



Seguridad y protección de datos

Lo que un equipo de TI o un auditor necesita verificar antes de conectar Askí a un ERP.

Versión 1.3 · 25 de agosto de 2026 · Complemento técnico de la política de privacidad publicada en aski.dev/privacy

Qué hace Askí con los datos

Askí es un asistente que responde preguntas de negocio consultando el ERP del cliente —Odoo, SAP S/4HANA o SAP Business One— en lenguaje natural. **Consulta en vivo, en modo solo lectura por defecto y con los permisos del usuario que se conecta.** No replica la base de datos del cliente ni la comparte con otros clientes.

Roles en el tratamiento

RESPONSABLE	ENCARGADO	SUBENCARGADO
La empresa cliente Dueña del ERP y de los datos que contiene. Decide qué se trata y para qué.	El socio implementador Gestiona la relación con la empresa cliente y contrata el servicio en su nombre.	Askí Trata los datos solo para responder las consultas que el propio usuario formula.

Firmamos acuerdo de tratamiento de datos y de confidencialidad a solicitud, incluidas las cláusulas de transferencia internacional. Si la organización tiene un formato propio, lo revisamos y lo firmamos.

Dónde está alojado

Componente	Proveedor	Qué recibe
Backend y base de datos	Railway (EE. UU.)	Aloja la infraestructura. Acceso operativo, sin consulta directa de los datos.
Modelo de lenguaje	Anthropic — Claude (EE. UU.)	Pregunta, esquema del ERP y un extracto acotado de filas. Ver más abajo.
Sitio y aplicación web	Vercel (EE. UU.)	Solo entrega de la interfaz. No recibe datos del ERP.
Enlace a ERP internos	Tailscale (EE. UU.)	Solo en conexiones por túnel. Datos del enlace: nombre de la organización, del equipo y rangos de red internos. No recibe el contenido de las consultas.
Copias de seguridad	Respaldo diario	Copia completa de la base, con retención de 30 días.
Correo, registros y errores	Resend · Better Stack · Sentry (EE. UU.)	Correos de la plataforma y trazas técnicas sin contenido de mensajes.

La lista completa de terceros, con qué recibe cada uno y su país, está publicada en aski.dev/privacy, sección 4. Hay transferencia internacional de datos hacia Estados Unidos y así está declarado.

Si el ERP no es alcanzable desde internet

Muchas instalaciones on-premise no están publicadas, y no tienen por qué estarlo. Para esos casos se instala un **nodo de red privada** (Tailscale) en una máquina de la misma red donde vive el ERP, y el backend entra por ahí.

Lo que NO hace falta • Ningún puerto de entrada abierto en el firewall del cliente: el nodo establece la conexión hacia afuera, igual que un navegador. • Ni IP pública, ni redirección de puertos, ni publicar el ERP. • No se toca el servidor del ERP: el nodo va en cualquier máquina siempre encendida de esa red (Linux si el ERP usa HTTPS).	Aislamiento y control • Cada cliente entra con su propia llave, etiquetada y revocable de forma independiente. • Las reglas de la red privada solo permiten backend → nodo del cliente, y únicamente hacia los puertos del ERP. Los nodos de dos clientes no se ven entre sí. • Las credenciales del ERP las introduce el propio cliente en la aplicación; no se comparten con nosotros por ningún canal.
---	---

El enlace corre como un servicio separado del backend principal, y la conexión se marca «por túnel» una a una: marcada así sale siempre por el túnel y nunca por internet; una conexión normal nunca lo usa.

Aislamiento entre clientes

1. **No se mantiene copia del ERP de ningún cliente.** No existe un repositorio común donde los datos de dos clientes puedan cruzarse: cada consulta se ejecuta en vivo contra la instancia de ese cliente y devuelve solo las filas de esa pregunta. Lo que sí se guarda es el historial de la conversación, ligado a la cuenta de quien preguntó.
2. **Cada conexión pertenece a un solo usuario.** Credenciales, conversaciones y mensajes están ligados al identificador de su dueño y toda consulta se filtra por el usuario autenticado. Ninguna ruta de la API devuelve una credencial en claro: no se muestra en la app, no se expone por la API y no aparece en el panel de administración ni en los registros.
3. **Aski no ve más de lo que ve el usuario conectado.** Consulta el ERP con las credenciales de ese usuario, sin elevación de privilegios. Si ese usuario no puede ver costos, márgenes o los datos de otra compañía, Aski tampoco.

Precisión técnica: para acelerar las respuestas se mantiene en memoria temporal un catálogo con nombres y etiquetas de *campos estándar* del ERP, común a instancias de la misma versión e idioma. Contiene nomenclatura —nombres y etiquetas de campos, y los valores de los campos de clasificación de baja cardinalidad: etapas, categorías, etiquetas—, nunca modelos a medida, nunca registros y nunca cifras. Antes de usarse se cruza con el esquema real de la instancia, así que nunca enseña a una instancia algo que no tenga.

Cifrado y control de accesos

Cifrado

- **En tránsito:** HTTPS con TLS 1.2 o superior en todos los tramos (app ↔ backend, backend ↔ ERP). **Excepción:** por túnel ese tramo va cifrado por WireGuard hacia una dirección privada fijada y el certificado del ERP no se valida — detalle en aski.dev/seguridad, sección 6.
- **En reposo:** la clave o API Key del ERP se cifra con AES-256-GCM antes de guardarse.
- **Cuentas:** contraseñas almacenadas como hash bcrypt; sesiones con tokens firmados.
- **Dispositivo:** almacenamiento cifrado con clave gestionada por Android Keystore.

Accesos y detección

- El acceso operativo a la base de datos está restringido a un número mínimo de administradores y se audita.
- Los intentos de inyección SQL o de manipulación del modelo se detectan antes de llegar a la IA y quedan registrados.
- Las peticiones de campos sensibles conocidos y de modelos restringidos se rechazan.
- El corte de acceso no depende de Aski: basta desactivar la clave o el usuario de servicio en el propio ERP.

Lo que esto no significa: la clave con la que se cifran las credenciales vive en el servidor, porque el backend necesita descifrarlas para abrir la conexión al ERP. Como operador de la plataforma, el acceso técnico existe. Preferimos declararlo antes que dejar entender otra cosa.

Solo lectura por defecto, y acciones con confirmación

Por defecto, las únicas operaciones que el sistema emite contra el ERP son de consulta, y sobre SAP S/4HANA es así siempre. La excepción son las **acciones con confirmación**: requieren activación explícita y existen en Enterprise Plus, en los planes SAP y en los Dedicated, sobre Odoo y SAP Business One. No son escritura libre — el sistema solo sabe ejecutar un catálogo cerrado de diez operaciones sobre un registro concreto (recordatorio de cobro, suelto o a los clientes de una lista; actividad de seguimiento, marcarla hecha o reprogramarla; aprobar o rechazar un documento; cambiar el responsable; marcar una oportunidad ganada o perdida — sobre Business One solo las dos primeras), nada se ejecuta sin confirmación explícita del usuario, y cada ejecución queda registrada con quién la pidió, qué se hizo y con qué datos exactos. Lo que queda fuera de ese catálogo se corta antes de tocar el ERP. Hay una escritura más, fuera de ese catálogo: si al programar un aviso el usuario elige recibirlo en la bandeja de su propio Odoo, cada entrega crea ahí un mensaje de notificación dirigido a él, sin tocar ningún registro de negocio. Los permisos y reglas de registro configurados en el ERP siguen mandando; Aski no abre ninguna puerta nueva. El detalle completo, en aski.dev/seguridad.

Qué recibe el modelo de inteligencia artificial

Para redactar la respuesta en lenguaje natural, Anthropic recibe la pregunta, el esquema del ERP (nombres de modelos y campos) y un extracto acotado de los registros que devolvió esa consulta: **hasta 20 filas por respuesta en modo normal y hasta 80 filas por consulta en Análisis profundo**. Ese extracto puede contener información del negocio, como nombres de clientes o importes. **Nunca se envía la base de datos completa ni las credenciales**. Anthropic retiene ese contenido hasta 30 días únicamente para detección de abuso, según sus términos, y no lo usa para entrenar modelos. Aski tampoco lo usa para entrenar nada.

Retención y borrado

Mientras la cuenta está activa se conservan el perfil, las credenciales cifradas, el historial de mensajes y el de facturación. La eliminación desde la app es inmediata y permanente, exige confirmación y volver a autenticarse, y borra historial de chat, credenciales, vocabulario aprendido, sesiones, tokens y el registro de seguridad asociado. Dos matices: el historial de facturación se conserva cinco años por normativa tributaria peruana, con el correo anonimizado; y una cuenta eliminada puede permanecer en copias de seguridad hasta 30 días, hasta que esas copias caduquen.

Lo que no tenemos

Declarado por nosotros, para que no aparezca como hallazgo de auditoría

- **No hay certificación SOC 2 ni ISO 27001.**
- **El pentest publicado es propio**, ejecutado y grabado por nosotros; no es la auditoría de un tercero independiente.
- **No se ofrece alojamiento en la Unión Europea** ni residencia de datos por región: toda la infraestructura está en Estados Unidos.

Responsable del tratamiento de datos: Jhon Jairo Rojas Ortiz · Perú · contacto@aski.dev

Respondemos consultas de seguridad y solicitudes de acuerdos en un máximo de 7 días hábiles. Si el auditor tiene un cuestionario, se responde por escrito.

Documentos de referencia: aski.dev/seguridad · aski.dev/privacy · aski.dev/terms