# Evaluación de Impacto en Protección de Datos (DPIA)

Activación del módulo de geolocalización de SentriaSec Guardian

**Objetivo del documento:** evaluar el impacto del tratamiento de datos de geolocalización de los equipos endpoint protegidos por SentriaSec Guardian en una organización, conforme al artículo 35 del Reglamento (UE) 2016/679 (RGPD) y al artículo 28 de la LOPDGDD (LO 3/2018).

Este documento es una **plantilla orientativa** proporcionada por SentriaSec como encargado del tratamiento. El responsable del tratamiento (cliente) debe completarla, evaluarla con su Delegado de Protección de Datos (DPO) y firmarla antes de activar los perfiles **«employee»** o **«personal»** de geolocalización en el dashboard.

## Cuándo es obligatorio realizar una DPIA

Según el RGPD art. 35.3, una DPIA es obligatoria cuando el tratamiento implica **observación sistemática a gran escala** de personas o monitorización del comportamiento. El tratamiento continuo de geolocalización de dispositivos asignados a empleados se enmarca en este supuesto, según el criterio del Comité Europeo de Protección de Datos (CEPD/EDPB) en sus directrices WP248.

# 1. Identificación de las partes

## 1.1 Responsable del tratamiento (cliente)

| | |
|---|---|
| **Razón social** | _____ |
| **NIF/CIF** | _____ |
| **Domicilio** | _____ |
| **Representante legal** | _____ |
| **DPO (si aplica)** | _____ |
| **Email contacto DPO** | _____ |

## 1.2 Encargado del tratamiento (proveedor)

| | |
|---|---|
| **Razón social** | SentriaSec / Project SAU |
| **Email contacto** | dpo@sentriasec.com |
| **Domicilio** | (Por determinar tras constitución formal) |
| **Servicio prestado** | Agente endpoint EDR con módulo de geolocalización opcional |
| **Subencargados** | Hetzner Online GmbH (DE) — alojamiento; Google LLC — Geolocation API; Cloudfla |
| **Ubicación de datos** | Unión Europea (Hetzner, Falkenstein, Alemania) |

# 2. Descripción del tratamiento

## 2.1 Naturaleza y finalidad

El módulo de geolocalización de SentriaSec Guardian determina la ubicación geográfica aproximada de cada equipo endpoint protegido, mediante **triangulación de redes WiFi visibles** (servicio de Google Geolocation API) o **geolocalización por dirección IP pública** (precisión a nivel de ciudad/proveedor).

Finalidades específicas:

• Localización de equipos en caso de pérdida o robo (modo LOCKDOWN)

• Detección de movimientos anómalos que puedan indicar uso fuera del perímetro autorizado

• Auditoría a posteriori en investigaciones de incidentes de seguridad

• Cumplimiento de obligaciones del responsable como custodio de los datos de la empresa contenidos en el equipo

## 2.2 Perfiles de activación

| Perfil | Frecuencia | DPIA req. | Caso de uso típico |
|---|---|---|---|
| lockdown_only | Solo en bloqueo | No | Default — solo geolocaliza si el equipo es declarado perdido/ro |

| | | | |
|---|---|---|---|
| employee | Cada 15 min en horario laboral | Sí (este documento) | Empresa con equipos asignados a empleados que pueden sal |
| personal | Cada 5 min continuo | No (requiere consentimiento explícito) | Autónomos o profesionales que son a la vez titulares del equip |

## 3. Base legal del tratamiento (RGPD art. 6)

El responsable identifica como base legal aplicable (marcar la que aplique):

- ■ Art. 6.1.b — Ejecución de un contrato (relación laboral con el empleado titular del equipo)
- ■ Art. 6.1.c — Cumplimiento de obligación legal (custodia de datos personales contenidos en el equipo)
- ■ Art. 6.1.f — Interés legítimo del responsable (defensa del patrimonio empresarial y de los datos contenidos)
- ■ Art. 6.1.a — Consentimiento del interesado (solo aplicable a perfil 'personal' o casos excepcionales)

**Importante:** el consentimiento del trabajador *no* es base legal válida en el contexto laboral por defecto (asimetría de poder, criterio AEPD). Use 6.1.b o 6.1.f con prueba de ponderación.

## 4. Categorías de datos tratados

| Categoría | Datos concretos |
|---|---|
| Identificación del equipo | ID interno (UUID hardware), número de serie, hostname |
| Ubicación geográfica | Latitud/longitud aproximada, ciudad, país, ISP, hora UTC |
| Red WiFi visible | BSSIDs cercanos (transmitidos a Google Geolocation API, sin nombres SSID) |
| Datos derivados | Cálculo de distancia respecto a ubicaciones previas, marca de anomalía |
| Datos NO tratados | Contenido de archivos, navegación, comunicaciones, datos biométricos |

*Ningún dato tratado por este módulo se considera categoría especial del art. 9 RGPD.*

## 5. Períodos de retención

| Tipo de dato | Retención por defecto | Configurable por cliente |
|---|---|---|
| Ubicaciones por heartbeat | 90 días | Sí (7 a 730 días) |
| Ubicaciones de LOCKDOWN | 180 días | Sí (igual rango) |
| Anomalías detectadas | 90 días | Sí (igual rango) |
| Logs de auditoría | 12 meses (obligación RGPD art. 30) | No (mínimo legal) |

Tras la retención, los datos se eliminan automáticamente por job nocturno (purge_expired_locations). El cliente puede solicitar borrado inmediato adicional en cualquier momento.

# 6. Medidas técnicas y organizativas (RGPD art. 32)

• **Cifrado en tránsito:** TLS 1.2/1.3 (TLS 1.0 y 1.1 rechazados) entre agente y servidor

• **Cifrado en reposo:** PostgreSQL con cifrado en disco LUKS en el servidor

• **Aislamiento multi-tenant:** Row-Level Security (RLS) en tabla events; filtrado por org_id en TODAS las queries

• **Autenticación del agente:** token HMAC-SHA256 firmado por equipo (rotativo cada 30 días)

• **Autenticación del dashboard:** sesiones en PostgreSQL con expiración, 2FA opcional

• **Auditoría:** cada consulta de geolocalización queda registrada con usuario, IP y timestamp

• **Minimización:** solo se almacenan lat/lng aproximados; los BSSIDs se transmiten pero no se persisten

• **Subprocesos:** Google Geolocation API recibe BSSIDs anonimizados (no se asocian a hostname/usuario)

• **Acceso restringido:** solo roles 'owner' y 'admin' del cliente pueden ver ubicaciones

• **Headers HTTP de seguridad:** HSTS, CSP, X-Frame-Options, COOP/COEP, Permissions-Policy

• **Parches automáticos:** sistema operativo del servidor con auto-update semanal (Ubuntu 24.04 LTS)

# 7. Evaluación de riesgos para los derechos y libertades

## 7.1 Matriz de riesgos identificados

| Riesgo | Probabilidad | Impacto | Riesgo residual |
|---|---|---|---|
| Acceso no autorizado a ubicaciones (interno SentriaSec) | Baja | Medio | Bajo |
| Brecha de seguridad en Hetzner / Cloudflare | Muy baja | Alto | Bajo |
| Uso indebido por el responsable (control encubierto del trabajador) | Media | Alto | Medio — mitigado por información obligatoria |
| Pérdida de datos por fallo del servidor | Baja | Bajo | Bajo |
| Reutilización fuera de finalidad declarada | Baja | Alto | Bajo — controlado por auditoría |

# 8. Obligaciones del responsable antes de activar geolocalización

• **Informar al personal afectado** por escrito sobre la activación de geolocalización, indicando finalidad, base legal, retención y cómo ejercer derechos (RGPD art. 13)

• **Actualizar el Registro de Actividades del Tratamiento** (RGPD art. 30) incluyendo esta actividad

• **Consultar al comité de empresa** si existe (Estatuto Trabajadores art. 64)

• **Revisar este DPIA periódicamente** (recomendación: cada 12 meses o ante cambios sustanciales)

• **Garantizar proporcionalidad**: no usar geolocalización para fines distintos a los declarados

• **Habilitar canal para ejercicio de derechos** (acceso, rectificación, supresión, oposición — RGPD art. 15-21)

• **Notificar brechas** a la AEPD en 72 h si se detecta acceso no autorizado a datos de geolocalización (RGPD art. 33)

## 9. Firma y aprobación

Los abajo firmantes declaran haber revisado y aprobado este Evaluación de Impacto en Protección de Datos para la activación del módulo de geolocalización de SentriaSec Guardian.

| Responsable del tratamiento | DPO (si aplica) |
|---|---|
| Nombre: _____ | Nombre: _____ |
| Cargo: _____ | Email: _____ |
| Fecha: _____ | Fecha: _____ |
| Firma: | Firma: |
| _____ | _____ |

**Una vez firmado, conserve este documento por un mínimo de 5 años para acreditar el cumplimiento del principio de responsabilidad proactiva (RGPD art. 5.2 — accountability) en caso de inspección AEPD.**

Si necesita apoyo técnico para completar este DPIA o cualquier aclaración sobre el tratamiento, puede contactar con: **dpo@sentriasec.com**