



CENTRO DE CONFIANZA

Política de privacidad

Qué datos trata Igniten, para qué, con quién los comparte, cuánto los conserva y cómo se ejercen los derechos sobre ellos

Versión	Fecha	Vigencia	Acceso	Contacto
1.0	25 de septiembre de 2026	Desde la disponibilidad general	Documento público	security@igniten.io

Vigencia. Este documento describe el servicio Igniten tal como se presta desde su disponibilidad general. Entra en vigor en la fecha en que la plataforma esté disponible comercialmente y rige para cada Cliente desde que celebra el contrato. Hasta entonces se publica solo con fines informativos y no genera obligaciones para ninguna de las partes.

Quién es responsable y cómo contactarnos

Esta política la emite Igniten, sociedad de responsabilidad limitada (LLC) constituida en el Estado de Wyoming, Estados Unidos de América («Igniten»).

La protección de los datos personales se rige por la norma imperativa que corresponde a cada titular: para los titulares en la República Argentina, la Ley 25.326 de Protección de los Datos Personales y su reglamentación, bajo el control de la Agencia de Acceso a la Información Pública (AAIP); y el Reglamento General de Protección de Datos de la Unión Europea (RGPD) cuando resulta aplicable. Esa protección no se renuncia ni se limita por el lugar de constitución de Igniten.

Para qué	Buzón
Consultas y pedidos sobre datos personales y privacidad	security@igniten.io
Reportar una vulnerabilidad o un incidente de seguridad	security@igniten.io
Soporte y avisos	security@igniten.io

La forma de reportar una vulnerabilidad se publica en <https://igniten.io/well-known/security.txt>, con el formato RFC 9116 .

1. A quién le habla este documento

Hay que separar tres situaciones, porque de esa separación depende casi todo lo demás:

- **El Cliente** es la empresa u organización que contrata el servicio. **Es quien decide** qué datos entran al sistema. Sobre esos datos, el Cliente es el responsable del tratamiento e Igniten es el encargado: los trata sólo para prestar el servicio y siguiendo las instrucciones del Cliente, en los términos del Acuerdo de tratamiento de datos.
- **La persona usuaria** es quien usa el producto dentro de esa organización.
- **La persona que visita el sitio igniten.io**, que puede no tener ninguna relación con un Cliente. Lo que se trata en el sitio está en la sección 12.

Igniten es además responsable de los datos que trata por cuenta propia: las cuentas de acceso al panel, los datos de facturación, las comunicaciones de soporte y los datos del sitio web.

Los datos que el sistema trata por cuenta del Cliente son de la organización, y llegan porque la organización lo decidió. Si usted es una persona usuaria y quiere saber por qué sus correos o sus mensajes están accesibles a través de esta herramienta, la respuesta es que **su organización conectó**

esa fuente, y las preguntas sobre esa decisión se responden ahí. Este documento explica qué hace el sistema con esos datos una vez que llegan.

2. Qué datos se recogen

2.1 Datos que el Cliente conecta

El sistema no elige qué recoger: recoge lo que el Cliente conecta, y no puede leer más de lo que los permisos concedidos por el Cliente habilitan. Las categorías, según las fuentes que el servicio admite:

- Correo electrónico: contenido, remitentes, destinatarios y adjuntos.
- Mensajería: mensajes de canales y conversaciones.
- Archivos y documentos, y su contenido.
- Calendario: eventos, participantes y disponibilidad.
- Transcripciones de reuniones.
- Conversaciones y campañas de LinkedIn.
- Registros del CRM del Cliente.
- Datos de las bases de datos que el Cliente conecte.
- Identidad de las personas usuarias y su pertenencia a grupos, desde el directorio del Cliente.
- **Las preguntas que se hacen en el producto y las respuestas que da.**
- Notas de voz enviadas al asistente: se transcriben y el audio se descarta; se conserva sólo el texto.

El sistema no clasifica ni distingue categorías especiales de datos. Si las fuentes que el Cliente conecta las contienen, es una decisión del Cliente sobre qué conecta.

2.2 Datos que Igniten trata por cuenta propia

- **Cuentas del panel:** nombre, correo y la identidad con que la persona inicia sesión. Cada persona tiene usuario y contraseña propios en el servicio de identidad de AWS (Cognito), con segundo factor obligatorio. En el plan Empresa, el acceso puede además federarse contra el proveedor de identidad corporativo del Cliente. La contraseña la custodia ese servicio de identidad; Igniten no la recibe ni la almacena en sus propios sistemas.
 - **Facturación:** el correo de facturación, el plan, los importes, las fechas y el estado de cada cobro. Los datos de la tarjeta los recibe directamente el procesador de pagos y no pasan por Igniten.
 - **Soporte:** lo que la persona escribe al pedir ayuda y nuestras respuestas.
 - **Sitio web:** lo descrito en la sección 12.
-

3. Para qué se usan, y con qué base

Los datos que el Cliente conecta se usan para prestar el servicio: buscar, responder preguntas, generar consultas y visualizaciones, y ejecutar las acciones que la persona usuaria pida y confirme. La base legal de ese tratamiento la determina el Cliente como responsable; Igniten lo realiza como prestación de servicios de tratamiento por cuenta de terceros (artículo 25 de la Ley 25.326).

Los datos propios de Igniten se usan:

- para dar acceso al panel y operar la cuenta, en ejecución del contrato con el Cliente;
- para registrar el consumo y facturar, en ejecución del contrato y en cumplimiento de obligaciones fiscales y contables;
- para responder pedidos de soporte, en ejecución del contrato;
- para medir y mejorar el sitio web: la analítica con cookies, sólo con el consentimiento de quien visita el sitio (sección 12).

Lo que no se hace:

- **Los datos de un cliente no se usan para entrenar modelos.** Igniten no entrena ni ajusta ningún modelo: usa modelos de terceros a través de su interfaz de programación, y contrata a sus proveedores de modelos bajo términos de retención cero y sin entrenamiento.
 - **No se venden datos.**
 - **No se cruzan datos entre clientes.** La separación la aplica el motor de base de datos (sección 6), no sólo el código de la aplicación.
 - **No se usan los datos para publicidad,** ni en el producto ni en el sitio.
-

4. Con quién se comparten

Acá está la respuesta que casi nadie escribe con precisión.

4.1 Proveedores de modelos de lenguaje

Para responder una pregunta, el sistema **envía texto a proveedores de modelos de lenguaje que son empresas distintas de Igniten**. Viaja el fragmento de contenido necesario para resolver la petición en curso —la pregunta, los fragmentos pertinentes de los documentos y correos indexados y, cuando hace falta, la estructura de las bases de datos conectadas— más las instrucciones del sistema. **No viaja el índice, ni el histórico, ni contenido de otras personas de la organización que no sea pertinente a esa consulta.**

Los proveedores de modelos están **nombrados uno por uno en la Lista de sub-procesadores**, con qué recibe cada uno.

- **El Cliente puede bloquear un proveedor para su organización** en todas las funciones generativas. El bloqueo no requiere una instalación distinta ni tiene un precio distinto.

- **Las incrustaciones vectoriales** que sostienen la búsqueda se generan con un único proveedor, común a todas las organizaciones, y se almacenan en la infraestructura de Igniten, no en la del proveedor.

4.2 Proveedores de fuentes y canales

Los proveedores de las fuentes y canales que el Cliente conecta —por ejemplo, Microsoft 365, Google Workspace, Slack o WhatsApp— reciben datos **porque son de donde vienen o hacia donde van los mensajes**. No se les envía nada que no sea de esa conversación o de esa fuente.

4.3 Infraestructura, identidad y cobro

- **Amazon Web Services (AWS)**: la nube donde corre el servicio, incluidos la base de datos, las claves, los respaldos, el correo transaccional y el servicio de identidad (Cognito).
- **Un procesador de pagos**, para el cobro de la suscripción.
- **Vercel y Google Analytics 4**, sólo para el sitio web público (sección 12). No reciben datos que los clientes procesen en el producto.

La lista completa de terceros, con qué recibe cada uno, para qué y en qué región, está en la **Lista de sub-procesadores**. Igniten avisa con 30 días corridos de anticipación antes de incorporar uno nuevo.

4.4 Autoridades

Igniten sólo entrega datos a una autoridad cuando una norma o una orden competente lo exige. Si se trata de datos del Cliente, se lo avisa antes de entregarlos, salvo que la ley lo prohíba.

5. Cuánto tiempo se guardan

Qué	Cuánto
El texto de las preguntas y respuestas enviadas al modelo, en el registro de llamadas al modelo	30 días , y vence solo
Los números de consumo (tokens y costo)	Mientras la cuenta esté activa; se borran en la baja
El contenido indexado y el resto de los datos del Cliente	Mientras la cuenta esté activa, con la profundidad de histórico que la organización configure. En la baja se destruye su clave y se purgan
El log de auditoría de las consultas y acciones del producto	Mientras la cuenta esté activa; se borra en la baja
El registro de los accesos del personal de Igniten y de los cambios de estado de la cuenta	365 días en los sistemas activos. Además se escribe en almacenamiento inalterable, donde nadie, ni siquiera Igniten, puede borrarlo ni acortar su retención
El archivo de «Exportar mis datos»	7 días en el almacenamiento de Igniten; después se elimina

Qué	Cuánto
Los respaldos	14 días. Tras la baja, el contenido que contienen es indescifrable (sección 8)
Lo que respalda lo facturado: suscripción, cobros y datos de facturación	7 años desde el cierre del ejercicio de la baja, conforme a la normativa fiscal y contable de los Estados Unidos
La constancia de la baja	6 años
Datos del sitio web	Según la sección 12

De lo que se conserva después de la baja **se quitan los datos personales que no hacen falta**: se anulan el correo de facturación y el de quien aceptó las condiciones de la clave propia, y de cada cobro se conservan sólo el identificador, el importe, la moneda, la fecha, el estado y el concepto.

El vencimiento de los 30 días **se fija en cada registro en el momento de crearlo**. La consecuencia conviene decirla: **cambiar la política más adelante no reescribe lo ya guardado**.

Una orden judicial o de una autoridad competente que exija conservar datos **suspende** los vencimientos mientras dure, sólo respecto de lo alcanzado por esa orden.

6. Cómo se protegen

- **Separación entre organizaciones aplicada por el motor de base de datos**: seguridad a nivel de fila en cada tabla, en modo forzado, con políticas separadas por operación. El rol con que se conecta la aplicación no es propietario de ninguna tabla, y una consulta sin el contexto de la organización devuelve cero filas, no todas.
- **Cifrado de sobre por organización**: cada organización tiene su propia clave de datos, versionada, que se guarda cifrada con **la clave maestra propia de esa organización**, en un servicio gestionado de claves respaldado por módulo de hardware. La clave de datos se desenvuelve en memoria sólo el tiempo necesario y nunca se guarda desenvuelta. Si un dato llegara por error a un contexto ajeno, el descifrado falla, en vez de devolver un texto incorrecto.
- **Cifrado autenticado en la capa de aplicación** sobre el contenido: mensajes, conversaciones, preguntas y respuestas, consultas generadas, texto de los documentos indexados, resúmenes, credenciales de integración y tokens. Debajo, el volumen de almacenamiento está cifrado con una clave de titularidad de Igniten.
- **Lo que no está cifrado con la clave de la organización, y se dice**: títulos, nombres de archivo, nombres de personas, fechas, nombres de tablas y columnas, y **los vectores de búsqueda**. No es un olvido: la búsqueda por texto opera sólo sobre esos metadatos, y un vector cifrado no se puede comparar por similitud. El contenido cifrado nunca se indexa para búsqueda de texto.
- **Las direcciones de correo de las listas de acceso** no se guardan en claro: se guarda un resumen calculado con la clave de la organización, que permite comparar permisos sin poder leer la dirección.
- **Control de acceso por elemento**: cada elemento indexado conserva la lista de identidades que podían verlo en el sistema de origen, y toda lectura se filtra contra esa lista. Si la identidad de quien

pregunta no se puede determinar, el resultado es vacío.

- **Cifrado en tránsito** con TLS en todo trayecto, incluido el tráfico entre los servicios internos de Igniten, con verificación de certificado.
- **Nadie de Igniten tiene acceso permanente a los datos.** El acceso es excepcional: se solicita con justificación escrita, se otorga por un plazo acotado y vence solo. Cada acceso genera un aviso a los administradores de la organización, queda en un registro inalterable y es visible en el panel del Cliente.
- **Controles bloqueantes en el desarrollo:** revisión obligatoria de cada cambio por una segunda persona, detección de secretos, análisis estático de seguridad y análisis de dependencias.
- **Incidentes:** ante un incidente de seguridad que afecte datos personales del Cliente, Igniten se lo notifica sin demora indebida y a más tardar dentro de las **72 horas** desde que toma conocimiento, en los términos del Acuerdo de tratamiento de datos.

7. Qué se registra del uso

- Un **log de auditoría por organización**, de sólo agregado, sin caminos de modificación ni de borrado en la aplicación.
- Un **registro de los accesos del personal de Igniten** y de los cambios de estado de la cuenta, que se escribe en almacenamiento inalterable, visible para el Cliente en su panel y exportable, a pedido, a su propio sistema de vigilancia.
- Un **registro de las llamadas al modelo:** qué modelo, cuántos tokens, cuánto costó, y el texto, que vence a los 30 días. En la baja del Cliente se borra entero.
- Registros técnicos de operación.

Ese registro de llamadas es de Igniten y vive en su propia base. Es una decisión deliberada: un almacén de trazas de un tercero guardaría preguntas y respuestas de todos los clientes fuera de las capas de separación, y sería el único lugar del sistema donde los datos de todos conviven. **Un registro propio hereda la separación y no agrega un proveedor más.**

8. Derechos

8.1 Qué derechos tiene

Toda persona puede ejercer, respecto de sus datos personales, los derechos de **acceso, rectificación, actualización y supresión** que reconoce la Ley 25.326, y además los de **oposición, limitación del tratamiento y portabilidad**, en los términos del RGPD cuando resulte aplicable.

- **Acceso:** se responde dentro de los **10 días corridos** desde el pedido. Es gratuito si se ejerce con intervalos no menores a seis meses, salvo que se acredite un interés legítimo para hacerlo antes.
- **Rectificación, actualización y supresión:** se resuelven dentro de los **5 días hábiles** desde el pedido.

La Agencia de Acceso a la Información Pública (AAIP), en su carácter de órgano de control de la Ley 25.326, tiene la atribución de atender las denuncias y reclamos que interpongan quienes resulten afectados en sus derechos por incumplimiento de las normas vigentes en materia de protección de datos personales.

8.2 Cómo se ejercen

- **Si sus datos llegaron porque su organización conectó una fuente**, el pedido va a su organización, que es la responsable de esos datos. Igniten la asiste y responde dentro de los plazos de arriba. Si el pedido llega a Igniten, se lo deriva a la organización sin demora.
- **Si se trata de datos que Igniten trata por cuenta propia** (cuentas del panel, facturación, soporte o el sitio web), escriba a security@igniten.io. Igniten puede pedir que acredite su identidad antes de responder.

8.3 Con qué cuenta el sistema

- **Exportación completa** de los datos de la organización, en autoservicio desde el panel, en formato legible, con la opción de exportar los datos de una persona concreta para atender el pedido de un titular.
- **Baja de una persona**: se detiene la captura de sus fuentes, se revocan sus accesos y se revoca su autorización ante el proveedor, con constancia de las fechas.
- **Baja del Cliente**, con constancia.
- **Consulta del registro de accesos** desde el panel.

El sistema no suprime a pedido un documento, un mensaje u otro elemento individual. La supresión se ejerce por estos mecanismos, e Igniten asiste a la organización dentro de ellos y de los plazos de arriba:

- **Supresión en el origen**: la organización suprime el dato en su propio sistema de origen, que es el que administra.
- **Desconexión de una fuente**: borra del sistema el contenido indexado de esa fuente.
- **Baja de una persona y baja del Cliente**, descriptas arriba y en la sección 8.4.

8.4 Hasta dónde llega el borrado

Se dice con precisión porque es lo que más se malinterpreta. Al dar de baja un Cliente, primero se ofrece la exportación, se detiene la captura y se revocan las credenciales ante cada proveedor. Después actúan dos mecanismos, con dos plazos:

- **El contenido se vuelve indescifrable de inmediato**, porque se destruye la clave maestra de la organización. Alcanza a todos los respaldos sin necesidad de reescribirlos: sin la clave, esos datos no se pueden leer. Incluye las direcciones de correo de las listas de acceso.
- **Los metadatos y los vectores de búsqueda**, que no están cifrados con esa clave, se eliminan por procedimiento de los sistemas activos de inmediato, y terminan de desaparecer cuando vence el último respaldo que los contenía, a los 14 días.

La constancia que se entrega indica los dos mecanismos con su fecha. Preferimos explicarlo así antes que afirmar un borrado total instantáneo, que nadie que conserve respaldos puede cumplir.

9. Dónde viven los datos

Igniten es una entidad de los Estados Unidos y trata los datos en ese país. El servicio corre sobre Amazon Web Services, en la región Norte de Virginia (us-east-1), con una réplica sincrónica en una segunda zona de disponibilidad de la misma región. Cada uno de los demás sub-procesadores trata los datos en la región que determina según sus propias condiciones; la Lista de sub-procesadores remite a cada uno.

Las transferencias internacionales de datos personales se amparan:

- desde la República Argentina, en las cláusulas contractuales modelo aprobadas por la AAIP, conforme al artículo 12 de la Ley 25.326 y su reglamentación;
 - desde el Espacio Económico Europeo, cuando resulta aplicable el RGPD, en las cláusulas contractuales tipo aprobadas por la Comisión Europea.
-

10. Menores

El producto es una herramienta de trabajo, dirigida a personas que trabajan en la organización Cliente. **No está dirigido a menores y no los identifica.** El sitio web tampoco está dirigido a menores.

11. Cambios en esta política

Cuando cambie esta política, Igniten publica la versión nueva con su fecha y avisa con **30 días corridos** de anticipación, por correo a los administradores de cada Cliente, indicando qué cambia. Los cambios exigidos por una norma o por una autoridad pueden aplicarse en el plazo que esa norma o autoridad fije.

Cuando cambie el conjunto de proveedores, esta política y la Lista de sub-procesadores cambian con él. Esa lista se deriva de forma automática de la configuración del producto, de modo que un proveedor nuevo no puede incorporarse sin figurar antes en ella.

12. Sitio web igniten.io y cookies

Esta sección se refiere sólo al sitio público igniten.io, no al producto.

12.1 Alojamiento

El sitio lo aloja **Vercel**, que recibe las solicitudes de quienes lo visitan para poder servir las páginas.

12.2 Analítica de visitas

El sitio usa **Google Analytics 4** para medir visitas y uso: qué páginas se ven y con qué elementos se interactúa. Para eso usa cookies de analítica (`_ga` y `_ga_*`).

- **Sólo con su consentimiento.** Al entrar al sitio se muestra un aviso de cookies con dos opciones, «Aceptar» y «Rechazar». Hasta que usted acepta, Google Analytics no se carga y no se guarda ninguna de sus cookies. Si rechaza, no se cargan.
- **Puede cambiar su elección en cualquier momento** desde el enlace «Preferencias de cookies» del pie de página.
- **Su elección se guarda en su propio navegador**, para no volver a preguntarle en cada visita.
- **La base legal de esta analítica es su consentimiento.** Retirarlo no afecta la licitud de la medición hecha mientras estuvo vigente.
- **Las funciones publicitarias están desactivadas:** el almacenamiento publicitario está denegado y Google Signals está apagado.
- **A Google Analytics no se le envían datos personales** como direcciones de correo ni los textos que una persona escribe en el sitio.
- Los datos de analítica se conservan **14 meses**.

Además, el sitio usa la **analítica web de Vercel**, que mide el uso de forma agregada y **sin cookies**. El sitio funciona igual acepte o rechace las cookies de analítica.

12.3 Formulario de acceso a la beta

Si deja su correo en el formulario de acceso a la beta, Igniten lo guarda en su CRM **sólo para contactarlo** por ese motivo. No se usa para otros fines ni se comparte con terceros. Se conserva hasta que pida que se elimine, escribiendo a security@igniten.io, o hasta que deje de ser necesario para ese fin.

12.4 Demostración del asistente

El texto que se escribe en la demostración del asistente se envía a un proveedor de modelos de lenguaje de la Lista de sub-procesadores sólo para generar la respuesta, y responde sobre datos ficticios. Ese proveedor trata el texto según sus propias condiciones. Igniten no guarda ese texto ni lo asocia a la persona. Para contar cuántas preguntas se hicieron, el sitio guarda un contador en el almacenamiento local del propio navegador. Le recomendamos no escribir datos personales ni información confidencial en la demostración.

12.5 Contratación

La página de contratación carga el formulario de pago del procesador de pagos. Los datos de la tarjeta los recibe directamente el procesador y no pasan por Igniten.