

POLÍTICA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN



En **GESTRACKING INGENIERÍA, S.L.** empresa dedicada a la **prestación de servicios de gestión de flotas y geolocalización de bienes móviles, incluyendo el tratamiento de la información asociada, así como el uso, desarrollo, mantenimiento y operación de las plataformas tecnológicas y sistemas de información que soportan dichos servicios**, nos comprometemos a implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) basado en la Norma ISO 27001:2022.

La Dirección establece esta Política como parte integral de nuestro **Sistema de Gestión de Seguridad de la Información (SGSI)**, alineado con los requisitos de la **norma ISO/IEC 27001**, con el fin de garantizar la calidad de nuestros productos y servicios, así como la protección de la información.

➤ Propósito

La política de seguridad de la información establece el compromiso de la organización con la protección de la información confidencial, la preservación de la integridad de los sistemas de información y la garantía de la disponibilidad de los recursos críticos. Esta política proporciona un marco para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con los requisitos de la norma ISO 27001.

➤ Alcance

Esta política se aplica a todos los activos de información, sistemas de información, procesos y personas dentro de la organización. Se extiende a todos los empleados, contratistas, consultores y terceros que interactúan con los sistemas de información de la organización.

➤ Compromiso de la Dirección

La alta dirección se compromete a proporcionar los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el SGSI. La dirección promueve una cultura de seguridad de la información, estableciendo objetivos y metas medibles para mejorar constantemente la postura de seguridad de la organización.

➤ Cumplimiento Legal y Regulatorio

La organización se compromete a cumplir con todas las leyes, regulaciones y requisitos contractuales aplicables relacionados con la seguridad de la información. Se establecerán procesos para monitorear y garantizar el cumplimiento continuo de estos requisitos.

➤ Identificación y Evaluación de Riesgos

La organización realiza evaluaciones periódicas de riesgos para identificar y evaluar los riesgos de seguridad de la información. Se implementarán controles adecuados para mitigar los riesgos identificados a un nivel aceptable.

POLÍTICA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN



➤ Protección de Activos de Información

Se implementan controles físicos y lógicos para proteger los activos de información contra amenazas internas y externas. Se establecen políticas y procedimientos para la gestión segura de datos, acceso a sistemas y servicios, y disposición segura de la información.

➤ Gestión de Incidentes de Seguridad

Se establecen procedimientos para la detección, notificación, respuesta y recuperación de incidentes de seguridad de la información. La organización se compromete a minimizar el impacto de los incidentes y a restaurar la operatividad normal de los sistemas de información lo antes posible.

➤ Formación y Concienciación

Se proporciona formación y concienciación en seguridad de la información a todos los empleados y partes interesadas relevantes. Se promueve una cultura de seguridad de la información mediante la sensibilización sobre las responsabilidades individuales y la importancia de la seguridad de la información.

➤ Revisión y Mejora Continua

El SGSI es objeto de revisiones periódicas para garantizar su eficacia, adecuación y mejora continua. Se establecen procesos para la revisión de la política de seguridad de la información y la identificación de áreas de mejora.

➤ Responsabilidades Individuales

Todos los empleados son responsables de cumplir con esta política, así como con los procedimientos y controles asociados. Se espera que todos contribuyan activamente a la protección de la información y al cumplimiento de los requisitos de seguridad de la organización.

➤ Principios

- **Confidencialidad:** garantizar que la información sensible solo esté disponible para aquellos que tengan autorización para acceder a ella.
- **Integridad:** asegurar que la información sea precisa, completa y no se haya modificado de manera no autorizada.
- **Disponibilidad:** asegurar que la información esté disponible y accesible cuando sea necesario para usuarios autorizados.
- **Autenticación:** verificar la identidad de los usuarios y garantizar que solo las personas autorizadas puedan acceder a los recursos de información.
- **Autorización:** controlar los derechos de acceso de los usuarios para garantizar que solo

POLÍTICA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN



tengan acceso a la información y los recursos que necesitan para realizar sus funciones.

- **Responsabilidad:** establecer la responsabilidad de los usuarios en el uso y manejo adecuado de la información y los recursos de la organización.
- **Resiliencia:** garantizar la capacidad de la organización para recuperarse de incidentes de seguridad de manera oportuna y eficiente.
- **Cumplimiento legal y normativo:** asegurar que la organización cumpla con todas las leyes, regulaciones y estándares relacionados con la seguridad de la información.
- **Gestión de riesgos:** identificar, evaluar y mitigar los riesgos de seguridad de la información para proteger los activos de la organización.
- **Cultura de seguridad:** fomentar una cultura organizacional que valore y priorice la seguridad de la información, involucrando a todos los empleados en la protección de los activos de la organización.

Esta Política del SGSI es comunicada, entendida y aplicada en todos los niveles de la organización y se revisa periódicamente para asegurar su continua adecuación al contexto de la empresa y a los objetivos estratégicos.

Madrid, a 02 de febrero de 2026

Fdo.: La dirección