



CENTRO DE CONFIANZA

Acuerdo de tratamiento de datos

Las condiciones con que Igniten trata, como encargado, los datos personales que el Cliente conecta al servicio

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.

Partes

Este Acuerdo de tratamiento de datos (el «Acuerdo») se celebra entre:

- **Igniten, sociedad de responsabilidad limitada (LLC) constituida en el Estado de Wyoming, Estados Unidos de América** («Igniten»); y
- la persona jurídica identificada a continuación (el «Cliente»):

Identificación del Cliente	
Razón social	-----
Identificación fiscal	-----
Domicilio legal	-----

Igniten y el Cliente son, en conjunto, las «Partes». Este Acuerdo forma parte del contrato de servicio celebrado entre ellas, integrado por los Términos de servicio y el plan contratado (el «Contrato»). En todo lo referido al tratamiento de datos personales, este Acuerdo prevalece sobre cualquier otra disposición del Contrato.

Definiciones

Los términos siguientes tienen, en este Acuerdo, el significado que se indica:

- **Ley aplicable de protección de datos:** la Ley 25.326 de Protección de los Datos Personales, su Decreto Reglamentario 1558/2001 y las disposiciones y resoluciones de la Agencia de Acceso a la Información Pública (la «AAIP»), su autoridad de control; y, cuando resulte aplicable al tratamiento, el Reglamento (UE) 2016/679 (el «RGPD»).
- **Datos personales:** toda información referida a personas humanas determinadas o determinables que el Cliente conecte al Servicio o que se genere con su uso.
- **Datos del Cliente:** los datos, personales o no, que ingresan al Servicio desde las fuentes que el Cliente conecta, o que las personas usuarias del Cliente producen al usarlo.
- **Titular:** la persona humana a la que se refieren los datos personales.
- **Tratamiento:** toda operación sobre datos personales, automatizada o no, incluidas la recolección, la conservación, la consulta, la comunicación y la supresión.
- **Servicio:** la plataforma de análisis conversacional de Igniten, tal como se describe en el Contrato.
- **Organización:** el espacio del Cliente dentro del Servicio, separado de los de cualquier otro cliente.
- **Sub-procesador:** todo tercero al que Igniten encarga una parte del tratamiento de datos del Cliente.

- **Incidente de seguridad:** toda violación de la seguridad que ocasione la destrucción, pérdida, alteración, comunicación o acceso no autorizados a datos del Cliente.
 - **Lista de sub-procesadores:** el documento publicado por Igniten en su centro de confianza, igniten.io/confianza, que identifica a cada sub-procesador, qué datos recibe y para qué.
-

1. Roles, objeto e instrucciones

1.1 Roles de las Partes

El Cliente es el **responsable del tratamiento**: decide qué fuentes conecta, qué datos ingresan al Servicio, con qué finalidad y qué personas de su organización acceden.

Igniten es el **encargado del tratamiento** en los términos del artículo 25 de la Ley 25.326 y, cuando aplique, del artículo 28 del RGPD. Igniten trata los datos del Cliente **únicamente para prestar el Servicio** y por cuenta del Cliente.

Igniten actúa como responsable sólo respecto de los datos de la relación comercial con el Cliente (datos de contacto, de facturación y de cobro), que se rigen por su Política de privacidad y no por este Acuerdo.

1.2 Objeto

Este Acuerdo regula las condiciones del tratamiento que Igniten realiza por cuenta del Cliente. La naturaleza, la finalidad, las categorías de datos y de titulares y la duración del tratamiento se describen en el Anexo I.

1.3 Instrucciones del Cliente

Igniten trata los datos del Cliente siguiendo sus instrucciones documentadas. El Contrato, este Acuerdo y la configuración que el Cliente establece en el Servicio constituyen esas instrucciones. En concreto, el Cliente las expresa:

- al elegir qué fuentes conecta y qué permisos concede en cada una;
- al retirar un permiso o desconectar una fuente, desde el Servicio o desde la consola de administración de su propio proveedor;
- al bloquear, para su Organización, a un proveedor de modelos listado como sub-procesador (cláusula 3.3);
- al confirmar, o no, cada operación con efecto externo que el asistente propone (cláusula 1.4).

Si Igniten considera que una instrucción infringe la ley aplicable de protección de datos, lo informa al Cliente sin demora y puede suspender su ejecución hasta que el Cliente la confirme o la modifique.

Igniten no trata los datos del Cliente para fines propios, no los vende ni los cede, y no los comunica a terceros salvo a los sub-procesadores de la cláusula 3 o cuando una norma o una orden de autoridad competente lo exija. En este último caso, y si la ley lo permite, Igniten avisa al Cliente antes de hacerlo.

1.4 Operaciones con efecto externo

Toda operación con efecto fuera del Servicio —enviar un correo, crear un evento, escribir en un sistema del Cliente— se genera primero como borrador y no llega al proveedor correspondiente sin la confirmación explícita de una persona autorizada del Cliente. Un borrador sin confirmar vence. No existe una vía de ejecución que omita esa confirmación.

2. Datos que se tratan

2.1 Alcance

El Servicio trata lo que el Cliente conecta. El alcance lo fija el Cliente al conceder permisos en sus proveedores de correo, documentos, mensajería y demás fuentes, y el Servicio no puede leer más de lo que esos permisos habilitan. Las aplicaciones que conectan el Servicio con esos proveedores se registran en el directorio de la organización del Cliente y a su nombre, de modo que el Cliente revoca el consentimiento desde su propia consola, sin intervención de Igniten.

Las categorías de datos y de titulares se detallan en el Anexo I.

2.2 Datos sensibles

El Servicio no clasifica ni distingue datos sensibles en el sentido del artículo 2 de la Ley 25.326 o categorías especiales en el sentido del artículo 9 del RGPD. Si las fuentes que el Cliente conecta contienen esos datos, el Cliente garantiza que cuenta con la base legal para su tratamiento y que la conexión es compatible con sus propias obligaciones. Igniten aplica a esos datos las mismas medidas de seguridad que al resto de los datos del Cliente, descriptas en el Anexo II.

2.3 Obligaciones del Cliente

El Cliente declara que los datos personales que conecta al Servicio fueron obtenidos lícitamente, que informó a los titulares en los términos del artículo 6 de la Ley 25.326 cuando correspondía, y que cuenta con base legal suficiente para encargar su tratamiento a Igniten.

3. Sub-procesadores

3.1 Autorización general

El Cliente autoriza a Igniten a recurrir a los sub-procesadores identificados en la Lista de sub-procesadores vigente a la fecha de firma. La Lista indica, para cada uno, qué datos recibe y con qué finalidad, y nombra de a uno a los proveedores de modelos.

3.2 Obligaciones frente a cada sub-procesador

Igniten impone a cada sub-procesador, por contrato, obligaciones de protección de datos no menos exigentes que las de este Acuerdo, y responde ante el Cliente por su cumplimiento como si se tratara de un incumplimiento propio.

3.3 Bloqueo de un proveedor de modelos

El Cliente puede bloquear, para su Organización, a cualquier proveedor de modelos de la Lista. El bloqueo alcanza a todo el procesamiento generativo de la Organización: ninguna solicitud de la Organización se envía a un proveedor bloqueado. Si el proveedor bloqueado es el que el Servicio usa por defecto para una función, el Servicio usa otro proveedor habilitado del plan; si no queda ninguno habilitado para esa función, la función no se ejecuta y el Servicio lo informa, sin reemplazar el resultado.

La generación de representaciones vectoriales (incrustaciones), que sostiene la búsqueda semántica, la realiza un único proveedor para todos los clientes, identificado en la Lista, y no admite bloqueo por Organización. Si el Cliente objeta a ese proveedor, se aplica lo previsto en la cláusula 3.4 para los sub-procesadores que no pueden bloquearse.

3.4 Nuevos sub-procesadores

Igniten avisa al Cliente con **al menos 30 días de anticipación** antes de incorporar un sub-procesador nuevo o de ampliar los datos que recibe uno existente. El aviso se envía por correo a las personas administradoras de la Organización y se refleja en la Lista publicada, e indica quién es el sub-procesador, qué datos recibirá y para qué.

Dentro de ese plazo, el Cliente puede objetar la incorporación por motivos razonables vinculados a la protección de datos. La objeción se ejerce **bloqueando al sub-procesador para la Organización del Cliente**, de modo que no reciba datos de ella.

Si por su función el sub-procesador no puede bloquearse para una sola Organización, Igniten lo informa en el aviso. En ese caso, y si las Partes no acuerdan una alternativa dentro del plazo de preaviso, el Cliente puede terminar el Contrato sin penalidad antes de que la incorporación surta efecto, con reintegro de la parte proporcional de lo abonado por el período no utilizado.

4. Seguridad de los datos

4.1 Obligación general

Igniten adopta las medidas técnicas y organizativas necesarias para garantizar la seguridad y la confidencialidad de los datos del Cliente, en los términos del artículo 9 de la Ley 25.326 y de las medidas de seguridad recomendadas por la AAIP. Esas medidas se describen en el Anexo II, en términos de mecanismo y de lo que cada una garantiza.

4.2 Actualización de las medidas

Igniten puede actualizar las medidas del Anexo II siempre que el nivel de protección resultante no sea inferior al descripto. Toda modificación que reduzca ese nivel requiere el consentimiento previo y por escrito del Cliente.

4.3 Personal de Igniten

Igniten garantiza que las personas autorizadas a tratar datos del Cliente están sujetas a una obligación de confidencialidad, legal o contractual, que subsiste después de terminada su relación con Igniten, conforme al artículo 10 de la Ley 25.326.

Ninguna persona de Igniten tiene acceso permanente a los datos del Cliente. El acceso excepcional para soporte o emergencia se rige por el Anexo II, sección 7: se solicita con justificación escrita, se otorga por un período acotado, vence solo, se le avisa al Cliente en el momento y queda registrado en el panel del Cliente.

5. Retención

Mientras el Contrato esté vigente, Igniten conserva los datos del Cliente durante el tiempo necesario para prestar el Servicio, con los plazos específicos siguientes:

Qué	Plazo
Texto de las solicitudes a los proveedores de modelos y de sus respuestas, registrado para la operación del Servicio	30 días desde su creación. El vencimiento se fija en cada registro al crearlo
Datos de consumo (cantidad de solicitudes y su costo), sin contenido	Mientras el Contrato esté vigente; se suprimen con la baja
Audio de las notas de voz	No se conserva: se transcribe y se descarta. Se conserva el texto, cifrado como el resto del contenido
Capturas de pantalla enviadas al asistente de configuración de integraciones	No se conservan: se procesan en la solicitud y se descartan
Resto de los datos del Cliente	Mientras el Contrato esté vigente; con la baja, borrado conforme a la cláusula 6
Exportación de los datos generada a pedido del Cliente	7 días en el almacenamiento del Servicio, y se suprime al completarse la baja

Después de la terminación del Contrato, Igniten conserva únicamente lo siguiente, cada cosa con su plazo y minimizada:

Qué	Plazo	Motivo
Registro de accesos de soporte y de cambios de estado de la Organización (quién accedió, cuándo, con qué justificación; quién suspendió la cuenta y por qué)	365 días	Rastro de seguridad y auditoría
Registros de lo facturado: suscripción, cobros, cierres mensuales y datos de facturación	7 años, conforme a la normativa fiscal y contable de los Estados Unidos	Obligación legal
Constancia de la baja: fechas del borrado y registro de la clave destruida	6 años	Prueba del cumplimiento de este Acuerdo

Lo que se conserva se minimiza: con la baja se anulan las direcciones de correo de facturación, y de cada cobro se guardan sólo el identificador del pago, el importe, la moneda, la fecha, el estado y el concepto. Igniten no recibe ni conserva datos de medios de pago.

Una orden de conservación emitida por autoridad judicial o administrativa competente suspende las purgas y el borrado que alcance, sólo en la medida y por el plazo que esa orden disponga. Igniten informa al Cliente de la orden cuando la ley lo permite.

6. Borrado

6.1 Baja de una persona usuaria

A pedido del Cliente, o cuando el Cliente retira a una persona de su directorio, Igniten ejecuta la baja de esa persona en este orden:

1. Se detiene la captura de contenido de las fuentes asociadas a esa persona. Va primero porque la captura no debe seguir trayendo contenido de quien ya no tiene acceso.
2. Se revocan sus concesiones de acceso dentro del Servicio.
3. Se revoca, ante cada proveedor, la autorización delegada que la persona había otorgado, y se registran la fecha del pedido de revocación y la de su confirmación por el proveedor.

6.2 Borrado de la Organización

Al terminar el Contrato, o antes a pedido del Cliente, Igniten borra los datos de la Organización en este orden, y deja constancia de cada paso con su fecha:

1. **Exportación.** Igniten pone a disposición del Cliente la exportación completa de sus datos (cláusula 12.1).
2. **Corte de la ingesta** de todas las fuentes de la Organización.
3. **Revocación** de las autorizaciones delegadas ante cada proveedor.
4. **Destrucción de la clave.** La clave maestra propia de la Organización se deshabilita de inmediato y se elimina en forma irreversible. Desde ese momento, todo el contenido cifrado de la Organización —

incluido el que está en los respaldos— es indescifrable, porque sin esa clave no hay forma de obtener las claves de datos que lo protegen. Alcanza también a las direcciones de correo de las listas de acceso, que se guardan como resumen calculado con esa clave y no en claro.

5. **Purga** de todos los registros de la Organización en todos los sistemas activos del Servicio, incluidos el registro de solicitudes a proveedores de modelos, los metadatos que se guardan sin cifrar (títulos, nombres de archivo, fechas) y las representaciones vectoriales, que no pueden cifrarse sin perder la búsqueda semántica. Se conserva sólo lo indicado en la cláusula 5 para después de la terminación.
6. **Constancia**, entregada al Cliente, con las dos fechas: la de destrucción de la clave y la de purga de los sistemas activos, más la fecha en que vence el último respaldo que contenía los metadatos y las representaciones vectoriales.

6.3 Respaldos

Los respaldos se conservan durante **14 días**. Ese plazo se comunica al contratar y rige para el borrado: los metadatos sin cifrar y las representaciones vectoriales de la Organización terminan de desaparecer cuando vence el último respaldo que los contenía; el contenido cifrado, en cambio, es indescifrable en los respaldos desde la destrucción de la clave. Igniten no restaura datos de una Organización borrada.

7. Asistencia al Cliente en el ejercicio de derechos

7.1 Obligación de asistencia

Igniten asiste al Cliente, con medidas técnicas y organizativas apropiadas, para que el Cliente responda a los pedidos de los titulares en ejercicio de sus derechos de acceso, rectificación, actualización y supresión (artículos 14 a 16 de la Ley 25.326) y, cuando aplique el RGPD, de los demás derechos que ese reglamento reconoce.

7.2 Plazos

Igniten entrega al Cliente la información o ejecuta la medida pedida dentro de plazos que le permitan cumplir los de la Ley 25.326:

- **acceso:** dentro de los **10 días corridos** desde el pedido del Cliente;
- **rectificación, actualización y supresión:** dentro de los **5 días hábiles** desde el pedido del Cliente.

7.3 Medios disponibles

El Servicio ofrece al Cliente los medios siguientes:

- **Acceso:** los datos del Cliente son consultables a través del Servicio, y la exportación puede acotarse a los datos de una persona determinada.
- **Rectificación y actualización:** el contenido se rectifica en el sistema de origen del Cliente, que es donde se genera y del que el Servicio lo toma.
- **Supresión:** el Servicio no suprime a pedido un documento, un mensaje u otro elemento individual. La supresión se ejerce por estos mecanismos:

- la supresión del dato por el Cliente en su sistema de origen, que es el que el Cliente administra;
 - la desconexión de una fuente, que borra del Servicio el contenido indexado de esa fuente;
 - la baja de una persona usuaria, descrita en la cláusula 6.1;
 - el borrado de la Organización completa, con destrucción de su clave y constancia, descrito en la cláusula 6.2.
- **Registro de accesos:** el Cliente ve en su panel quién de Igniten accedió a sus datos, cuándo y con qué justificación.

Igniten asiste al Cliente, dentro de esos mecanismos y de los plazos de la cláusula 7.2, para que responda al pedido del titular.

7.4 Pedidos recibidos por Igniten

Si un titular dirige un pedido directamente a Igniten respecto de datos del Cliente, Igniten lo remite al Cliente sin demora y no lo responde por su cuenta, salvo instrucción del Cliente.

8. Ubicación de los datos y transferencias internacionales

8.1 Ubicación

Igniten es una entidad constituida en los Estados Unidos de América y trata los datos del Cliente en ese país. Los datos del Cliente se almacenan en infraestructura de nube ubicada en los Estados Unidos, región Norte de Virginia (us-east-1). Los demás sub-procesadores los tratan en la región que cada uno determina según sus propias condiciones, como indica la Lista de sub-procesadores.

8.2 Transferencias internacionales

La prestación del Servicio implica la transferencia internacional de datos personales hacia los Estados Unidos, donde Igniten los trata. Esas transferencias se realizan sobre la base de:

- para los datos transferidos desde la República Argentina, conforme al artículo 12 de la Ley 25.326 y a su reglamentación, las **cláusulas contractuales modelo** aprobadas por la AAIP para la transferencia internacional de datos personales, que las Partes incorporan a este Acuerdo por referencia y que Igniten suscribe, a su vez, con cada sub-procesador; y
- para los datos transferidos desde el Espacio Económico Europeo, cuando al tratamiento le resulte aplicable el RGPD, las **cláusulas contractuales tipo** adoptadas por la Comisión Europea mediante la Decisión de Ejecución (UE) 2021/914, en el módulo que corresponda a la relación entre las Partes, que también se incorporan por referencia.

Ante una contradicción entre este Acuerdo y esas cláusulas, prevalecen las cláusulas. A pedido del Cliente, Igniten entrega copia de las cláusulas suscriptas con cada sub-procesador, pudiendo omitir la información comercial que no se refiera a la protección de datos.

9. Continuidad y respaldos

La base de datos del Servicio es gestionada, con réplica sincrónica en una segunda zona de disponibilidad, respaldos automáticos cifrados con una clave de titularidad de Igniten y recuperación a cualquier punto en el tiempo dentro de la ventana de retención de 14 días.

Igniten ensaya periódicamente la restauración, incluida la de una única Organización a partir de un respaldo completo sin afectar los datos de las demás, y conserva el acta de cada ensayo con los tiempos medidos. El Cliente puede solicitar la constancia del último ensayo conforme a la cláusula 11.

10. Incidentes de seguridad

10.1 Aviso al Cliente

Igniten notifica al Cliente todo incidente de seguridad que afecte datos del Cliente **sin demora indebida y a más tardar dentro de las 72 horas** desde que toma conocimiento de él. La notificación se envía por correo a todas las personas administradoras de la Organización.

10.2 Contenido del aviso

La notificación incluye, en la medida en que se conozca:

- la naturaleza del incidente, las categorías y el número aproximado de titulares y de registros afectados;
- las consecuencias probables;
- las medidas adoptadas o propuestas para contenerlo y mitigar sus efectos;
- el nombre y los datos de contacto de la persona de Igniten que coordina la respuesta.

Si no es posible reunir toda la información al mismo tiempo, Igniten la entrega por etapas, sin demorar el primer aviso.

10.3 Respuesta

La respuesta sigue una secuencia definida de antemano: contener, preservar la evidencia antes de limpiar y recién después reparar. Igniten puede suspender una Organización sin afectar a ninguna otra. Los responsables de decidir, redactar y notificar están designados de antemano. Un incidente que exponga datos de una Organización a otra se clasifica siempre con la severidad máxima, cualquiera sea su volumen.

10.4 Cooperación

Igniten coopera con el Cliente para que este cumpla sus propias obligaciones de notificación a la AAIP, a otras autoridades de control y a los titulares. La notificación del incidente no implica reconocimiento de responsabilidad.

10.5 Reporte de vulnerabilidades

Cualquier persona puede reportar una vulnerabilidad a security@igniten.io. La política de divulgación se publica en el centro de confianza y en la ruta `/.well-known/security.txt` del sitio, según el estándar RFC 9116.

11. Auditoría

11.1 Documentación

A pedido del Cliente, Igniten pone a su disposición la información necesaria para demostrar el cumplimiento de este Acuerdo, que comprende:

- las respuestas a cuestionarios de seguridad razonables, y el cuestionario CAIQ Lite ya respondido y publicado en el centro de confianza;
- la documentación técnica de los controles descritos en el Anexo II, incluida la que se entrega bajo acuerdo de confidencialidad;
- los informes de auditoría de terceros independientes, cuando existan. A la fecha Igniten no cuenta con un informe SOC 2; su calendario se publica en el centro de confianza.

11.2 Inspección

Si la documentación no alcanza para demostrar el cumplimiento, o si lo exige una autoridad de control, el Cliente puede realizar una inspección, por sí o por un auditor independiente obligado a confidencialidad, con estas condiciones:

- preaviso escrito no menor a 30 días, salvo que la inspección responda a un incidente de seguridad o a un requerimiento de autoridad;
 - no más de una vez por año calendario, con las mismas excepciones;
 - en horario hábil, con un alcance acordado previamente y sin afectar la operación del Servicio;
 - sin acceso a datos de otras Organizaciones ni a información que comprometa su seguridad;
 - a costo del Cliente.
-

12. Terminación: devolución y borrado

12.1 Devolución

Durante los **30 días** siguientes a la terminación del Contrato, cualquiera sea su causa, el Cliente puede obtener la exportación completa de sus datos desde el panel del Servicio, en un formato estructurado, de uso común y legible por máquina. A pedido del Cliente, Igniten la genera por él.

12.2 Borrado

Vencido ese plazo, o antes si el Cliente lo pide por escrito, Igniten borra los datos del Cliente conforme a la cláusula 6.2 y le entrega la constancia de la cláusula 6.2, paso 6, que indica los dos mecanismos con su fecha y el vencimiento del último respaldo. Esto da cumplimiento al artículo 25, inciso 2, de la Ley 25.326.

Se exceptúa sólo lo que la cláusula 5 enumera para después de la terminación, con su plazo, y lo que una orden de conservación obligue a mantener.

13. Confidencialidad

Igniten trata los datos del Cliente como información confidencial y no los divulga sino en los casos previstos en este Acuerdo. Esta obligación subsiste después de la terminación del Contrato y mientras Igniten conserve cualquier dato del Cliente.

14. Responsabilidad

Cada Parte responde frente a la otra por los daños que le cause el incumplimiento de sus obligaciones bajo este Acuerdo o bajo la ley aplicable de protección de datos. Esa responsabilidad se rige por los límites que establece el Contrato, salvo en caso de dolo o culpa grave, y salvo en la medida en que una norma imperativa disponga otra cosa.

Cada Parte responde frente a los titulares y a las autoridades de control conforme a la ley aplicable.

15. Vigencia y modificaciones

15.1 Vigencia

Este Acuerdo entra en vigor en la fecha de su firma y rige mientras Igniten trate datos del Cliente, aun después de terminado el Contrato.

15.2 Modificaciones

Igniten puede modificar este Acuerdo con un aviso de **30 días** a las personas administradoras de la Organización. Si el Cliente no acepta la modificación, puede terminar el Contrato antes de que entre en vigor, sin penalidad. Una modificación exigida por una norma o por una autoridad de control puede regir en un plazo menor, cuando esa norma o autoridad lo impongan.

15.3 Nulidad parcial

Si una disposición de este Acuerdo fuese declarada inválida, el resto conserva su validez, y la disposición inválida se reemplaza por la válida que mejor refleje su finalidad.

16. Ley aplicable y jurisdicción

Este Acuerdo se rige por las leyes del Estado de Wyoming, Estados Unidos de América. Toda controversia derivada de él se somete a los tribunales del Estado de Wyoming.

Lo anterior no afecta la protección de los datos personales, que se rige en todo caso por la norma imperativa que corresponda al titular: la Ley 25.326, su reglamentación y la competencia de la AAIP para los titulares en la República Argentina, y el RGPD cuando resulte aplicable. Esa protección no puede renunciarse ni limitarse por la elección de ley o de jurisdicción de este Acuerdo.

Si una norma imperativa del país del Cliente le reconoce el derecho a litigar ante otra jurisdicción, esa norma prevalece sobre esta cláusula.

17. Contactos

Para qué	Dirección
Reportar una vulnerabilidad o un incidente de seguridad	security@igniten.io
Consultas y pedidos sobre datos personales y privacidad	security@igniten.io
Avisos y notificaciones del Cliente a Igniten	security@igniten.io

Las notificaciones de Igniten al Cliente se envían a las personas administradoras de la Organización registradas en el Servicio. Todas las del Cliente a Igniten, incluidas las de incidentes de seguridad y los pedidos sobre datos personales, se envían a security@igniten.io.

Firmas

En prueba de conformidad, las Partes firman este Acuerdo en la fecha indicada.

	Por Igniten	Por el Cliente
Razón social	Igniten, sociedad de responsabilidad limitada (LLC) constituida en el Estado de Wyoming, Estados Unidos de América	_____
Nombre de quien firma	_____	_____
Cargo	Managing Member	_____
Firma		
Fecha		

Anexo I · Descripción del tratamiento

Naturaleza y finalidad

Igniten trata los datos del Cliente para prestar el Servicio: capturar el contenido de las fuentes conectadas, indexarlo, responder las preguntas de las personas usuarias del Cliente con base en ese contenido y en las bases de datos que el Cliente conecta, y preparar las operaciones con efecto externo que el Cliente confirme.

Duración

Mientras el Contrato esté vigente, y después sólo con los plazos de las cláusulas 5, 6 y 12.

Categorías de titulares

- Personas usuarias del Servicio en la organización del Cliente.
- Empleados, contratistas y demás integrantes de la organización del Cliente cuyos datos figuren en las fuentes conectadas.
- Terceros cuyos datos figuren en esas fuentes: remitentes y destinatarios de correos, participantes de reuniones y conversaciones, contactos, clientes y proveedores del Cliente.

Categorías de datos

Categoría	De dónde ingresa
Correo electrónico: contenido, remitentes, destinatarios y adjuntos	Servicios de correo corporativo que el Cliente conecta
Mensajería: mensajes de canales y conversaciones	Plataformas de mensajería que el Cliente conecta
Archivos y documentos	Servicios de almacenamiento de documentos que el Cliente conecta
Calendario: eventos, participantes y disponibilidad	Servicios de calendario que el Cliente conecta
Transcripciones de reuniones	Servicios de grabación de reuniones que el Cliente conecta
Conversaciones y campañas en redes profesionales	Herramientas de prospección que el Cliente conecta
Registros de gestión de clientes	El sistema de gestión de clientes del Cliente
Datos de las bases de datos del Cliente	Las bases que el Cliente conecta
Identidad de las personas usuarias: nombre, dirección de correo y pertenencia a grupos	Los directorios del Cliente
Preguntas y respuestas, en texto o por nota de voz	El uso del Servicio

Los proveedores concretos de cada categoría se identifican en la Lista de sub-procesadores.

Anexo II · Medidas técnicas y organizativas

Este anexo describe cada control por su mecanismo y por lo que garantiza. La documentación técnica ampliada se entrega conforme a la cláusula 11.

1. Separación entre Organizaciones

- La separación la aplica el motor de base de datos, no sólo la aplicación: seguridad a nivel de fila activada en cada tabla, en modo forzado (`FORCE ROW LEVEL SECURITY`), de modo que ni el propietario de la tabla evade las políticas.
- El rol con el que la aplicación se conecta no es propietario de ninguna tabla; las migraciones corren con un rol distinto.
- Las políticas están separadas por operación, con verificación en las de escritura: no puede insertarse una fila atribuida a otra Organización.
- El identificador de la Organización se fija por transacción, como parámetro y nunca por interpolación de texto. Una consulta sin ese contexto devuelve cero filas, no todas.
- El agrupador de conexiones opera en modo transacción, de modo que el contexto de una solicitud no alcanza a la siguiente.
- El conjunto de tablas protegidas se deriva del catálogo de la base, y una comprobación automática rechaza cualquier tabla sin política.
- Una batería de pruebas dedicada intenta cruzar la separación en cada punto de acceso —lectura por identificador directo, escritura atribuida a otra Organización, sesión de una sobre el dominio de otra, descifrado con la clave equivocada—, y ningún punto de acceso nuevo se aprueba sin su prueba de aislamiento.

2. Cifrado

- **En tránsito:** TLS en todo trayecto, incluido el tráfico entre los servicios internos, con verificación de certificado. La base de datos y la memoria intermedia rechazan conexiones sin cifrar.
- **En reposo, primera capa:** cifrado del volumen con una clave de titularidad de Igniten, no la clave por defecto del proveedor de nube.
- **En reposo, segunda capa:** cifrado autenticado en la capa de aplicación, con estructura de sobre. Cada Organización tiene su propia clave maestra, en un servicio gestionado de claves respaldado por módulo de hardware, creada al dar de alta la Organización. Esa clave maestra cifra la clave de datos de la Organización, y la clave de datos cifra el contenido: mensajes y conversaciones, preguntas y consultas generadas, resultados, texto de los documentos indexados y sus fragmentos, resúmenes, credenciales de integración, autorizaciones delegadas y el detalle del registro de auditoría.
- La clave de datos se descifra en la memoria del proceso sólo durante el tiempo necesario y nunca se guarda descifrada. Las claves están versionadas, de modo que rotarlas no exige interrumpir el Servicio.

- Si un dato de una Organización llegara a un contexto ajeno, el descifrado falla de forma explícita: no devuelve texto incorrecto ni datos parciales.
- Un acceso al almacenamiento, a un respaldo o a una réplica no alcanza para leer el contenido.
- **Clave maestra en la cuenta del Cliente:** en el plan Empresa, la clave maestra de la Organización puede residir en la propia cuenta de nube del Cliente. Igniten la usa, pero no la posee: si el Cliente revoca el permiso, Igniten pierde el acceso a sus datos en el acto; si el Cliente borra esa clave, sus datos no se recuperan, ni siquiera desde un respaldo.

3. Lo que queda sin cifrar, y por qué

Qué	Por qué
Títulos de documentos y nombres de archivo	Se muestran y se buscan por texto
Nombres de tablas y columnas de las bases del Cliente	Son la base sobre la que el asistente razona para escribir la consulta
Fechas y marcas de tiempo	Se usan para ordenar y filtrar
Nombres de participantes	Se muestran y se buscan
Representaciones vectoriales (incrustaciones)	Una representación cifrada no puede compararse por similitud; cifrarla anularía la búsqueda semántica

La búsqueda por texto opera exclusivamente sobre esos metadatos en claro. El contenido cifrado nunca se indexa para búsqueda de texto. Estos datos se eliminan por procedimiento en el borrado (cláusula 6.2, paso 5).

4. Control de acceso al contenido

- Cada elemento indexado conserva la lista de identidades que podían verlo en el sistema de origen, y toda lectura se filtra contra esa lista en la base de datos.
- El control cierra ante la duda: si el conjunto de identidades de quien pregunta está vacío, el resultado es cero.
- La pertenencia a grupos se deriva del lado del servidor; lo que se afirme desde el cliente sobre sus propios grupos se descarta.
- Las direcciones de correo de esas listas no se guardan en claro: se guarda un resumen calculado con la clave de la Organización, que permite comparar sin poder leer.

5. Credenciales de integración

Se almacenan cifradas y son de sólo escritura: la interfaz de administración no puede devolverlas y sólo expone metadatos y los últimos cuatro caracteres. Los registros de auditoría guardan la referencia y la longitud de la credencial, nunca su valor. Los secretos de operación se guardan en un gestor de secretos gestionado, y cada servicio recibe sólo los que necesita.

6. Identidad y sesión de las personas usuarias

- Las personas usuarias del panel se autentican en el servicio gestionado de identidad de Igniten, con usuario y contraseña propios y segundo factor obligatorio. En el plan Empresa, el Cliente puede además federar el acceso contra su propio proveedor de identidad corporativo, con intercambio de código y clave de prueba.
- El proveedor de identidad autentica; nunca autoriza. Los permisos se resuelven contra el padrón de la Organización por el par Organización y dirección de correo, nunca por la dirección sola.
- Las cookies de sesión son seguras, inaccesibles desde el navegador, con envío entre sitios restringido y ligadas al dominio exacto. La sesión se regenera al iniciar.

7. Acceso del personal de Igniten

- Nadie en Igniten tiene acceso permanente a los datos de producción ni credenciales de producción asignadas.
- El acceso excepcional se solicita con justificación escrita, se otorga por un período acotado y vence solo. Cuando hay una segunda persona disponible, la concesión requiere su aprobación; cuando no, el acceso vence igual, se registra igual y se avisa igual.
- Cada concesión genera en el momento un aviso por correo a todas las personas administradoras de la Organización, y queda visible en su panel.
- Una conciliación automática compara los accesos efectivamente ocurridos con las concesiones registradas; un acceso sin concesión dispara una alerta y el aviso al Cliente.
- Hay separación de funciones: quien despliega el Servicio no puede leer datos del Cliente.
- El registro de accesos se escribe en almacenamiento con bloqueo de objeto en modo cumplimiento: ni la cuenta administradora de Igniten puede borrarlo ni acortar su retención. A pedido del Cliente, Igniten exporta ese registro a un sistema del propio Cliente.

8. Contenido con instrucciones ocultas

- Cada elemento pasa, antes de indexarse, por un evaluador dedicado que detecta instrucciones dirigidas al asistente; el veredicto se guarda con el elemento. Los criterios del evaluador no se publican y se comparten bajo acuerdo de confidencialidad.
- El contenido marcado se neutraliza antes de entrar al contexto del asistente, por cualquier camino de búsqueda.
- El análisis de planillas no ejecuta código: sólo admite las construcciones de consulta de una lista cerrada, corre con el acceso externo apagado, en memoria y por solicitud, dentro de un proceso aislado sin red, con sistema de archivos de sólo lectura y sin credenciales.
- Ninguna operación con efecto externo se ejecuta sin confirmación humana (cláusula 1.4).

9. Acceso a las redes internas del Cliente

- Cuando una base de datos del Cliente está dentro de su red, la conexión la establece un conector que el Cliente instala y que abre la sesión hacia Igniten, nunca al revés, sobre TLS con autenticación mutua por certificado y sin puertos de entrada abiertos.

- Cada conector tiene su propio certificado, revocable individualmente, y su propio canal aislado dentro de la infraestructura de Igniten.
- La lista de destinos alcanzables es un archivo que vive en la infraestructura del Cliente y que sólo el Cliente edita. Igniten puede solicitar un destino nuevo, pero no concedérselo.
- Igniten no almacena la topología de la red del Cliente.
- El conector se distribuye como imagen firmada y verificable, con inventario de componentes, y el Cliente puede fijar una versión en lugar de aceptar actualizaciones automáticas. Su código no es de acceso público: está disponible para revisión del Cliente, a pedido y bajo acuerdo de confidencialidad.

10. Desarrollo y cambios

- Todo cambio requiere la aprobación de una persona distinta de su autor antes de incorporarse.
- La cadena de integración bloquea un cambio ante la detección de secretos en el historial, hallazgos de análisis estático de seguridad, dependencias con vulnerabilidades conocidas o hallazgos en el escaneo de imágenes.
- Las imágenes se firman y se referencian por su huella, con inventario de componentes; una imagen sin firma verificable no se despliega.
- Las cuentas del personal de Igniten exigen segundo factor.

11. Continuidad, detección y respuesta

- Base de datos gestionada con alta disponibilidad, respaldos cifrados y recuperación a un punto en el tiempo (cláusula 9), con restauración de una sola Organización ensayada.
- Detección de amenazas y alertas sobre la infraestructura, con aviso a las personas responsables.
- Procedimiento de respuesta a incidentes con responsables designados y corte por Organización (cláusula 10).