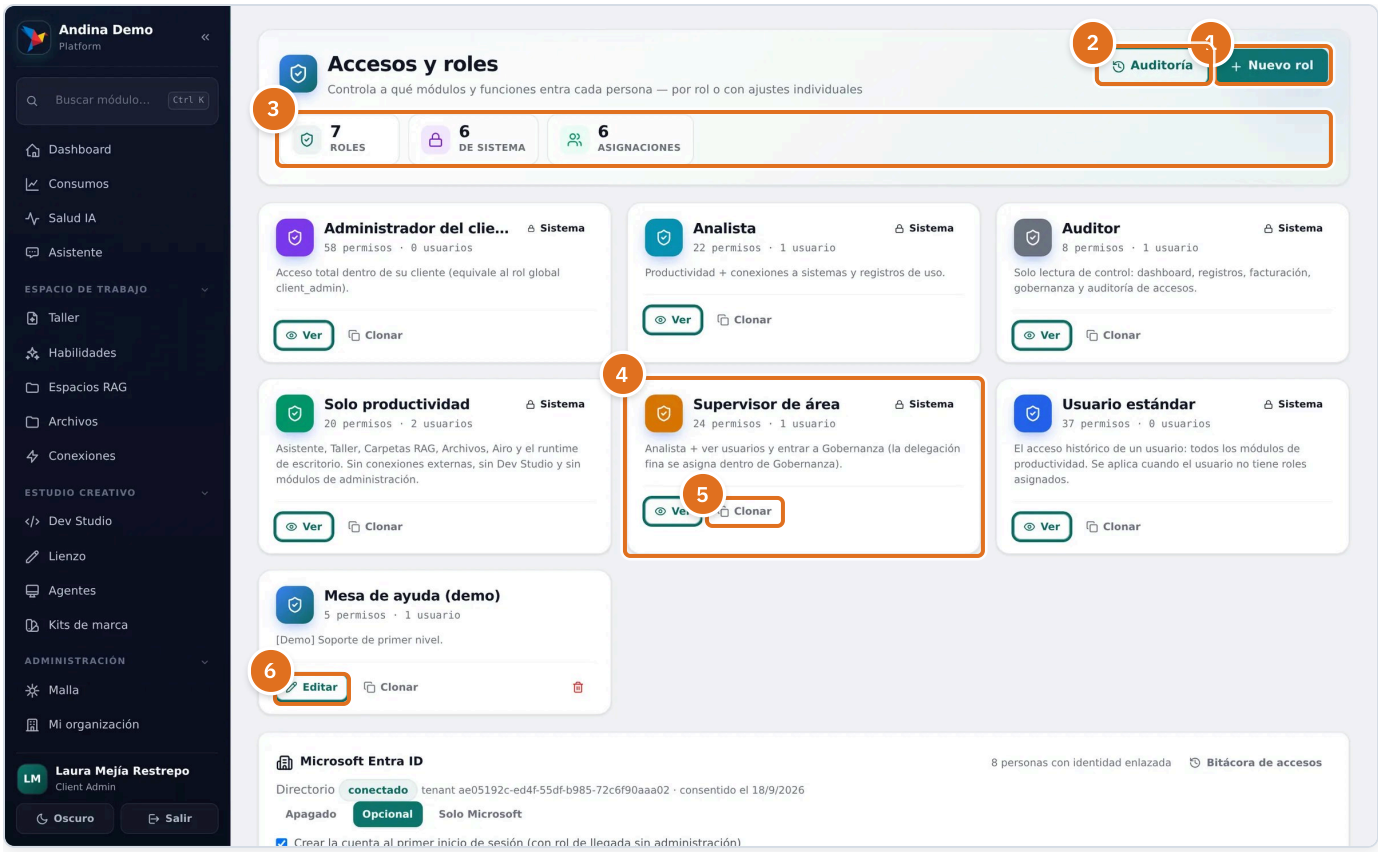


Figura 1. Los roles de acceso de una organización de ejemplo: plantillas de sistema y un rol propio.

1. **Nuevo rol.** Abre el editor para crear un rol de acceso marcando qué módulos y funciones permite.
2. **Auditoría.** Abre el registro de todos los cambios de roles y permisos: qué se hizo, quién y cuándo.
3. **Roles · De sistema · Asignaciones.** Cuántos roles hay, cuántos son de sistema (no se pueden cambiar) y cuántas veces están asignados a personas.
4. **Sistema.** Un rol con su nombre, cuántos permisos da y a cuántos usuarios; los que dicen «Sistema» son fijos y solo se pueden ver o clonar.
5. **Clonar.** Crea una copia editable del rol para personalizarla sin tocar el original.
6. **Editar.** Abre el rol para cambiar sus permisos; en un rol de sistema el botón dice «Ver» y solo lo muestra.

REGLA DEL SISTEMA

Los roles de sistema son inmutables: en ellos el botón dice **Ver**. Clónalos para personalizarlos.

REGLA DEL SISTEMA

Un rol propio solo se puede eliminar si no está asignado a nadie.

CONSEJO

¿Con cuántas personas se sostiene todo esto? La guía Gobierno de la IA define los 7 perfiles del gobierno y te deja proyectar tu equipo según el tamaño de tu empresa.

Tabla 2. Qué hace cada elemento de «Accesos y roles: la pantalla» · los usan: Administradores de la organización

Elemento	Qué hace
Nuevo rol	Abre el editor para crear un rol de acceso marcando qué módulos y funciones permite.
Auditoría	Abre el registro de todos los cambios de roles y permisos: qué se hizo, quién y cuándo.
Roles · De sistema · Asignaciones	Cuántos roles hay, cuántos son de sistema (no se pueden cambiar) y cuántas veces están asignados a personas.
Sistema	Un rol con su nombre, cuántos permisos da y a cuántos usuarios; los que dicen «Sistema» son fijos y solo se pueden ver o clonar.
Clonar	Crea una copia editable del rol para personalizarla sin tocar el original.
Editar	Abre el rol para cambiar sus permisos; en un rol de sistema el botón dice «Ver» y solo lo muestra.

CAPÍTULO 7

Crear o clonar un rol

Marca módulos completos o funciones sueltas

DÓNDE ESTÁ
Administración › Accesos y roles

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
Administradores de la organización

CUÁNDO USARLA
Cuando ninguna plantilla encaja con lo que un grupo de personas debe poder hacer.

El editor del rol pide nombre, color y descripción, y la lista de **módulos y funciones** que permite 2: marca un módulo completo o solo algunas de sus funciones; el contador de cada módulo dice cuántas quedan permitidas. Para encontrar un permiso, escríbelo en el buscador 1. Al lado, una vista previa muestra el menú que verá quien tenga el rol. **Guardar** 3 lo guarda; en un rol nuevo el botón dice **Crear rol**.

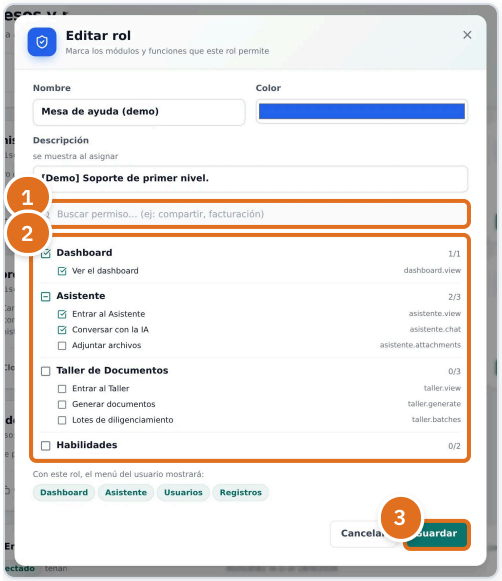


Figura 2. El editor de un rol propio con sus módulos y funciones.

1. **Buscar permiso... (ej: compartir, facturación).** Filtra la lista de módulos y funciones del editor por nombre.
2. **Módulos y funciones.** Marca un módulo completo o funciones sueltas; el contador de cada módulo dice cuántas funciones quedan permitidas.
3. **Crear rol.** Guarda el rol (dice «Guardar» al editar); si tu organización lo exige, antes pide un código por WhatsApp.

PASO A PASO

1. Pulsa **Nuevo rol**, o **Clonar** en la plantilla que más se parezca.
2. Escribe el nombre y la descripción del rol.
3. Marca los módulos y funciones que permite 2.

4. Pulsa **Crear rol** (o **Guardar**, si lo estás editando) 3. Si tu organización lo exige, SIAC te pide antes un código por WhatsApp.
5. Asígnalo a las personas desde **Usuarios** › ··· › **Accesos** (siguiente sección).

SI SIAC NO LO DEJA AVANZAR

«No puedes conceder un permiso que no posees o que no existe: …»

Por qué aparece. Anti-escalación: nadie concede permisos que no posee. El mensaje nombra los permisos en cuestión.

Qué hacer. Pide a quien tenga ese permiso que haga el cambio, o que te lo conceda primero.

Tabla 3. Qué hace cada elemento de «Crear o clonar un rol» · los usan: Administradores de la organización

Elemento	Qué hace
Buscar permiso… (ej: compartir, facturación)	Filtra la lista de módulos y funciones del editor por nombre.
Módulos y funciones	Marca un módulo completo o funciones sueltas; el contador de cada módulo dice cuántas funciones quedan permitidas.
Crear rol	Guarda el rol (dice «Guardar» al editar); si tu organización lo exige, antes pide un código por WhatsApp.

CAPÍTULO 8

Los accesos de una persona

Roles, ajustes individuales y permisos efectivos con procedencia

DÓNDE ESTÁ
Administración › Usuarios

DIRECCIÓN
`/users`

QUIÉN LA USA
Administradores de la organización

CUÁNDO USARLA
Cuando asignas un rol, o alguien no ve (o ve de más) un módulo.

La asignación se hace en **Usuarios › ··· › Accesos**. En **Roles de acceso** 1 asignas o quitas roles; en **Ajustes individuales** 2 concedes o deniegas un permiso puntual con su motivo. **Permisos efectivos** 3 muestra **por qué** la persona tiene cada permiso («por el rol Analista», «denegado individualmente») y **Ver como** 4 previsualiza el menú que verá.



Figura 3. Los accesos de una persona: un rol asignado y un permiso concedido aparte, con su motivo.

1. **Roles de acceso.** Los roles de la organización: pulsa Asignar para dárselo a la persona o Asignado ✓ para quitárselo. Sin ningún rol, conserva su acceso por defecto.
2. **Ajustes individuales.** Concede o deniega un permiso solo a esta persona, con un motivo que queda en la auditoría; la denegación siempre gana sobre cualquier rol.
3. **Permisos efectivos.** Pestaña con cada permiso que la persona tiene o no tiene, y por qué: el rol que lo da o el ajuste que lo niega.
4. **Ver como.** Muestra los módulos del menú que verá la persona al entrar, con sus accesos de hoy.

IMPORTANTE

Un usuario **sin roles asignados** conserva su acceso histórico completo; al asignarle roles, su acceso pasa a ser **exactamente** el de sus roles.

REGLA DEL SISTEMA

La denegación siempre gana, incluso sobre un rol amplio. Nadie concede permisos que no posee (anti-escalación), el sistema impide dejarte sin administrador de accesos (anti-lockout), los cambios pueden exigir código por WhatsApp si tu organización activó la verificación, y todo queda en la auditoría con su detalle.

SI SIAC NO LO DEJA AVANZAR

«Este cambio dejaría al cliente sin ningún administrador de accesos. Asigna primero ese permiso a otra persona.»

Por qué aparece. Quitarías el último permiso de administrar accesos de tu organización.

Qué hacer. Asigna ese permiso a otra persona y repite el cambio.

Tabla 4. Qué hace cada elemento de «Los accesos de una persona» · los usan: Administradores de la organización

Elemento	Qué hace
Roles de acceso	Los roles de la organización: pulsa Asignar para dárselo a la persona o Asignado ✓ para quitárselo. Sin ningún rol, conserva su acceso por defecto.
Ajustes individuales	Concede o deniega un permiso solo a esta persona, con un motivo que queda en la auditoría; la denegación siempre gana sobre cualquier rol.
Permisos efectivos	Pestaña con cada permiso que la persona tiene o no tiene, y por qué: el rol que lo da o el ajuste que lo niega.
Ver como	Muestra los módulos del menú que verá la persona al entrar, con sus accesos de hoy.

CAPÍTULO 9

Quién usa SIAC Desktop

El acceso al escritorio, con su porqué

DÓNDE ESTÁ
Administración › Accesos y roles

DIRECCIÓN
`/seguridad`

QUIÉN LA USA
Administradores de la organización

CUÁNDO USARLA
Cuando alguien necesita (o ya no debe tener) el agente de SIAC en su computador.

Acceso al escritorio 1 lista quién puede iniciar sesión en la app de escritorio (Windows y macOS) y **por qué**: un rol que incluye «Usar el runtime» o una excepción individual. Busca a una persona 2 y da o quita el acceso con un clic (Dar acceso, Quitar acceso); quitárselo a alguien que lo hereda de un rol crea una excepción que **niega**, sin tocar el rol. Más abajo, **Runtime de escritorio** define qué puede hacer el agente dentro de esos equipos, por empresa, área, perfil o persona: lo detalla el manual de Runtime.

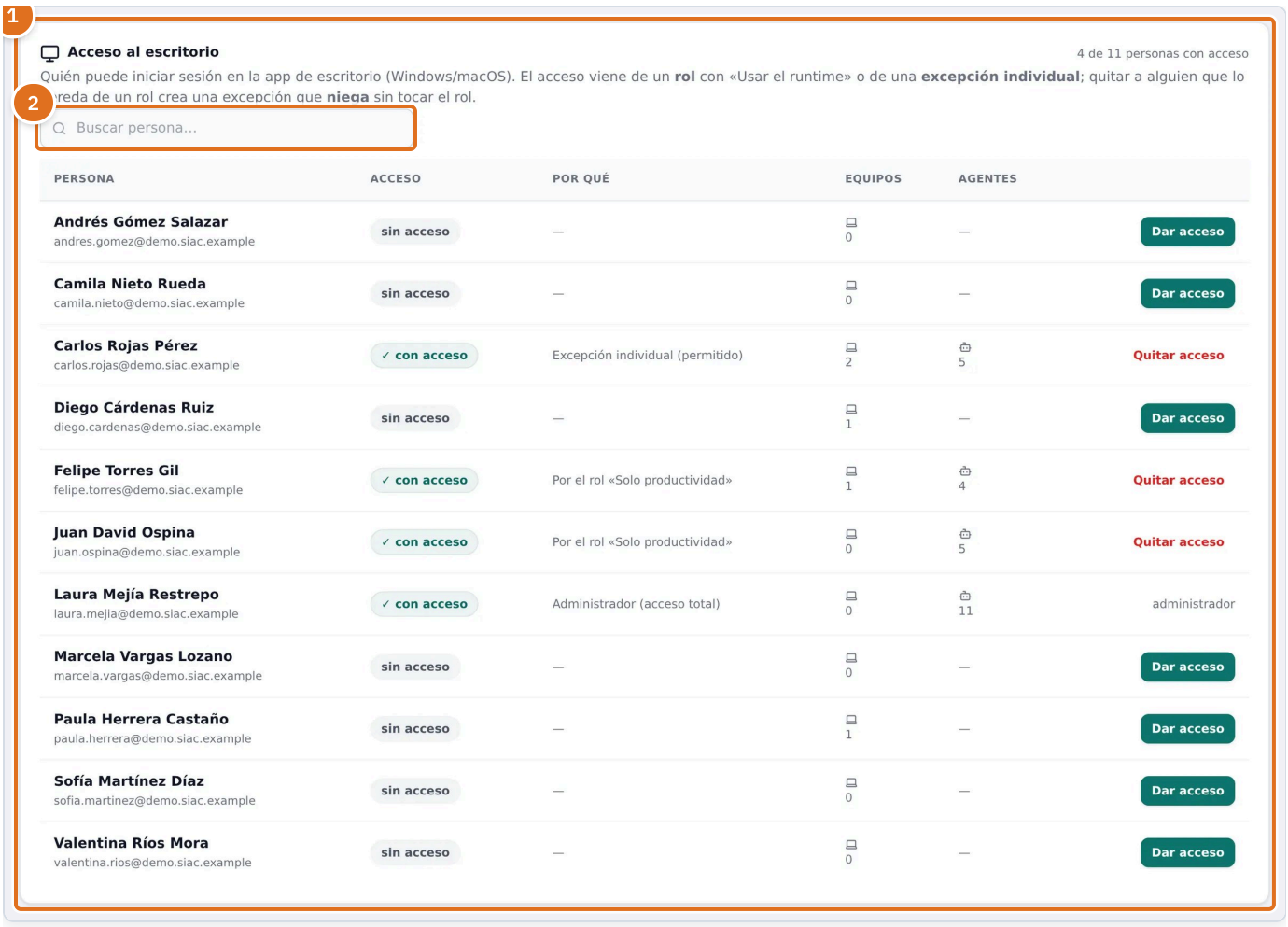


Figura 4. Quién puede usar SIAC Desktop en una organización de ejemplo, y por qué.

1. **Acceso al escritorio.** Lista quién puede iniciar sesión en SIAC Desktop, por qué (rol o excepción), cuántos equipos y agentes tiene, con acciones para dar o quitar el acceso.
2. **Buscar persona...** Filtra la tabla de acceso al escritorio por nombre o correo.

Tabla 5. Qué hace cada elemento de «Quién usa SIAC Desktop» · los usan: Administradores de la organización

Elemento	Qué hace
Acceso al escritorio	Lista quién puede iniciar sesión en SIAC Desktop, por qué (rol o excepción), cuántos equipos y agentes tiene, con acciones para dar o quitar el acceso.
Buscar persona...	Filtra la tabla de acceso al escritorio por nombre o correo.

CAPÍTULO 10

Cifrado y custodia de llaves

En tránsito, en reposo, y quién guarda las llaves

En tránsito. Todo lo que va y viene entre tu equipo, tu navegador y la plataforma viaja por TLS. También lo que la plataforma envía al proveedor del modelo.

En reposo. Los datos viven en una base con acceso restringido, y por encima hay una segunda capa para lo que más importa: los secretos se guardan cifrados columna a columna —credenciales de conexiones a sistemas de terceros, tokens de integración, el historial de conversaciones del asistente—. Aunque alguien obtuviera una copia de la base, esos campos son ilegibles sin la llave.

Las llaves. Se guardan fuera de la base, en la configuración del servicio, y se pueden rotar: la llave nueva pasa a cifrar y la anterior se conserva solo para poder leer lo viejo mientras se vuelve a cifrar. En una instancia dedicada esa llave es exclusivamente tuya.

Una regla que conviene conocer: SIAC lleva un historial de versiones de tus agentes y procesos, para poder volver atrás si un cambio salió mal. Ese historial excluye por diseño cualquier campo que contenga un secreto. Un historial es, por definición, algo que se conserva y se puede consultar; meter allí una credencial sería fabricar una fuga con buena intención.

CAPÍTULO 11

Aislamiento y contención

Contener el daño antes de que exista

Buena parte de la seguridad de una plataforma de IA no está en impedir que algo salga mal, sino en acotar hasta dónde puede llegar cuando sale mal. Estos son los cercos:

- **Entre organizaciones: todo dato sabe de quién es.** En el plano compartido, cada registro lleva su organización y toda consulta filtra por ella. En una instancia dedicada el problema no existe: no hay datos de terceros.
- **Fabricación de documentos: una red sin salida.** Cuando la IA escribe código para construir un Excel o una presentación, ese código corre en un contenedor conectado a una red sin acceso a internet. Aunque el modelo generara algo indebido, no tiene por dónde mandarlo fuera.
- **Navegación: no sirve de puente a tu red.** Cuando un agente consulta una página, el destino se resuelve y se comprueba antes de pedirlo: se rechazan direcciones internas, privadas y las de servicios de metadatos de nube — incluso si una dirección pública redirige hacia ellas.
- **Recursos: ninguna tarea ahoga a las demás.** Los trabajos pesados corren con límites duros de CPU y memoria impuestos por el sistema, no solo por la aplicación. Una tarea desbocada no puede degradar el servicio de los demás.

CAPÍTULO 12

El rastro que no se puede alterar

Auditoría encadenada por huella



Cadena de auditoría por huella: cada registro guarda la huella del anterior

Un registro de actividad sirve para auditar solo si no se puede editar sin que se note. Un archivo de texto al que alguien con acceso puede quitarle una línea no prueba nada.

En SIAC, la actividad de un proceso **se encadena**: cada anotación incluye la huella de la anterior. Cambiar una anotación cambia su huella, y a partir de ahí todas las siguientes dejan de cuadrar. Borrar una deja un hueco en la numeración. No impide que alguien lo intente; hace imposible que pase inadvertido. Si alguien edita el registro #2 para borrar lo que hizo, su huella cambia (por ejemplo, de `7b02…` a `f3aa…`), el #3 sigue apuntando a una anterior que ya no existe y la cadena ya no cuadra. Basta con recalcular la cadena para saber si alguien la tocó — y desde dónde.

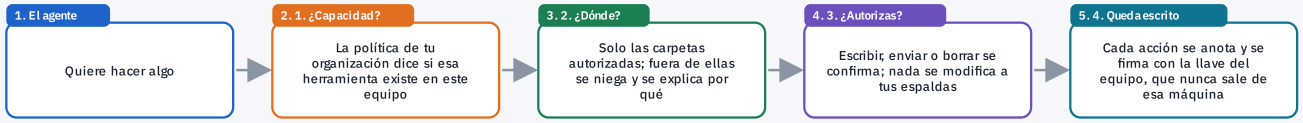
Lo mismo se aplica a la actividad del escritorio, con un añadido: cada equipo firma sus anotaciones con una llave que nunca sale de esa máquina. Una anotación que no verifica se marca como no verificada en vez de aceptarse en silencio.

Además de esa cadena, queda un **registro administrativo** de las acciones que cambian el gobierno —crear usuarios, cambiar permisos, tocar presupuestos, entrar por soporte— con quién lo hizo, cuándo y desde dónde. Los cambios de accesos los ves en **Auditoría** de Accesos y roles.

CAPÍTULO 13

El equipo del usuario

Un agente en la máquina de tu gente, con correa corta



Las cuatro compuertas que atraviesa una acción del agente en el equipo del usuario

SIAC puede trabajar dentro del equipo del usuario: leer un archivo, preparar un documento, usar Excel. Es donde más valor da y también donde más cuidado exige, porque ahí está todo lo demás de esa persona.

El principio es que **el equipo ejecuta, pero no decide**. Lo que puede hacer lo dicta una política que firma tu organización y que el equipo verifica antes de aplicar. Un archivo de configuración editado a mano no sirve: sin firma válida, no se aplica.

Lo no declarado, no se puede. Si la política no nombra una capacidad o una carpeta, la respuesta es no. Un equipo que se queda sin conexión conserva lo último firmado durante un tiempo y después se cierra: no se queda abierto por inercia. El usuario siempre tiene un freno inmediato desde la barra del sistema para detener lo que el agente esté haciendo, sin necesidad de encontrar la ventana.

Una precisión que suele hacer falta en las revisiones: las carpetas que el agente puede tocar las decide tu organización en la política, no el usuario y no SIAC. El usuario puede restringir aún más lo que ya se le concedió, nunca ampliarlo.

CAPÍTULO 14

Continuidad y respaldo

Qué pasa si se cae el servidor

Para una instancia dedicada, la continuidad es un nivel que se contrata, y cada nivel promete dos números: cuánta información se puede perder en el peor caso y cuánto tarda el servicio en volver.

- **Nivel base.** Copia diaria completa. Pérdida máxima 24 h · vuelta en menos de 8 h.
- **Nivel alto.** Réplica continua a otra región. Pérdida máxima 5 min · vuelta en menos de 30 min.
- **Probado, no prometido.** El plan de recuperación se ensaya de verdad: se apaga la principal y se cronometra la vuelta.

El nivel alto mantiene una copia viva en otra región, alimentada de forma continua. Si la principal cae, la copia toma el relevo; cuando la principal vuelve, el regreso se hace en una ventana acordada y solo después de comparar tabla por tabla que las dos coinciden. Si no coinciden, el regreso automático se niega y espera a una persona: preferimos un servicio que sigue en la copia a uno que vuelve perdiendo escrituras.

Por qué esto importa más que el número: un plan de recuperación que nunca se ha ejecutado es una hipótesis. El de SIAC se ensaya matando la principal a propósito y midiendo el tiempo real de vuelta, con las etapas registradas. Los números de arriba son compromisos contractuales con margen sobre lo medido, no estimaciones optimistas.

CAPÍTULO 15

Retención y borrado

Cuánto se guarda, y qué no se borra nunca

SIAC distingue dos cosas que suelen confundirse: el detalle de cada petición y el agregado que resume tu actividad.

- **El detalle** —cada llamada, con su modelo, su costo y su huella— se conserva durante la ventana que tu plan cubre, con un mínimo de cinco años. Hay niveles de archivo extendido si tu sector exige más, y se contratan con precio a la vista.
- **El agregado** —tus estadísticas por día, por proceso, por área— no se borra. Es lo que sostiene la comparación histórica y el retorno de inversión: si se purgara, tu serie de años se rompería y ningún informe pasado volvería a cuadrar.
- **La auditoría** tampoco se purga con el detalle. Un registro de quién hizo qué que caduca antes que la obligación de conservarlo no cumple su función.

Cuando terminas la relación con SIAC, tus datos se exportan en formato utilizable y se eliminan según lo pactado. La exportación se verifica antes de dar por buena la eliminación.

CAPÍTULO 16

Cuándo puede entrar SIAC

Cuándo podemos entrar, y cómo lo sabes

Es la pregunta incómoda y merece una respuesta directa: sí, existe una forma de que soporte entre a tu instancia, porque sin ella no se puede diagnosticar un problema que solo ocurre en tu servidor. Lo que importa es bajo qué condiciones.

- **Modo por defecto: tú abres la puerta.** Soporte no puede entrar hasta que un administrador de tu organización abre una ventana de soporte. Sin esa ventana abierta, el acceso se rechaza aunque la credencial sea válida.
- **Credencial de un solo uso y corta.** El acceso usa una credencial emitida para esa sesión, con caducidad de una hora, que tu instancia verifica por firma. No hay contraseñas de soporte guardadas ni acceso remoto permanente al servidor.
- **Rastro: siempre queda escrito.** Cada entrada de soporte y cada comando ejecutado quedan en tu auditoría, con quién fue y cuándo. No hay modo silencioso.
- **Modo contractual: solo si tú lo eliges.** Algunas organizaciones prefieren que soporte pueda entrar sin esperar aprobación para acortar los tiempos de respuesta. Es una opción que tú activas, y sigue registrando y notificando cada acceso.

Lo que soporte no hace nunca: leer el contenido de tus conversaciones ni tus documentos como parte de la operación normal. El diagnóstico trabaja sobre el estado del servicio —si responde, si tiene espacio, qué versión corre—, no sobre lo que tu gente escribió.

CAPÍTULO 17

Lo que no hacemos

Lo que no hacemos con tu información

- **No entrenamos con tu contenido.** Ni modelos propios ni los del proveedor. Lo que tu gente escribe se usa para responderle, y para nada más.
- **No vendemos datos.** Ni a terceros, ni para publicidad, ni agregados «anonimizados».
- **No mezclamos organizaciones.** Ninguna función de SIAC compara tu actividad con la de otro cliente ni la usa como referencia.
- **No abrimos capacidades solas.** Una función nueva que toque archivos, conexiones o el equipo del usuario llega cerrada. Alguien de tu organización tiene que abrirla, y queda registrado quién.

CAPÍTULO 18

Reportar una vulnerabilidad

Si encuentras un fallo, cuéntanoslo

Si detectas una vulnerabilidad —en la plataforma, en los complementos de Office, en la aplicación de escritorio o en esta misma documentación— escríbenos a `soporte@siac.com.co` con el asunto «Seguridad». Pedimos dos cosas: que no accedas a datos de terceros para demostrarlo, y que nos des margen para corregirlo antes de publicarlo. Respondemos con acuse en días hábiles y te mantenemos al tanto hasta el cierre. Si el hallazgo es real y lo reportaste así, lo reconocemos.

¿Tu área de riesgos necesita más detalle?

Esta página describe el modelo. Para una revisión formal entregamos, bajo acuerdo de confidencialidad, el inventario detallado de controles, la arquitectura de referencia, la matriz de responsabilidades, la política de gestión de incidentes y las respuestas al cuestionario de seguridad que use tu organización. **Solicita el detalle técnico** en `bercontsoft@bercont.com`: ese buzón es para documentación y consultas comerciales. Si lo que tienes es un hallazgo de seguridad, va por el canal de arriba: `soporte@siac.com.co`.

Relacionado: Cómo se gobierna el uso · Política de privacidad · Todos los manuales.

Última revisión del modelo: 25 de agosto de 2026. Este documento describe el estado vigente de la plataforma y se actualiza cuando el modelo cambia. Para condiciones contractuales concretas —SLA, tratamiento de datos, subencargados— manda tu contrato con SIAC.

CAPÍTULO 19

Preguntas frecuentes

¿Cómo doy acceso solo a algunos módulos a una persona?

Crea o clona un rol (por ejemplo **Solo productividad**), ajusta sus módulos y asígnalo a la persona en **Usuarios › ··· › Accesos**.

¿Por qué no puedo editar un rol de sistema?

Porque son inmutables: clónalo y personaliza la copia.

¿Por qué no puedo conceder un permiso?

Solo puedes conceder permisos que tú mismo posees (anti-escalación).

¿SIAC usa lo que escribimos para entrenar modelos?

No. Ni modelos propios ni los del proveedor: lo que tu gente escribe se usa para responderle, y para nada más.

¿Dónde se guardan nuestros datos?

En el plano compartido, en la región que opera SIAC. En una instancia dedicada, en la región que tú eliges del catálogo habilitado (México, Chile, Brasil).