Onsites AI

LIBRO BLANCO DE SEGURIDAD · EDICIÓN 2.0

Seguridad y residencia de datos

Quién custodia los datos, por escrito

Cifrado, control de acceso, auditoría, plazos de copia y borrado, límites de datos de la IA y notificación de incidentes: cada punto con lo que hacemos y quién es responsable. Sin adjetivos que no se puedan verificar.



Versión
Edición 2.0

Publicado
Noviembre de 2026

Se aplica a
Nube · Nube privada · Autoalojado

ID del documento
ONS-SC-ES-2.0

© 2026 Onsites AI · Se regenera con cada versión; la edición más reciente en onsitesai.com/download.html

Contenido

01 **Roles de encargado y límites de los datos** Quién controla, quién trata, a qué llega la IA 03

02 **Cifrado, acceso y auditoría** Cómo se implementan los nueve controles 04

03 **Residencia, copias y ciclo de vida** Dónde están los datos, cuánto duran y cómo se borran 05

04 **Cuestionario y notificación** Respuestas cortas, reporte de vulnerabilidades, contactos 06

Resumen

Onsites AI trata los datos de los clientes como datos en custodia. Tanto los despliegues en la nube como los autoalojados tienen cifrado, control de acceso y registros de auditoría; en autoalojado, todo puede quedarse dentro de su propia red. Este documento describe cómo se implementa cada uno de los nueve controles y dice con claridad qué parte es de cada lado, porque la parte difícil de una revisión de seguridad rara vez es una carencia: es un límite mal definido.

9 controles	**TLS 1.3**	**1** día laborable	**3** despliegues
Incorporados, mapeables a un cuestionario	En tránsito en todas partes; también cifrado en reposo	Para acusar recibo de un informe de seguridad	Nube, nube privada, límites del autoalojado

Los nueve controles de un vistazo

01 TRANSPORTE
TLS 1.3

02 EN REPOSO
Medios de almacenamiento cifrados

03 CLAVES
Guardadas aparte de los datos

04 USUARIOS
Roles, restringibles a solo lectura

05 AISLAMIENTO
Los espacios de trabajo no se ven entre sí

06 COMPARTICIÓN
Enlaces con caducidad y límite de aperturas

07 AUDITORÍA
Quién, cuándo, qué cambió

08 COPIAS
Automáticas en planes de pago, exportables

09 LÍMITE DE IA
Solo este espacio de trabajo, sin entrenamiento

PROPÓSITO

Para revisiones de seguridad, cuestionarios de proveedores y comprobaciones de cumplimiento. Utilizable como anexo de una presentación.

SE APLICA A

SaaS en la nube, nube privada y autoalojado. Donde el comportamiento difiere, se señala la diferencia.

DECLARACIÓN

Describe el comportamiento incorporado del producto; no es una certificación de terceros. Las auditorías independientes se encargan por separado.

COMENTARIOS

Edición 2.0, noviembre de 2026. Correcciones e informes de seguridad: support@onsitesai.com.

01

ROLES Y LÍMITES

Quién controla, quién trata, qué puede ver la IA

La primera pregunta de cualquier revisión de seguridad es sobre roles: de quién son los datos, quién los trata y si ese tratamiento los entrega a alguien más. Nuestro reparto es simple: el cliente es el responsable, nosotros somos el encargado, y los únicos subencargados son la infraestructura y los modelos, que cambian según el despliegue.

1.1 Tres roles

Responsable

El cliente

Decide qué se recoge, cuánto tiempo se conserva y quién puede verlo. Los usuarios, los roles y los permisos son suyos de configurar; la exportación y el borrado son suyos de activar.

Encargado

Onsites AI

Trata los datos según la configuración: los guarda, los recupera, redacta y emite documentos. No se usan para fines propios ni se reutilizan entre espacios de trabajo.

Subencargados

Infraestructura y modelos

En la nube: nuestra infraestructura y los servicios de modelo que llamamos. En autoalojado: los aporta el cliente y nosotros no custodiamos ninguno.

1.2 Cuatro puntos de límite en una sola llamada de IA

Dentro

Datos del espacio de trabajo

Hilos, cuentas, documentos, pedidos. Visibles solo para los miembros de este espacio de trabajo, según su rol.

En la recuperación

Filtro de permisos

El contexto se recorta a lo que puede ver el usuario que pregunta; los registros que no puede abrir nunca entran en la ventana.

En la inferencia

Contexto mínimo

Solo lo que necesita esta tarea. El autoalojado puede apuntar a un endpoint interno para que nada salga de la red.

En la devolución

Respuesta con fuentes

Cada afirmación cita el registro que la sostiene. Nada se escribe en un conjunto de entrenamiento ni se reutiliza en otro sitio.

Figura 1-1 Cuatro puntos por los que podrían filtrarse datos y qué lo impide en cada uno. Quite cualquiera de ellos y el límite deja de sostenerse, y por eso las fuentes son obligatorias y no opcionales.

1.3 Cuatro reglas bajo las que trabaja la IA

- **Solo este espacio de trabajo.** Copilot, Harness, Agent Studio y Desk leen el espacio de trabajo actual y nada más, en todos los despliegues.
- **Fuentes en cada respuesta.** Si una afirmación no se puede rastrear hasta un hilo, un campo o un archivo, no se escribe en la respuesta.
- **Sin entrenamiento.** Los datos de clientes no entrenan modelos compartidos ni públicos. En autoalojado, el modelo y la clave son suyos por defecto.
- **Se puede apagar.** La IA se puede desactivar para un espacio de trabajo o un miembro; el resto del producto sigue funcionando sin degradarse.

1.4 Cómo cambian los roles según el despliegue

En la nube y en la nube privada operamos la infraestructura y gestionamos las claves de los modelos; la instancia privada fija su región en el aprovisionamiento. En autoalojado el cliente es dueño de los hosts, el endpoint, las claves y el almacenamiento, y puede funcionar totalmente sin conexión. Los controles son idénticos: solo cambia quién aporta la capa inferior.

> **«¿Puede su personal ver nuestras conversaciones?»** En la nube, el soporte puede ver registros redactados y detalles de errores mientras diagnostica; el cuerpo de las conversaciones y los adjuntos no son material habitual de soporte. Si eso no es aceptable, el autoalojado elimina la pregunta por completo.

02

CONTROLES

Nueve controles y cómo se implementa cada uno

Los cuestionarios preguntan control por control, así que este capítulo responde en el mismo orden: cifrado, acceso, registros, compartición e IA. Cada fila dice lo que hacemos y quién lo hace, que es lo que un evaluador comprueba de verdad.

2.1 Cifrado y claves

Fase	Implementación	Responsable
En tránsito	TLS 1.3 de extremo a extremo; en autoalojado, TLS termina en su proxy con su certificado	Nosotros en la nube; el cliente en autoalojado
En reposo	Cifrado en nuestro almacenamiento; en sus discos, lo gestiona su sistema operativo o su capa de almacenamiento	Nosotros en la nube; el cliente en autoalojado
Claves	Guardadas aparte de los datos; solo el personal de la plataforma	Nosotros en la nube; el cliente las custodia en autoalojado
Copias	Los archivos de copia también están cifrados; el destino depende del despliegue	Véase el capítulo 3

2.2 Control de acceso

- **Por usuario y rol.** Lo que ve una persona depende de su usuario y su rol; cualquier rol se puede restringir a solo lectura para finanzas o dirección.
- **Aislamiento de espacios de trabajo.** Los espacios de trabajo no se ven entre sí; los datos no se mueven entre ellos y la recuperación de la IA hereda el mismo límite.
- **Revocación inmediata.** Retirar un usuario revoca su acceso al instante.
- **Controles de compartición.** Archivos y carpetas privados compartidos por público; los enlaces públicos pueden llevar caducidad y límite de aperturas, y revocarse en cualquier momento.

2.3 Auditoría

Los cambios de estado en documentos y conversaciones registran el operador, la hora y el detalle: quién envió un presupuesto, quién cambió un importe, quién confirmó un contrato. El registro se exporta con el resto de los datos, así que meses después sigue sirviendo como prueba de aprobación en lugar de vivir en un flujo de actividad que se desplaza. Las acciones de Desk se registran igual: lo que leyó, lo que escribió y cuántos créditos gastó.

2.4 Dónde quedan los controles en el recorrido



Figura 2-1 Los controles a lo largo del recorrido. Recorrer estos cuatro tramos en una revisión encuentra huecos más rápido que recorrer la lista de funciones.

Cómo verificarlo Pida una muestra redactada de cada cosa: un cambio de estado, un cambio de permisos y un registro de ejecución de la IA. Una muestra vale más que una casilla marcada en un cuestionario.

03

RESIDENCIA

Dónde están, cuánto duran, cómo se borran

La residencia suele ser tres preguntas en una: qué región guarda los datos, cuánto se conservan las copias y qué pasa al terminar. Las dos primeras las decide el despliegue; la tercera depende de si usted exportó.

3.1 Ciclo de vida de un registro



Creado

Escrito en el espacio de trabajo

Conversaciones, cuentas, documentos y archivos llegan al espacio de trabajo y son visibles según los permisos.

En uso

Lectura y escritura diarias

El equipo y la IA trabajan sobre el mismo registro; cada escritura queda registrada con quién la hizo.

Copiado

Copia cifrada

Los espacios de trabajo de pago en la nube se copian automáticamente; el autoalojado ejecuta el script incluido y guarda los medios.

Exportado / terminado

Retirado o borrado

Exportación en formato estándar; borrado a petición, con copias que caducan según la política de retención.

Figura 3-1 Cuatro etapas. La que conviene acordar por adelantado es la última: quién activa el borrado y cuánto sobreviven las copias.

3.2 Residencia y copias por despliegue

Despliegue	Ubicación de los datos	Copia	Borrado
SaaS en la nube	Nuestra infraestructura	Automática en los planes de pago	A petición; las copias caducan según la política
Nube privada	Instancia y región de copia elegidas en el aprovisionamiento	Automática, en la misma región	Como arriba, sin cambiar de región
Autoalojado	Su centro de datos o nube privada	Script incluido con la licencia	Lo ejecuta usted; nosotros aportamos los pasos y la lista de comprobación

La región se fija en el aprovisionamiento y no cambia después; mover de región se gestiona como una instancia nueva.

3.3 Exportación, bajada de plan y retención

- **La exportación es un derecho, no un interruptor.** Conversaciones, contactos y documentos salen en formatos estándar: sin formatos cautivos y sin cuota.
- **Bajar de plan no borra.** Quitar un paquete o un plan conserva los datos; no se purgan por exceso de cuota.
- **Los espacios gratuitos no tienen copia en el servidor.** La exportación programada es su única copia.
- **El borrado se confirma.** Entregamos un registro de ejecución y la fecha de caducidad de las copias.

3.4 Cómo fijar la retención

Datos	Sugerencia	Motivo
Conversaciones y cuentas	Mientras dure el negocio	La posventa y la recompra dependen del hilo.
Presupuestos, contratos, facturas	Según la normativa fiscal	Normalmente más tiempo que las conversaciones; los números y las versiones deben poder revisarse.
Registro de auditoría	Más tiempo que los documentos	Las aprobaciones y las discrepancias necesitan «quién cambió qué y cuándo».
Copias de seguridad	Menos tiempo que los datos vivos	Las copias existen para restaurar, no para archivar; la caducidad evita disputas al borrar.

Ponga tres fechas en el contrato ① los días de exportación tras la baja; ② la retención de las copias; ③ el plazo para confirmar el borrado por escrito. Resuelven más que una casilla marcada.

04

CUESTIONARIO

Respuestas cortas y cómo notificar una vulnerabilidad

Las filas de abajo son las preguntas que aparecen en casi todas las revisiones de proveedor. Las respuestas se pueden citar tal cual; para cualquier otra cosa, envíe su cuestionario y lo rellenaremos en su formato en lugar de contestar con un folleto.

4.1 Preguntas habituales

Pregunta	Respuesta
¿Se usan los datos de clientes para entrenar modelos?	No. La IA solo lee este espacio de trabajo y no se usa para entrenar modelos compartidos ni públicos; en autoalojado el modelo se queda dentro de su red.
¿Podemos elegir dónde se almacenan los datos?	La nube privada elige la instancia y la región de copia en el aprovisionamiento. La nube usa una región estándar; el autoalojado está donde estén sus hosts.
¿Puede su personal leer las conversaciones de los clientes?	En la nube, el soporte puede ver registros redactados mientras diagnostica; el cuerpo de las conversaciones y los adjuntos no son material habitual de soporte. Para una separación más estricta, elija autoalojado.
¿Guardan registros de auditoría y podemos exportarlos?	Sí. Los cambios de estado, los cambios de permisos y las ejecuciones de IA registran quién, cuándo y qué; todo se exporta con sus datos.
¿Se pueden limitar y revocar los enlaces de archivos?	Sí. Comparta por público, fije una caducidad y un límite de aperturas, y revoque en cualquier momento.
¿Qué pasa con los datos cuando nos vamos?	Exportación en formato estándar; borrado a petición con un registro de ejecución y la fecha de caducidad de las copias.
¿Se puede limitar el gasto en IA?	Sí. Un tope blando avisa y continúa; un tope duro detiene las llamadas de IA en el umbral mientras el resto del producto sigue.

4.2 Notificar una vulnerabilidad

Paso 01

Notifique

Escriba a support@onsitesai.com; llega al equipo que construye el producto afectado.

Paso 02

Acuse de recibo

En un día laborable, con una evaluación inicial y un contacto con nombre.

Paso 03

Corrección

Programada según la gravedad, con el progreso compartido durante el trabajo y no solo en la entrega.

Paso 04

Cierre

Hallazgos y las acciones que correspondan al cliente, resumidos; una lista de comprobación si necesita actuar.

Figura 4-1 Vía de notificación. No hay programa de recompensas por errores, pero quien informa aparece acreditado salvo que pida lo contrario.

4.4 Documentos relacionados

Documento	ID del documento	Uso
Manual de producto	ONS-PM-ES-2.0	Productos, alcance, opciones de despliegue, precios (21 páginas).
Guía de despliegue autoalojado	ONS-SH-ES-2.0	Viabilidad, arquitectura, requisitos, coste (6 páginas).
Seguridad y residencia de datos	ONS-SC-ES-2.0	Este documento, para cuestionarios y revisiones (6 páginas).

Contacto Seguridad y cumplimiento: support@onsitesai.com — acuse de recibo en un día laborable.
Documentos: onsitesai.com/download.html · Evaluación de autoalojado: onsitesai.com/self-host