



GARMAN
CIA. LTDA.

Política de Privacidad y Protección de Datos Personales **Compañía GARMAN SECURITY GARMANTECHNÉSECURITY** **CIA.LTDA.**

1. Antecedentes

La Compañía GARMAN SECURITY GARMANTECHNÉSECURITY CIA.LTDA. (en adelante, “la Compañía”) desarrolla actividades relacionadas con la prestación de servicios de seguridad privada, incluyendo videovigilancia, monitoreo CCTV, análisis mediante inteligencia artificial, vigilancia física con guardias de seguridad, atención de incidentes y soporte tecnológico en sistemas de seguridad electrónica. Debido a la naturaleza de estas actividades, la Compañía realiza un tratamiento constante de datos personales, incluidos datos sensibles, datos biométricos y datos captados en espacios videovigilados.

Esta Política establece los principios y lineamientos que rigen dicho tratamiento, con el fin de garantizar la protección integral de los derechos de los titulares, en observancia de la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento y estándares internacionales.

2. Objeto

El propósito de esta Política es regular la forma en que la Compañía obtiene, utiliza, conserva, comunica y elimina los datos personales de todas las personas naturales con quienes mantiene una relación: trabajadores, proveedores, clientes, usuarios, visitantes, terceros y personas captadas a través de sistemas de videovigilancia. Asimismo, establece las obligaciones y responsabilidades internas para garantizar que el tratamiento de datos se realice con estricta observancia del marco normativo aplicable.

La Compañía podrá modificar o actualizar esta Política cuando existan cambios normativos, tecnológicos u operativos que así lo ameriten, comprometiéndose a comunicar dichas actualizaciones de manera oportuna mediante los canales institucionales disponibles.

3. Responsable del Tratamiento

- **Razón social:** GARMAN SECURITY GARMANTECHNÉSECURITY CIA.LTDA.
- **RUC:** 1391871643001
- **Domicilio:** Manabí, Portoviejo, calle Segundo Rivas.
- **Correo de contacto:** info@garmansecurity.com

4. Delegado de Protección de Datos Personales (DPD)



En cumplimiento de la LOPDP, la Compañía ha designado un Delegado de Protección de Datos Personales (DPD), quien actúa como punto de contacto entre los titulares, la Autoridad Nacional y la propia Compañía. El DPD supervisa las prácticas internas de tratamiento, asesora a las áreas responsables, coordina la atención de solicitudes y gestiona los incidentes relacionados con seguridad de la información.

El Delegado de Protección de Datos Personales es el abogado Carlos Leonardo Espinel Acosta, con quien se podrán contactar al correo electrónico: protecciondatos@garmansecurity.com

5. Normativa Aplicable

El tratamiento de datos personales realizado por la Compañía se encuentra regulado por la LOPDP, su Reglamento General y las disposiciones complementarias emitidas por la Autoridad Nacional. Asimismo, se observan las normas vigentes en materia de seguridad privada, contratación laboral, comercio, tributación y cualquier otra que, por su naturaleza, sea aplicable al tratamiento de datos personales.

6. Definiciones

- a. Autoridad de Protección de Datos Personales:** Autoridad independiente encargada de supervisar la aplicación de la ley, reglamentos y resoluciones relacionadas, para proteger los derechos y libertades fundamentales en cuanto al tratamiento de datos personales.
- b. Base de datos o fichero:** Conjunto estructurado de datos, sin importar su forma o modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso.
- c. Cadena de custodia:** Conjunto de procedimientos que garantizan la integridad, autenticidad y trazabilidad de las grabaciones.
- d. CCTV:** Circuito cerrado de televisión utilizado para monitoreo.
- e. Consentimiento:** Manifestación de voluntad, libre, específica, informada e inequívoca, mediante la cual el titular de los datos acepta el tratamiento de sus datos personales.
- f. Dato personal:** dato que identifica o hace identificable a una persona natural, directa o indirectamente.



g. Dato sensible: datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

h. Delegado de Protección de Datos Personales: persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos personales, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la SPDP, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos personales.

i. Destinatario: persona natural o jurídica que ha sido comunicada con datos personales.

j. DVR/NVR: Dispositivos de grabación digital o en red.

k. Encargado del Tratamiento: Persona física o jurídica, pública o privada, que realiza el tratamiento de datos personales por cuenta del responsable del tratamiento.

l. Exportación de grabaciones: Copia controlada de grabaciones para fines legales o investigativos.

m. Responsable del tratamiento: persona natural o jurídica, que sólo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.

n. On premise (Infraestructura del cliente): Modalidad de prestación del servicio en la cual los sistemas de videovigilancia, monitoreo y almacenamiento de grabaciones se encuentran instalados y operan sobre infraestructura tecnológica propiedad y control del cliente, tales como servidores, DVR, NVR u otros dispositivos locales. En este esquema, el almacenamiento y la conservación de las grabaciones dependen de la capacidad disponible del hardware instalado, operando generalmente bajo mecanismos de sobrescritura automática.

o. Sobrescritura: Proceso automático mediante el cual las grabaciones más antiguas son reemplazadas por nuevas grabaciones cuando se agota la capacidad de almacenamiento.



p. Software as a Service - SaaS (Infraestructura de la Compañía):

Modalidad de prestación del servicio en la cual los sistemas de videovigilancia, monitoreo y almacenamiento de grabaciones son proporcionados a través de plataformas tecnológicas administradas por la Compañía, accesibles de forma remota. En este esquema, la infraestructura, el almacenamiento y los plazos de conservación de las grabaciones son gestionados por la Compañía, siendo el tiempo máximo de conservación de hasta sesenta (60) días, salvo requerimiento legal, judicial o contractual en contrario.

q. Titular de datos personales: persona natural cuyos datos son objeto de tratamiento.

r. Transferencia o comunicación: manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. los datos personales que comuniquen deben ser exactos, completos y actualizados.

s. Videovigilancia: Sistema de captación, grabación y visualización de imágenes con fines de seguridad.

7. Obtención de Datos Personales

La Compañía obtiene datos personales a través de diversos medios, dependiendo del tipo de relación existente. Entre estos se encuentran formularios físicos y electrónicos, comunicaciones directas, contratos laborales o comerciales, sistemas tecnológicos de seguridad, cámaras de videovigilancia instaladas tanto por la Compañía como por sus clientes, plataformas de monitoreo, sistemas basados en inteligencia artificial y procedimientos operativos internos relacionados con la gestión de incidentes de seguridad.

La recopilación siempre se realiza de forma lícita y transparente, asegurando que el titular conozca, cuando sea necesario, el alcance del tratamiento y los fines específicos a los que sus datos serán destinados.

8. Categorías de Datos Tratados

La Compañía trata diferentes categorías de datos personales, las cuales varían en función de la relación con el titular. Esto puede incluir:

- Datos de Identificación: Nombres, apellidos, cédula de identidad, RUC.



- Datos sensibles: Datos de salud, biométricos.
- Datos de Contacto: Dirección, número de teléfono, correo electrónico.
- Datos Financieros: Información de pago y facturación, historial crediticio.
- Datos Patrimoniales: Información de activos y pasivos.
- Datos Comerciales: Historial de compras, referencias comerciales, preferencias de productos, información sobre proyectos y necesidades específicas.
- Datos Laborales: Información de empleados y candidatos a empleo.
- Datos de Navegación: Información recopilada a través de cookies y tecnologías similares en nuestro sitio web.
- Datos especiales: Datos relativos de la salud, datos personales crediticios, datos de personas con discapacidad y de sus sustitutos, datos de niñas, niños y adolescentes.
- Metadatos que podrían ser datos personales.

Dentro de las operaciones de videovigilancia y monitoreo, la Compañía puede captar imágenes, grabaciones de video, registros audiovisuales, metadatos asociados al funcionamiento del sistema y alertas generadas mediante software especializado. Cuando los sistemas integran funciones de análisis basados en inteligencia artificial, pueden procesarse datos biométricos derivados, tales como patrones faciales o lectura de placas vehiculares.

9. Base Legal para el Tratamiento

El tratamiento de datos personales por parte de la compañía se basa en la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP) del 26 de mayo de 2021 publicada en Registro Oficial No.459, y el Reglamento General de Protección de Datos (RGPD) expedido el 6 de noviembre de 2023.

La Compañía GARMAN SECURITY GARMANTECHNÉSECURITY CIA.LTDA. trata los datos personales conforme al artículo 26 de la LOPDP, con base en los siguientes preceptos:

El tratamiento de datos se sustenta en:

- El consentimiento del titular.



- Cumplimiento de obligaciones contractuales y legales.
- Interés legítimo de vigilancia y seguridad privada.

En el contexto específico de los servicios de videovigilancia y monitoreo, el interés legítimo y la finalidad de seguridad constituyen bases fundamentales que permiten la captación y almacenamiento temporal de imágenes y grabaciones.

10. Fines del Tratamiento

Los datos recolectados serán utilizados para:

- Prestación de servicios de videovigilancia, monitoreo CCTV y seguridad física.
- Detección y gestión de alertas por movimientos inusuales.
- Respuesta inmediata: llamadas a ECU 911, Policía Nacional, fuerzas de seguridad, movilización de guardias
- Grabación, almacenamiento y recuperación de imágenes
- Mantenimiento de sistemas de seguridad
- Gestión administrativa, contractual y operativa
- Gestión laboral: procesos de ingreso, permanencia y control interno
- Cumplimiento normativo y obligaciones legales
- Seguridad, prevención de delitos y protección de personas
- Proporcionar atención al cliente, asistencia técnica y seguimiento postventa.
- Evaluar y mejorar nuestros productos y servicios.
- Procesamiento de solicitudes de empleo y gestión de la relación laboral con los empleados.

11. Conservación de los Datos

Los datos personales serán conservados únicamente durante el tiempo estrictamente necesario para cumplir con las finalidades para las cuales fueron recolectados, en observancia del principio de limitación del plazo de conservación.

a) Servicio prestado con infraestructura del cliente (on premise):

Cuando las grabaciones se almacenan en dispositivos de almacenamiento propiedad del cliente (DVR, NVR o servidores locales), el plazo de conservación no es fijo y depende de la capacidad de almacenamiento disponible. En estos casos, las grabaciones se gestionan mediante sobrescritura automática, y el tiempo de conservación está sujeto a la configuración técnica y la capacidad del hardware instalado.



b) **Servicio prestado con infraestructura de la Compañía (Software as a Service - SaaS):** Cuando el servicio se presta sobre infraestructura tecnológica administrada por la Compañía, el plazo máximo de conservación de las grabaciones será de hasta sesenta (60) días, salvo que exista un requerimiento legal, judicial o contractual que justifique su conservación por un período mayor.

En todos los casos, la eliminación de las grabaciones se realizará de forma automática y segura, garantizando que no se conserven más allá del plazo permitido.

12. Transferencia y Comunicación de Datos

La Compañía podrá comunicar datos personales a autoridades competentes como la Policía Nacional, el ECU 911, Fiscalía o autoridades judiciales, cuando ello sea necesario para atender incidentes, prevenir riesgos o dar cumplimiento a mandatos legales. Asimismo, ciertos datos podrán ser compartidos con proveedores tecnológicos, aliados operativos o clientes que actúen como corresponsables, encargados o destinatarios del tratamiento.

En caso de que sea necesaria una transferencia internacional de datos, la Compañía asegurará la implementación de medidas y salvaguardas adecuadas, en cumplimiento con lo dispuesto por la LOPDP.

13. Derechos de los Titulares

Los titulares podrán ejercer los derechos de acceso, rectificación, actualización, eliminación, oposición, suspensión y portabilidad de sus datos personales, de acuerdo con la LOPDP.

- **Acceso:** conocer y solicitar la información que está siendo tratada.
- **Rectificación:** pedir la corrección o actualización de sus datos.
- **Eliminación:** solicitar la supresión de sus datos cuando ya no sean necesarios para la finalidad con la que fueron recolectados, salvo que GARMAN/el Responsable cuente con una base de legitimación que lo faculte a mantener los datos.
- **Suspensión:** exigir el cese temporal del tratamiento, por ejemplo, cuando se discuta la exactitud de los datos, el tratamiento sea ilícito o el responsable ya no los requiera.
- **Oposición:** negarse al tratamiento de sus datos, especialmente frente a fines de mercadotecnia directa o cuando exista un interés legítimo que no prevalezca sobre sus derechos.



- **Revisión de decisiones automatizadas:** evitar ser objeto de valoraciones exclusivamente automáticas, pudiendo solicitar explicaciones y una revisión humana.

14. Procedimiento para el Ejercicio de Derechos

Los titulares de los datos pueden ejercer sus derechos enviando una solicitud escrita dirigida al Delegado de Protección de Datos Personales a:

Correo Electrónico: protecciondatos@garmansecurity.com

Dirección: Oficinas de la compañía Garman, Portoviejo, calle Segundo Rivas.

La solicitud debe contener:

- Identificación del titular.
- Descripción clara y precisa del derecho que desea ejercer.
- Documentos que acrediten la identidad del solicitante o su representación legal.
- Cualquier otra información o documento relevante para la solicitud.

15. Seguridad de la Información

La Compañía implementa medidas técnicas, organizativas y jurídicas destinadas a proteger la confidencialidad, integridad y disponibilidad de los datos personales. Entre estas se encuentran mecanismos de control de acceso, autenticación por perfiles, registro de actividades en los sistemas de monitoreo, protocolos para la entrega de grabaciones, redes seguras, políticas internas de seguridad y programas de capacitación continua dirigidos a su personal. Además, realiza evaluaciones y auditorías periódicas para verificar la efectividad de dichas medidas.

16. Tratamiento de Datos mediante Sistemas de Videovigilancia y Monitoreo

Los sistemas de videovigilancia instalados en las instalaciones propias de la Compañía y en las instalaciones de los clientes cumplen una función preventiva y de protección, para seguridad de bienes, personas e instalaciones. Las imágenes captadas se utilizan exclusivamente para fines de seguridad y no se emplean para propósitos distintos a los establecidos en esta Política.

Cuando las cámaras incorporan inteligencia artificial, los datos biométricos derivados son procesados únicamente para facilitar la identificación o detección de patrones relacionados con seguridad. En ningún caso la Compañía realizará



GARMAN
CIA. LTDA.

perfilamientos o decisiones automatizadas que produzcan efectos jurídicos sin intervención humana.

Actualmente, la Compañía no utiliza cámaras ni sistemas de videovigilancia con funcionalidades de inteligencia artificial.

Cualquier referencia a tecnologías de análisis automatizado, reconocimiento facial, lectura de placas u otras funcionalidades similares corresponde a un escenario eventual y futuro, cuya implementación estará sujeta a evaluaciones de impacto, actualización de políticas, adecuación contractual y cumplimiento estricto de la normativa de protección de datos personales vigente.

17. Uso de Cookies

El portal web de la compañía no emplea cookies para análisis estadístico, personalización de contenidos ni mejora de la experiencia del usuario.

18. Contacto

Para consultas, solicitudes o información adicional relacionada con esta Política o con el tratamiento de datos personales realizado por la Compañía, los titulares pueden escribir al correo habilitado para tal efecto: protecciondatos@garmansecurity.com y/o llenar el Formulario para el Ejercicio de Derechos disponible en la página web.

19. Actualizaciones

Esta Política podrá ser actualizada por la Compañía cuando existan cambios tecnológicos, operativos o normativos que lo requieran. La versión vigente estará siempre disponible a través de los canales oficiales.

Fecha de última actualización: 02 de febrero de 2026

GARCIA BAZURTO MARCELA

Gerente General

GARMAN SECURITY GARMANTECHNÉSECURITY CIA.LTDA.