nonimo

WHITE PAPER DE SEGURIDAD

Seguridad de Nonimo Gateway: white paper para tu DPO

Qué pasa con cada petición que tu empresa manda a la IA a través de Nonimo Gateway, dónde se procesa y qué documentación te queda para el RGPD.

El equipo de Nonimo

Noviembre de 2026

nonimo.eu

WHITE PAPER DE SEGURIDAD

Seguridad de Nonimo Gateway: white paper para tu DPO

Qué pasa con cada petición que tu empresa manda a la IA a través de Nonimo Gateway, dónde se procesa y qué documentación te queda para el RGPD.

El equipo de Nonimo · Noviembre de 2026 · 15 min de lectura

Qué encontrarás dentro

- El resumen de una página para el delegado de protección de datos
- El recorrido de una petición, de tu aplicación al proveedor de IA y de vuelta
- La máquina confidencial en Irlanda: qué es y qué garantiza
- Qué se guarda cifrado, dónde y cuándo se borra el Gateway
- Responsable, encargado y subencargado: el papel de cada parte
- Los artículos del RGPD que toca y la documentación que te deja
- Las preguntas que tu DPO nos puede hacer, con la respuesta corta

En pocas palabras

- Nonimo Gateway sustituye los datos personales por etiquetas antes de que la petición salga hacia el proveedor de IA y los repone en la respuesta.
- Cada cliente tiene su propia máquina confidencial de Microsoft Azure en Irlanda, con la memoria cifrada por el procesador.
- Lo que se guarda (ajustes, la clave del proveedor y tus términos) va cifrado en la misma región. El texto hace el camino y no se queda.
- Nonimo recibe solo cifras. Tu DPO recibe un informe mensual y un registro por petición que sirven para el registro de actividades y la EIPD.

Este documento está pensado para que el delegado de protección de datos (DPD o DPO, como se le suele llamar), quien lleva los sistemas y la asesoría jurídica de una pyme puedan valorar Nonimo Gateway antes de conectarlo a nada.

Cuenta qué le pasa a cada petición que tu empresa manda a un modelo de IA, dónde se procesa, quién puede ver qué, qué se guarda y qué papeles te quedan para el expediente. Se centra en lo que hace el Gateway y en lo que te garantiza.

01

El resumen para tu DPO

Si solo tienes cinco minutos, esto es lo que hay que saber.

Qué hace. Nonimo Gateway se coloca entre las aplicaciones de tu empresa y el proveedor de IA que hayáis elegido (por ejemplo, OpenAI o Claude de Anthropic).

Antes de que salga cada petición, detecta los datos personales (nombres de personas, empresas, documentos de identidad, cuentas bancarias, correos y teléfonos) y los sustituye por etiquetas como `[PERSONA_1]` o `[IBAN_1]`. Cuando llega la respuesta, vuelve a colocar cada dato real en su sitio. Tus usuarios leen un texto normal.

Dónde. En una máquina confidencial de Microsoft Azure dedicada solo a tu empresa, en Irlanda. Su memoria está cifrada por el propio procesador y solo arranca versiones publicadas del Gateway.

Quién ve qué. El proveedor de IA recibe la petición con etiquetas. Tus aplicaciones reciben la respuesta con los datos reales. Nonimo recibe cifras: cuántas peticiones y cuántos datos se han tapado. Lo que procesa tu máquina no lo lee el personal de Nonimo ni el de Microsoft.

Qué se guarda. Tus ajustes, la clave de tu proveedor de IA y los términos que añadas en el panel, cifrados y en la misma región. El texto de las peticiones hace el camino y no se queda.

Cuándo se borra. A los tres días seguidos sin uso durante la prueba (con aviso un día antes), al acabar la prueba sin plan, al acabar la suscripción o cuando lo pidas.

Qué documentos te quedan. Un informe mensual con cifras por tipo de dato y un registro por petición exportable en CSV o JSONL. Ninguno de los dos contiene datos personales. El contrato de encargo del tratamiento se pide en support@nonimo.ai o en hello@nonimo.ai.

02

El recorrido de una petición

Para entender lo que garantiza el Gateway, lo más útil es seguir una petición de principio a fin. Imagina que el equipo de cobros de tu empresa usa una herramienta interna que redacta cartas de reclamación con un modelo de IA.



FIGURA 1

1. Tu aplicación envía la petición a tu Gateway. La conexión va por HTTPS, a una dirección que es solo tuya y con una clave de acceso propia.

Para tu equipo de desarrollo, el cambio es pequeño: el Gateway es compatible con la API de OpenAI (chat completions y responses) y con la de Anthropic (messages). Se cambian la dirección base y la clave; el SDK oficial, los modelos, los mensajes y la lógica de la aplicación se quedan como estaban.

2. El Gateway tapa los datos personales. La frase que escribió la herramienta, `Reclama a Juan Español Español, DNI 00000000X, el recibo devuelto`, sale de tu máquina convertida en `Reclama a [PERSONA_1], DNI [DNI_1], el recibo devuelto`.

Las etiquetas son coherentes a lo largo de toda la conversación: la misma persona lleva la misma etiqueta de principio a fin, y el modelo puede razonar sobre ella sin conocerla.

3. El proveedor de IA responde. Recibe una petición con etiquetas y responde con etiquetas. Lo contratas tú, con tu propia clave, y por eso sus condiciones son las que tengas pactadas con él.

4. El Gateway repone los datos reales. Antes de que la respuesta llegue a tu aplicación, cada etiqueta vuelve a ser el dato que sustituía.

Esto funciona también cuando la respuesta llega por trozos (streaming) y en las llamadas a herramientas (tool calls), que es por donde muchas integraciones pasan datos de un sistema a otro.

5. Nonimo recibe una cifra. Al final del camino, lo único que sale hacia Nonimo es un recuento: una petición más y tantos datos tapados de cada tipo, además de lo necesario para renovar la licencia.

Tú decides qué hace el Gateway con cada tipo de dato: taparlo, detener la petición o solo avisar y contarlo. Así puedes, por ejemplo, tapar nombres y cuentas en todas las herramientas y detener cualquier petición que lleve un documento de identidad en un proceso concreto.

Si tu negocio tiene nombres propios que también conviene proteger (un proyecto, un cliente importante, una marca interna), los añades en el panel como términos y se tapan igual que el resto.

03

Dónde corre: tu máquina confidencial en Irlanda

Cada cliente de Nonimo Gateway en la Unión Europea tiene **su propia máquina confidencial de Microsoft Azure en Irlanda**. La máquina está dedicada a tu empresa y procesa solo sus peticiones, separadas de las de cualquier otro cliente.

«Confidencial» tiene aquí un significado técnico concreto. Azure ofrece contenedores confidenciales basados en **AMD SEV-SNP**, una tecnología pública en la que el procesador cifra la memoria de la máquina mientras trabaja [4].

El efecto práctico es que lo que hay en memoria (las peticiones mientras se procesan) queda cifrado frente al sistema que aloja la máquina. De ahí salen dos compromisos:

- Lo que procesa tu Gateway no lo lee el personal de Nonimo ni el de Microsoft.
- Tu máquina solo arranca versiones publicadas del Gateway. Cada actualización llega como una versión nueva publicada.

Para el expediente de protección de datos, esto se traduce en tres hechos sencillos de documentar: el tratamiento se hace en la Unión Europea (Irlanda), en una máquina dedicada, y con la memoria cifrada por hardware.

> **Nota:** el proveedor de IA que elijas puede tratar la petición en otro lugar, según lo que tengas contratado con él. Lo que le llega va con etiquetas en lugar de los datos personales. Es un punto que conviene reflejar en tu análisis de transferencias, del que hablamos más abajo.

04

Qué se guarda, cómo y cuándo se borra

Un Gateway necesita recordar unas pocas cosas para funcionar de un día para otro. Son estas, y solo estas:

Qué	Dónde y cómo	Quién puede descifrarlo
Tus ajustes (qué hacer con cada tipo de dato)	Cifrado, en la misma región que tu máquina	Solo tu máquina, con una versión publicada del Gateway
La clave de tu proveedor de IA	Cifrada, en la misma región	Solo tu máquina, con una versión publicada
Los términos que añadas en el panel	Cifrados, en la misma región	Solo tu máquina, con una versión publicada
El texto de las peticiones y respuestas	Hace el camino y no se queda	Solo tu máquina, mientras lo procesa
La tabla que une cada etiqueta con su dato real	Vive en la memoria mientras dura la petición y nunca se escribe en disco	Solo tu máquina, mientras lo procesa
Las cifras de uso	En el panel y en el registro por petición	Tú; Nonimo, solo los totales

Lo guardado sobrevive a reinicios y actualizaciones: no tienes que volver a configurar nada cuando sale una versión nueva.

El borrado está atado a la vida del Gateway, y se produce en cuatro situaciones:

1. **Tres días seguidos sin uso durante la prueba.** Te avisamos un día antes, para que puedas evitarlo si lo necesitas.
2. **Fin de la prueba sin plan.** La prueba dura 10 días; si no eliges un plan, el Gateway se borra.
3. **Fin de la suscripción.**
4. **A petición tuya**, en cualquier momento.

Con el Gateway se borra lo que guardaba cifrado. Así tu DPO puede escribir en el registro de actividades un plazo de conservación claro para lo que se guarda y otro, inmediato, para el texto.

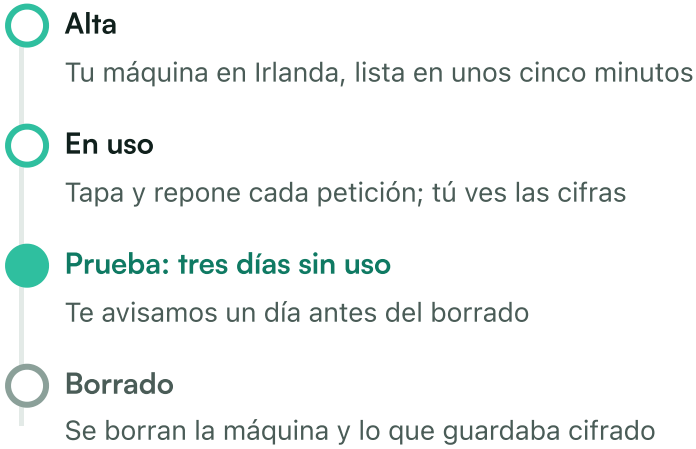

FIGURA 2

05

Accesos y claves

En el Gateway hay tres claves distintas, y conviene que tu equipo sepa para qué sirve cada una:

- **La clave de acceso de tus aplicaciones.** Es la que usan tus herramientas para hablar con tu Gateway, junto con su dirección propia y siempre por HTTPS.
- **La clave del proveedor de IA.** La pegas tú en la página de tu Gateway. Se guarda cifrada en la misma región, solo la descifra tu máquina y es la que tu Gateway usa para llamar al proveedor en nombre de tu empresa.
- **La clave del panel.** Es otra, distinta de la de las aplicaciones. Da acceso a los ajustes, a los términos, al informe y al registro.

Separar la clave de las aplicaciones de la del panel permite que quien integra una herramienta no tenga por qué tener acceso a la configuración, y al revés.

Si tu equipo trabaja con asistentes de IA para programar (Claude Code, Cursor y similares), hay un **conector MCP local** que se ejecuta en la máquina de la persona que desarrolla.

Con él, el asistente puede consultar el estado del Gateway, guardar las claves en el fichero de entorno con la confirmación de esa persona, localizar en el código dónde se llama al proveedor y proponer el cambio, hacer una prueba con datos inventados y descargar el informe para el DPO.

Las claves viajan de la máquina de tu equipo a tu Gateway sin pasar por Nonimo.

06

Quién es quién en el tratamiento

Para el RGPD, lo primero es fijar los papeles. En el uso de Nonimo Gateway quedan así:

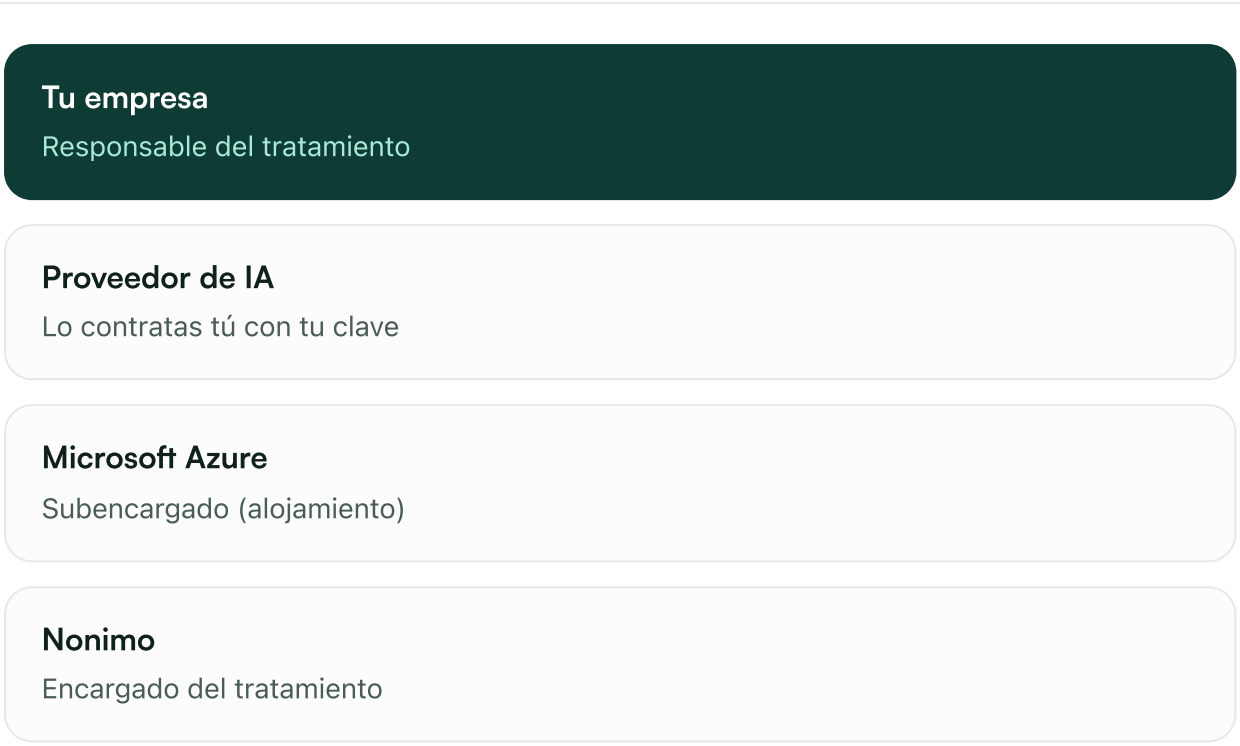

FIGURA 3

Parte	Papel	Qué hace con los datos
Tu empresa	Responsable del tratamiento	Decide para qué se usa la IA y con qué datos
Nonimo	Encargado del tratamiento	Trata el texto que pasa por el Gateway por cuenta de tu empresa
Microsoft Azure	Subencargado	Aloja la máquina confidencial en Irlanda
Tu proveedor de IA	Lo contratas tú, con tu clave	Recibe la petición ya con etiquetas
Cloudflare	Servicio de Nonimo para las licencias y los recuentos	Lleva las licencias y los recuentos; el texto va por otro camino
Paddle	Vendedor autorizado y responsable independiente	Cobra la suscripción y trata los datos de la compra

Dos matices para tu asesoría jurídica. El primero: Cloudflare no aparece como subencargado porque no interviene en el texto que tratas con el Gateway: lleva licencias y recuentos.

El segundo: el proveedor de IA tiene su propia relación contractual contigo, porque la clave es tuya; conviene revisar sus condiciones de tratamiento igual que harías con cualquier otro proveedor.

07

El marco legal: lo que el Gateway aporta a tu cumplimiento

El análisis jurídico corresponde a tu empresa; el Gateway le aporta piezas concretas para varios artículos del Reglamento General de Protección de Datos (RGPD) [1].

Minimización (art. 5.1.c). El principio pide que los datos sean «adecuados, pertinentes y limitados a lo necesario» en relación con sus fines.

Para redactar una carta, resumir un expediente o clasificar una incidencia, el modelo de IA necesita el contenido y la estructura, no el nombre ni el número de cuenta de la persona. Al sustituirlos por etiquetas, el proveedor recibe lo que necesita para el trabajo.

Protección de datos desde el diseño (art. 25). El artículo cita expresamente la seudonimización como ejemplo de medida técnica. Colocar el Gateway entre tus aplicaciones y la IA hace que la protección esté en el camino de cada petición, sin depender de que cada persona se acuerde de quitar los datos.

Encargado del tratamiento (art. 28). Nonimo actúa como encargado para el texto que pasa por el Gateway alojado. El contrato de encargo se pide en support@nonimo.ai o en hello@nonimo.ai.

Registro de actividades (art. 30). El informe mensual y el registro por petición te dan los datos para describir el tratamiento con cifras reales: qué tipos de datos personales pasan por las herramientas de IA y en qué volumen.

Seguridad del tratamiento (art. 32.1.a). El artículo menciona la seudonimización y el cifrado entre las medidas apropiadas.

El Gateway trabaja con la memoria cifrada por el procesador, guarda cifrado lo que conserva y hace que el proveedor reciba etiquetas en lugar de los datos; tu asesoría valorará cómo encaja cada pieza en el análisis de riesgos.

Evaluación de impacto (art. 35). Si el uso de la IA en tu empresa requiere una EIPD, el recorrido de este documento, la tabla de papeles y las cifras del informe son material directo para describir el tratamiento, sus riesgos y las medidas aplicadas.

Transferencias internacionales (capítulo V). Tu Gateway trata los datos en Irlanda. Si tu proveedor de IA está fuera del Espacio Económico Europeo, lo que le llega lleva etiquetas en lugar de los datos personales. Tu asesoría jurídica valorará cómo encaja esto en vuestro análisis de transferencias.

Una precisión sobre la seudonimización

El RGPD define la seudonimización en su art. 4.5 como el tratamiento que impide atribuir los datos a una persona sin información adicional que se guarda por separado.

El considerando 26 recuerda que los datos seudonimizados siguen siendo datos personales para quien puede reidentificarlos, y que los datos anónimos quedan fuera del Reglamento. El Comité Europeo de Protección de Datos (CEPD) desarrolla el concepto en sus Directrices 01/2025 sobre seudonimización [2].

En su sentencia de 4 de septiembre de 2025 (asunto C-413/23 P, SEPD contra JUR) [3], el Tribunal de Justicia de la Unión Europea señaló que unos datos seudonimizados no son necesariamente datos personales para un destinatario que no tiene medios razonables para reidentificar a la persona.

Según el Tribunal, hay que mirarlo desde la perspectiva de cada destinatario. Conviene leerlo con prudencia: para tu empresa, que conoce a sus clientes, los datos siguen siendo personales y el RGPD se aplica de lleno. Lo que cambia es lo que recibe el proveedor de IA.

La AEPD también ha publicado orientaciones sobre inteligencia artificial y protección de datos, que merece la pena tener a mano al preparar la EIPD.

08

La prueba que queda

Un DPO no se conforma con que le digan que algo funciona: necesita poder enseñarlo. El Gateway deja dos documentos, los dos sin datos personales.

El informe mensual. Está en el panel y está pensado para el DPO. Dice cuántos datos personales se han tapado y de qué tipo, solo con cifras. Un ejemplo de ficción de cómo se lee:

Noviembre	Datos tapados
Personas	4.108
Empresas	1.256
DNI y NIE	1.874
IBAN	962
Correos y teléfonos	1.117
Total	**9.317**

El registro por petición. Para cada petición guarda la hora, el proveedor, el modelo y el recuento por tipo de dato. Se exporta en CSV o en JSONL, así que se puede cargar en una hoja de cálculo o en la herramienta de registros de tu equipo.

Está construido para recoger cifras: el texto de las peticiones no forma parte de él.

Estos dos documentos te sirven, por ejemplo, para:

- Completar la ficha del tratamiento en el **registro de actividades** con volúmenes reales.
- Describir las medidas aplicadas en la **EIPD** y actualizarla con datos de uso.
- Responder a un **cliente** que pregunta qué hacéis con sus datos cuando usáis IA.
- Atender a un **auditor** o a una revisión interna con algo más que una política escrita.

09

Preguntas que tu DPO nos puede hacer

Estas son las que un DPO suele plantear antes de dar el visto bueno, con la respuesta corta.

1. **¿Dónde se procesan los datos?** En una máquina confidencial de Microsoft Azure en Irlanda, dedicada a tu empresa.
2. **¿Quién puede leer lo que procesa esa máquina?** La máquina solo arranca las versiones publicadas del Gateway, y lo que procesa no lo lee el personal de Nonimo ni el de Microsoft.
3. **¿Qué recibe el proveedor de IA?** La petición con etiquetas en lugar de los datos personales. Lo contratas tú, con tu clave.
4. **¿Qué recibe Nonimo?** Cifras: el total de peticiones y de datos tapados, y lo necesario para renovar la licencia.
5. **¿Qué se guarda y dónde?** Ajustes, la clave del proveedor y tus términos, cifrados en la misma región. Solo los descifra tu máquina con una versión publicada.
6. **¿Y el texto de las peticiones?** Va de tu aplicación al proveedor y vuelve; en tu Gateway solo está mientras se procesa.
7. **¿Funciona con respuestas en streaming y con herramientas?** Sí. Los datos reales vuelven también en las respuestas por trozos y en las llamadas a herramientas.
8. **¿Qué papel tiene Nonimo en el RGPD?** Encargado del tratamiento para el texto que pasa por el Gateway. Tu empresa es la responsable.
9. **¿Hay contrato de encargo?** Sí. Se pide en support@nonimo.ai o en hello@nonimo.ai.
10. **¿Quiénes son los subencargados?** Microsoft Azure, que aloja la máquina. Cloudflare y Paddle tienen otros papeles, descritos en la tabla de este documento.
11. **¿Cuándo se borra todo?** A los tres días seguidos sin uso durante la prueba (con aviso un día antes), al acabar la prueba sin plan, al acabar la suscripción o cuando lo pidas.
12. **¿Qué puedo enseñar a un auditor?** El informe mensual y el registro por petición en CSV o JSONL, ambos sin datos personales.

Si quieres ver cómo encaja el Gateway en el resto de medidas, tienes más detalle en la página de seguridad. Los planes disponibles están en precios, y la presentación general del producto, en la portada.

10

Fuentes

1. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD): arts. 4.5, 5.1.c, 25, 28, 30, 32.1.a, 35, capítulo V y considerando 26 — https://eur-lex.europa.eu/eli/reg/2016/679/oj
2. CEPD, Directrices 01/2025 sobre seudonimización (adoptadas el 16 de enero de 2025, consulta pública) — https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en
3. TJUE, sentencia de 4 de septiembre de 2025, asunto C-413/23 P, SEPD contra JUR (SRB) — https://curia.europa.eu/juris/liste.jsf?num=C-413/23
4. Microsoft, documentación pública de Azure Confidential Computing (contenedores confidenciales y AMD SEV-SNP) — https://learn.microsoft.com/azure/confidential-computing/