

POLÍTICA DE CIFRADO DE LA INFORMACIÓN



1. Propósito

GESTRACKING INGENIERÍA, S.L. establece las directrices para la aplicación del cifrado en la información con un nivel alto de confidencialidad, garantizando su protección tanto en tránsito como en almacenamiento.

2. Alcance

Esta política aplica a toda la información clasificada como de alta confidencialidad dentro de la organización, así como a todos los empleados, contratistas y terceros que manejen dicha información.

3. Directrices

3.1. Cifrado en Tránsito

Toda información clasificada como de alta confidencialidad debe ser cifrada durante su transmisión a través de redes internas y externas mediante protocolos seguros como TLS (Transport Layer Security) o IPsec.

3.2. Cifrado en Almacenamiento

La información clasificada como de alta confidencialidad almacenada en dispositivos o sistemas deberá estar protegida mediante **mecanismos de seguridad adecuados al nivel de riesgo**, que podrán incluir **cifrado robusto (por ejemplo, AES-256) cuando aplique**, así como **controles de acceso, segregación de entornos y otras medidas técnicas y organizativas equivalentes**.

El acceso a los sistemas de almacenamiento estará restringido conforme a los principios de **mínimo privilegio y necesidad de conocer**.

3.3. Gestión de Claves de Cifrado

Las claves criptográficas utilizadas para el cifrado de la información deben ser gestionadas de acuerdo con los estándares de seguridad establecidos, garantizando su protección contra accesos no autorizados y su renovación periódica.

3.4. Monitoreo y Cumplimiento

Se realizarán auditorías periódicas para verificar el cumplimiento de esta política y detectar posibles vulnerabilidades en la protección de la información confidencial.

4. Ciclo de Vida del Cifrado de la Información

El ciclo de vida del cifrado de la información comprende las siguientes etapas:

4.1. Generación

Las claves criptográficas deben ser generadas utilizando algoritmos seguros y herramientas aprobadas por la organización.

POLÍTICA DE CIFRADO DE LA INFORMACIÓN



4.2. Transporte al Punto de Explotación

Las claves deben ser transportadas de manera segura mediante canales protegidos, asegurando su integridad y confidencialidad.

4.3. Custodia Durante la Explotación

Durante su uso activo, las claves deben ser almacenadas de manera segura, con acceso restringido y mecanismos de auditoría.

4.4. Archivo Posterior a su Retirada de Explotación Activa

Las claves que ya no estén en uso activo deben ser archivadas de manera segura, manteniendo su confidencialidad y accesibilidad restringida.

4.5. Destrucción Final

Las claves criptográficas deben ser eliminadas de forma irreversible cuando ya no sean necesarias, siguiendo procedimientos seguros de destrucción.

5. Responsabilidades

- El Departamento de IT MGR será responsable de supervisar la implementación de esta política.
- Los usuarios deben cumplir con las disposiciones establecidas y reportar cualquier incidente relacionado con la seguridad de la información.

6. Sanciones

El incumplimiento de esta política podrá resultar en acciones disciplinarias, incluyendo la terminación del contrato de trabajo o la aplicación de sanciones legales, según corresponda.

7. Revisión y Actualización

Esta política será revisada periódicamente para asegurar su efectividad y cumplimiento con los marcos regulatorios aplicables.

Madrid, a 02 de febrero de 2026

Fdo.: La dirección

