

Contrato de encargo del tratamiento

AI Services LLC (OpenWAF) · Versión 2026-10-27. Publicado en <https://openwaf.dev/es/legal/encargo-de-tratamiento/>. Se acepta electrónicamente en el alta, sin firma por separado (apartado 1).

En resumen

- Para el tráfico de tus sitios web, tus zonas DNS y los demás datos del Anexo I, tú eres el responsable del tratamiento y nosotros tu encargado (art. 28 RGPD), y tu proveedor de servicios según la CCPA/CPRA.
- Solo tratamos esos datos siguiendo tus instrucciones, que son la configuración que fijas mediante el panel, la API, la CLI o el servidor MCP.
- Los datos se quedan en la Unión Europea: Alemania (Hetzner) y, para el nodo de borde de Madrid, España (Vultr). Nuestros subencargados figuran en el Anexo III y en la página de [Subencargados](#).
- Te avisaremos de cualquier violación de la seguridad de los datos personales sin dilación indebida y, en todo caso, en un plazo de 72 horas desde que tengamos conocimiento de ella.
- Las transferencias fuera del EEE se amparan en las cláusulas contractuales tipo de la UE (módulos 2 y 3), incorporadas en el apartado 9, y en el Addendum del Reino Unido.
- Los eventos de seguridad caducan a los 30 días; tus datos se borran en los 30 días siguientes al cierre de tu cuenta y de las copias de seguridad en un máximo de 6 meses.

1. Partes e incorporación

Este Contrato de encargo de tratamiento («Contrato») se celebra entre el cliente que usa OpenWAF Cloud (el «Cliente»), como responsable del tratamiento, y AI Services LLC, con nombre comercial OpenWAF, 99 Wall Street #2351, New York, NY 10005, EE. UU. («OpenWAF»), como encargado del tratamiento. Forma parte de las [Condiciones de servicio](#) y se celebra cuando el Cliente lo acepta en el alta, marcando su casilla antes de que se cree la organización del Cliente, sin necesidad de firmarlo por separado. OpenWAF registra la versión aceptada (identificada por su fecha, actualmente 2026-10-27), el usuario que lo acepta y la fecha y hora de la aceptación. Si el Cliente es una agencia que actúa por cuenta de sus propios clientes, el Cliente actúa como encargado de ellos y OpenWAF actúa como su subencargado en los mismos términos.

2. Objeto, duración, naturaleza y finalidad

- **Objeto:** el tratamiento de datos personales necesario para prestar los servicios de DNS autoritativo, cortafuegos de aplicaciones web (WAF), caché en el borde y servicios relacionados para los dominios y sitios web del Cliente, y la pasarela de Egress IA si el Cliente la activa.
- **Duración:** mientras el Cliente use el servicio y, después, hasta que los datos se borren como se describe en el apartado 10.
- **Naturaleza:** recibir, inspeccionar, filtrar, guardar en caché, reenviar y registrar peticiones HTTP(S) dirigidas a los nombres de host con proxy del Cliente; responder consultas DNS; enviar los correos del control de acceso; recoger mediciones de rendimiento de usuarios reales si se activan; inspeccionar y reenviar a los proveedores que elija el Cliente las peticiones de sus agentes de IA si se activa Egress IA; guardar la configuración del Cliente.

- **Finalidad:** proteger y acelerar los sitios web del Cliente, servir sus zonas DNS y proteger las llamadas salientes de sus agentes de IA, según la configuración del Cliente.

Los detalles figuran en el [Anexo I](#).

3. Instrucciones documentadas

OpenWAF trata los datos personales únicamente siguiendo instrucciones documentadas del Cliente, salvo que la ley le obligue a otra cosa; en ese caso, OpenWAF informará al Cliente antes del tratamiento, salvo que la ley lo prohíba. La configuración que el Cliente fija mediante el panel, la API, la CLI o el servidor MCP, junto con este Contrato y las Condiciones de servicio, constituye las instrucciones del Cliente. OpenWAF avisará al Cliente si, en su opinión, una instrucción infringe la normativa de protección de datos.

El Cliente es responsable de contar con una base jurídica para el tratamiento, de informar a los visitantes de sus sitios web y a las personas que autorice en el control de acceso, y de la licitud de sus instrucciones.

4. Confidencialidad

OpenWAF garantiza que las personas autorizadas para tratar datos personales se han comprometido a respetar la confidencialidad o están sujetas a una obligación legal de confidencialidad adecuada, y que esa obligación subsiste después de terminar su relación.

5. Seguridad

OpenWAF aplica las medidas técnicas y organizativas descritas en el [Anexo II](#), adecuadas al riesgo conforme al artículo 32 RGPD. OpenWAF puede actualizar esas medidas siempre que no se reduzca el nivel general de seguridad. El estado actual de nuestro programa de seguridad se publica en nuestra [página de seguridad](#).

6. Subencargados

El Cliente otorga a OpenWAF una autorización general por escrito para recurrir a los subencargados indicados en el [Anexo III](#), que también se publican en la página de [Subencargados](#). OpenWAF informará al Cliente por correo a los propietarios de la cuenta con al menos 30 días de antelación antes de añadir o sustituir un subencargado. El Cliente puede oponerse en ese plazo por motivos razonables de protección de datos; si las partes no llegan a una solución, el Cliente puede poner fin al servicio. OpenWAF impone por contrato a cada subencargado obligaciones de protección de datos que ofrecen al menos el mismo nivel de protección que este Contrato y sigue respondiendo ante el Cliente de su cumplimiento.

Los proveedores que el propio Cliente elige y contrata, como los proveedores de modelos de IA que configura en Egress IA con sus propias claves de API, o sus propios servidores de origen, no son subencargados de OpenWAF: OpenWAF solo les envía datos por instrucción del Cliente.

7. Asistencia al Cliente

Teniendo en cuenta la naturaleza del tratamiento, OpenWAF ayudará al Cliente, siempre que sea posible:

- a responder a las solicitudes de los interesados que ejerzan sus derechos. Si OpenWAF recibe una solicitud de este tipo directamente, la reenviará al Cliente sin dilación indebida y no la contestará por sí misma, salvo que el Cliente se lo indique;
- a cumplir sus obligaciones de seguridad, notificación de violaciones, evaluaciones de impacto relativas a la protección de datos y consulta previa a la autoridad de control (artículos 32 a 36 RGPD), con la información de la que disponga OpenWAF.

8. Violaciones de la seguridad de los datos personales

OpenWAF notificará al Cliente cualquier violación de la seguridad de los datos personales que afecte a los datos del Cliente sin dilación indebida y, en todo caso, en un plazo de 72 horas desde que tenga conocimiento de ella, por correo a los propietarios de la cuenta. La notificación incluirá, en la medida en que se disponga de ella, la información del artículo 33.3 RGPD: la naturaleza de la violación, las categorías y el número aproximado de interesados y de registros afectados, un punto de contacto, las consecuencias probables y las medidas adoptadas o propuestas. La información que no esté disponible al principio podrá facilitarse por fases. OpenWAF adoptará medidas razonables para contener la violación y mitigar sus efectos, y no informará a terceros de una violación que afecte a los datos del Cliente sin el acuerdo de este, salvo que la ley lo exija.

9. Transferencias internacionales

Los datos del Cliente se guardan y se tratan en la Unión Europea (Alemania y, para el nodo de borde de Madrid, España). Al Services LLC está establecida en Estados Unidos, su personal y sus colaboradores pueden acceder a los datos desde fuera del Espacio Económico Europeo (EEE), y algunos subencargados del Anexo III están establecidos en Estados Unidos. Para cualquiera de esas transferencias:

- las partes incorporan por referencia las [cláusulas contractuales tipo](#) aprobadas por la Decisión de Ejecución (UE) 2021/914 de la Comisión («CCT»): el módulo 2 (de responsable a encargado) cuando el Cliente es responsable y el módulo 3 (de encargado a encargado) cuando el Cliente es encargado. El Cliente es el exportador de datos y OpenWAF el importador;
- en las CCT: se aplica la cláusula 7 (cláusula de incorporación); en la cláusula 9 se aplica la opción 2 (autorización general por escrito), con el plazo de aviso del apartado 6; no se aplica la redacción opcional de la cláusula 11; en la cláusula 17 se aplica la opción 1 y el Derecho aplicable es el español; en la cláusula 18 se eligen los tribunales de España; la autoridad de control competente según la cláusula 13 es la indicada en el Anexo I.C; los Anexos I, II y III de este Contrato completan los anexos de las CCT;
- para los datos sujetos al RGPD del Reino Unido se aplica el Addendum de transferencias internacionales de datos a las CCT emitido por la autoridad británica (Information Commissioner, versión B1.0), completado con la información de este Contrato; para los datos sujetos a la Ley federal suiza de protección de datos, se aplican las CCT con el Comisionado Federal suizo de Protección de Datos e Información como autoridad competente y entendiendo las referencias al RGPD como hechas a esa Ley;
- en caso de contradicción entre este Contrato y las CCT, prevalecen las CCT.

10. Supresión y devolución de los datos

- Los eventos de seguridad, las mediciones de rendimiento de usuarios reales, los informes de bots de IA y los eventos de bloqueo de Egress IA caducan y se borran 30 días después de registrarse.
- Cuando se cierra la cuenta, OpenWAF borra los datos del Cliente de sus sistemas en producción, incluidas su configuración, las direcciones de correo del control de acceso, las claves privadas de los certificados y las claves de proveedor de Egress IA, en un plazo de 30 días, salvo que la ley le obligue a conservarlos. Las copias que haya en las copias de seguridad se borran cuando estas caducan, como máximo 6 meses después, y entretanto no se restauran en los sistemas en producción salvo para recuperarse de un incidente.
- Antes de cerrar la cuenta, el Cliente puede obtener su configuración mediante la API o la CLI, o pedir a OpenWAF en support@openwaf.dev una copia. Si lo solicita, OpenWAF le confirmará el borrado por escrito.

11. Información y auditorías

OpenWAF pondrá a disposición del Cliente la información necesaria para demostrar el cumplimiento del artículo 28 RGPD, incluida una descripción de su programa de seguridad y de su estado, y permitirá y contribuirá a la realización de auditorías, incluidas inspecciones, por parte del Cliente o de un auditor independiente designado por él. Las auditorías requieren un preaviso razonable, corren a cargo del Cliente, están sujetas a confidencialidad, no deben comprometer la seguridad de otros clientes y pueden realizarse una vez al año, salvo que se haya producido una violación de la seguridad de los datos personales o lo exija una autoridad de control. Si en el futuro OpenWAF obtiene un informe de auditoría independiente, el Cliente acepta basarse primero en él, en la medida en que cubra lo que se quiera auditar.

12. Registro de actividades de tratamiento

OpenWAF lleva un registro de las categorías de actividades de tratamiento que efectúa por cuenta de sus clientes, como exige el artículo 30.2 RGPD, y lo pondrá a disposición de la autoridad de control competente cuando lo solicite.

13. Condiciones de proveedor de servicios según la CCPA/CPRA

En la medida en que la California Consumer Privacy Act modificada por la California Privacy Rights Act se aplique a la información personal que OpenWAF trata para el Cliente, OpenWAF actúa como proveedor de servicios del Cliente y no: venderá ni compartirá esa información personal; la conservará, usará ni comunicará para ningún fin distinto de prestar el servicio descrito en el apartado 2, ni fuera de la relación comercial directa con el Cliente; ni la combinará con información personal que reciba de otras fuentes, salvo en lo que permita la ley. OpenWAF cumplirá las obligaciones que le impone la CCPA/CPRA, ofrecerá el mismo nivel de protección de la privacidad que exige la ley y avisará al Cliente si deja de poder cumplirlas. El Cliente puede adoptar medidas razonables para detener y remediar un uso no autorizado. OpenWAF certifica que entiende estas restricciones.

14. Responsabilidad y prelación

La responsabilidad de cada parte según este Contrato se rige por las [Condiciones de servicio](#), en la medida en que la ley lo permita y sin limitar los derechos que las CCT dan a los interesados. En caso de

contradicción entre este Contrato y las Condiciones de servicio sobre el tratamiento de datos personales, prevalece este Contrato.

Anexo I. Detalles del tratamiento

A. Lista de partes

Exportador de datos

El Cliente, identificado en su cuenta (nombre, dirección y correo de contacto del propietario de la cuenta). Papel: responsable o, en el caso de agencias que actúan por cuenta de sus clientes, encargado. Actividades: uso de OpenWAF Cloud para sus dominios y sitios web. Firma y fecha: la aceptación en el alta, registrada como se describe en el apartado 1.

Importador de datos

AI Services LLC (OpenWAF), 99 Wall Street #2351, New York, NY 10005, EE. UU. Contacto: support@openwaf.dev; seguridad: security@openwaf.dev. Papel: encargado o subencargado. Actividades: los servicios descritos en el apartado 2. Firma y fecha: como para el exportador.

B. Descripción del tratamiento

Categorías de interesados

Visitantes de los sitios web del Cliente y usuarios de sus zonas DNS; personas que el Cliente autoriza en el control de acceso; usuarios de los agentes de IA del Cliente, si se activa Egress IA; personal del Cliente y miembros de su cuenta.

Categorías de datos personales

Direcciones IP; metadatos de las peticiones, incluidos el nombre de host, la ruta, el método y cabeceras como el agente de usuario; huella TLS; país y número de sistema autónomo (ASN) derivados de la dirección IP; detalles de los eventos de seguridad (hora, estado, acción, regla, tipo de ataque y mensaje); direcciones de correo del control de acceso y códigos de un solo uso; mediciones de rendimiento de usuarios reales (ruta de la página, métricas de rendimiento, país y clase de dispositivo, sin guardar la dirección IP ni el agente de usuario); clasificación de las peticiones por bots de IA; en Egress IA, el contenido de las peticiones de los agentes de IA del Cliente, inspeccionado en memoria y no guardado, y los eventos de bloqueo (hora, agente, destino, identificadores de detección, dirección IP del cliente, método y ruta, nunca el cuerpo de la petición). Las consultas DNS se tratan para responderlas. Las respuestas de los sitios web del Cliente pueden guardarse en la caché de los nodos de borde según la configuración del Cliente.

Categorías especiales de datos

No se prevén. El servicio no está diseñado para tratar categorías especiales de datos; si el contenido de las peticiones incluye alguno, solo se trata en tránsito o en la caché que configure el Cliente.

Frecuencia

Continúa, mientras se use el servicio.

Conservación

Eventos de seguridad, mediciones de rendimiento de usuarios reales, informes de bots de IA y eventos de bloqueo de Egress IA: 30 días. Configuración y datos de la cuenta: mientras exista la cuenta y hasta 30 días después de su cierre. Copias de seguridad: las de las bases de datos, 90 días; las del sistema, 6 meses como máximo.

Transferencias a subencargados

Las descritas en el Anexo III, durante el tratamiento.

C. Autoridad de control competente

La autoridad de control del Estado miembro de la UE en el que esté establecido el Cliente o, si el Cliente no está establecido en la UE, la Agencia Española de Protección de Datos (AEPD).

Anexo II. Medidas técnicas y organizativas

- **Ubicación:** plano de control, bases de datos, servidores DNS y servidor de correo alojados en la Unión Europea (Hetzner, Alemania); nodos de borde en Alemania (Hetzner) y España (Vultr, Madrid).
- **Cifrado en tránsito:** TLS hacia los visitantes, hacia los orígenes y en los documentos de configuración enviados a los nodos de borde, con intercambio de claves híbrido X25519 + ML-KEM-768 preferente; verificación del certificado del origen (full strict) y TLS mutuo hacia los orígenes cuando el Cliente lo activa.
- **Cifrado en reposo:** claves privadas de los certificados subidos e importados y cuenta ACME cifradas con AES-256-GCM; copias de seguridad de sistemas de ficheros cifradas en origen antes de salir del servidor.
- **Integridad de la configuración:** documentos de configuración firmados con Ed25519, que los nodos de borde verifican antes de usarlos; los nodos siguen sirviendo la última configuración válida si el plano de control no está accesible.
- **Control de acceso:** inicio de sesión sin contraseña (códigos de un solo uso por correo, o cuentas de Google o GitHub con la dirección de correo verificada); sesiones en cookies HttpOnly y Secure con protección CSRF; roles y limitación de miembros y tokens a un cliente o una zona; tokens de API guardados solo como hashes y con caducidad obligatoria (como máximo 365 días); OAuth 2.1 con PKCE para el servidor MCP.
- **Aislamiento entre clientes:** a los datos de un cliente solo se llega a través del ámbito de su propia organización, cubierto por pruebas automáticas entre organizaciones.
- **Gestión de secretos:** claves de proveedor de Egress IA y secretos de la infraestructura guardados en un gestor de secretos dedicado (OpenBao), con roles de mínimo privilegio: el plano de control puede escribir las claves de proveedor pero no leerlas, y la pasarela puede leerlas pero no escribirlas.
- **Gestión de cambios:** versionado de la configuración con historial, comparación y vuelta atrás; motivo obligatorio en cada cambio y registro de auditoría de quién cambió qué, cuándo y por qué.
- **Seguridad de red:** servidor DNS primario oculto, accesible solo para los secundarios públicos; cortafuegos en los servidores y en los proveedores; acceso de administración restringido por reglas de cortafuegos; bases de datos accesibles solo desde nuestros propios servidores.
- **Disponibilidad:** varios nodos de borde con respuestas DNS comprobadas que retiran un nodo caído en cerca de un minuto; dos servidores DNS secundarios en centros de datos distintos; supervisión externa continua de los nodos de borde, el DNS, el plano de control y los certificados, con alertas; copias de seguridad diarias en un almacenamiento separado en la UE.
- **Gestión de vulnerabilidades:** análisis automático diario del código desplegado, las dependencias, las imágenes de contenedor y los paquetes del sistema operativo, priorizado con el catálogo de vulnerabilidades explotadas de CISA (KEV) y EPSS; detección de secretos en la integración continua de nuestro repositorio público de código abierto y antes de cada publicación de este sitio web.
- **Minimización de datos:** caducidad automática de los eventos a los 30 días; sin guardar dirección IP ni agente de usuario en la monitorización de usuarios reales; Egress IA nunca guarda el cuerpo de las peticiones.

- **Organización:** un sistema de gestión de la seguridad de la información alineado con ISO/IEC 27001:2022, con políticas documentadas (control de acceso, criptografía, proveedores, desarrollo seguro, registros, copias de seguridad y continuidad, respuesta a incidentes y gestión de vulnerabilidades), un registro de riesgos y un procedimiento documentado de respuesta a incidentes; acceso limitado a las personas que lo necesitan.

Anexo III. Subencargados

Subencargado	Ubicación	Tratamiento de datos del Cliente
Hetzner Online GmbH	Alemania (UE)	Infraestructura: plano de control, bases de datos, servidores DNS, nodos de borde, servidor de correo (correos del control de acceso) y almacenamiento de copias de seguridad.
The Constant Company, LLC (Vultr)	Madrid, España (UE)	Infraestructura del nodo de borde de Madrid: tráfico de los visitantes dirigidos a ese nodo (terminación TLS, WAF, caché).
Cloudflare, Inc.	EE. UU. (red global)	Proxy de red delante del panel, del servicio del plano de control del que nuestros nodos de borde obtienen su configuración (documentos de configuración, que pueden incluir direcciones de correo del control de acceso y claves privadas de certificados) y del servicio de Egress IA (peticiones de los agentes de IA del Cliente, si lo activa). Cloudflare descifra el contenido en tránsito.
Internet Security Research Group (Let's Encrypt)	EE. UU.	Emisión de certificados TLS. Solo recibe nombres de host.