# Política Sistema de Gestión de Seguridad de la Información

Desde su fundación en 1963, SepsaMedha se especializa en el diseño y fabricación de convertidores auxiliares de potencia y sistemas embarcados para ferrocarriles, siendo un referente en el sector industrial ferroviario a nivel nacional e internacional. En un entorno cada vez más digitalizado y competitivo, la protección de la información se ha convertido en un pilar fundamental para garantizar la continuidad, la innovación y la confianza de nuestros clientes y socios.

En SepsaMedha somos plenamente conscientes de la importancia de salvaguardar la información técnica, comercial y operativa que manejamos, especialmente aquella relacionada con el desarrollo y funcionamiento de sistemas críticos para el sector ferroviario. Para ello, la Dirección asume el compromiso de implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información conforme a los requisitos de la norma ISO 27001, así como cumplir con las exigencias de Esquema Nacional de Seguridad, que permita la mejora continua de la seguridad de nuestros sistemas.

## Compromiso con la Seguridad de la Información

En SepsaMedha entendemos que la información es uno de los activos más valiosos para el desarrollo de nuestra actividad industrial y para la confianza de nuestros clientes y colaboradores. Para ello, asumimos un compromiso firme y permanente con la protección de toda la información que gestionamos. Este compromiso se fundamente en tres principios esenciales que guían todas nuestras acciones en materia de seguridad de la información:

- Confidencialidad: proteger la información técnica, comercial y de clientes frente a accesos no autorizados, especialmente aquella relacionada con el diseño y funcionamiento de sistemas críticos ferroviarios.
- Integridad: garantizar la exactitud y fiabilidad de los datos y documentación técnica a lo largo de todo el ciclo de vida del producto, desde el diseño hasta la entrega y mantenimiento.
- Disponibilidad: asegurar que la información y los sistemas necesarios para la operación, fabricación y soporte estén disponibles para el personal autorizado cuando se requiera, minimizando cualquier interrupción que pueda afectar la producción o la seguridad operativa.
- Autenticidad: garantiza que una entidad o usuario es realmente quien dice ser, asegurando la veracidad del origen de los datos mediante mecanismos como contraseñas, certificados o autenticación multifactor.

- Trazabilidad: permite registrar y seguir todas las acciones realizadas sobre la información, identificando quién accede, modifica o transfiere datos y cuándo lo hace, facilitando auditorías y la detección de incidentes.

Principios y acciones

Para garantizar la protección efectiva de la información en todos los ámbitos de nuestra actividad, en SepsaMedha hemos definido una serie de principios y acciones que orientan nuestra gestión y refuerzan nuestro compromiso con la seguridad de la información:

- Cumplimiento normativo: cumplir con todos los requisitos legales, reglamentarios y contractuales aplicables al sector ferroviario e industrial, así como los compromisos adquiridos con clientes y socios.
- Gestión de riesgos: evaluar y tratar los riesgos que puedan afectar a la seguridad de la información, prestando especial atención a la protección de la propiedad intelectual, los datos de clientes y la continuidad de la producción
- Mejora continua: revisar y mejorar de manera continua el Sistema de Gestión de Seguridad de la Información (SGSI), adaptándonos a los avances tecnológicos, las nuevas amenazas y las necesidades del sector ferroviario.
- Formación y concienciación: promover la formación y concienciación de todo el personal en materia de seguridad de la información, asegurando que cada empleado conoce y asume su responsabilidad en la protección de los activos de información.
- Gestión de incidentes: establecer procedimientos eficaces para la notificación y gestión de incidentes de seguridad, priorizando la rápida recuperación de los sistemas críticos y la comunicación transparente con las partes interesadas.
- Relación con proveedores y colaboradores: exigir y promover el cumplimiento de los requisitos de seguridad de la información a proveedores y colaboradores que tengan acceso a información o sistemas de la empresa.

D. Martin Ressnig
Director General

Pinto, 27 de Junio de 2025