

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La información es uno de los activos más importantes para DB Cargo Iberia Rail Logistics, S.A. y nuestro grupo DB Cargo. La continuidad de la actividad de la compañía depende de su disponibilidad, integridad y confidencialidad.

Por lo tanto, es imprescindible realizar una gestión profesional de los riesgos, adoptando sin dilación las medidas oportunas para proteger los activos de los sistemas de información frente a accesos no autorizados, modificaciones, comunicaciones o destrucciones, ya sean intencionadas o fortuitas, internas o externas.

Para todo ello, esta política establece un marco en base a los siguientes puntos.

Alcance.

Esta política se aplica a todos los empleados, contratistas, proveedores y terceros que tengan acceso a los activos de información de DB Cargo Iberia Rail Logistics, incluyendo sistemas, datos y redes, tanto en oficinas como en instalaciones operativas.

Objetivos.

- Proteger la información sensible de la empresa y sus clientes.
- Garantizar la continuidad de las operaciones ferroviarias.
- Cumplir con los requisitos legales y regulatorios.
- Minimizar el riesgo de incidentes de seguridad de la información.
- Promover una cultura de seguridad de la información en toda la organización.

Principios.

- **Confidencialidad:** La información debe ser accesible solo para personas autorizadas.
- **Integridad:** La información debe ser precisa y completa, y protegida contra modificaciones no autorizadas.
- **Disponibilidad:** La información y los sistemas deben estar disponibles cuando se necesiten.
- **Legalidad:** Todas las actividades de procesamiento de información deben cumplir con las leyes y regulaciones aplicables.
- **Responsabilidad:** Cada empleado es responsable de proteger la información a la que tiene acceso.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Controles de Seguridad.

Transfesa Logistics implementará los siguientes controles de seguridad, basados en la norma ISO 27001:

- **Control de Acceso:** Se implementarán controles de acceso basados en roles y el principio de mínimo privilegio.
- **Gestión de Activos:** Se mantendrá un inventario de activos de información y se clasificarán según su valor y sensibilidad.
- **Seguridad Física:** Se protegerán las instalaciones y equipos contra accesos no autorizados y daños ambientales.
- **Seguridad de Redes:** Se implementarán firewalls, sistemas de detección de intrusiones y otras medidas para proteger las redes.
- **Gestión de Incidentes:** Se establecerá un proceso para detectar, responder y recuperarse de incidentes de seguridad.
- **Conciencia y Capacitación:** Se proporcionará capacitación regular a los empleados sobre seguridad de la información.
- **Evaluación y Mejora:** Se realizarán auditorías y revisiones periódicas para evaluar la eficacia del sistema de gestión de seguridad de la información y realizar mejoras continuas.

Responsabilidades.

- La **Alta Dirección** es responsable de aprobar y respaldar esta política.
- El **Responsable de Seguridad de la Información (CISO)** es responsable de implementar y mantener el sistema de gestión de seguridad de la información.
- Los **Gerentes de Departamento** son responsables de asegurar el cumplimiento de esta política en sus áreas.
- Todos los **Empleados** son responsables de cumplir con esta política y reportar cualquier incidente de seguridad.

Cumplimiento

El incumplimiento de esta política puede resultar en acciones disciplinarias.

Revisión

Esta política se revisará y actualizará periódicamente para asegurar su relevancia y eficacia de manera anual, así como los objetivos de seguridad.

Directora Ejecutiva



Idoia Galindo Jimenez

Responsable Sistemas



Ibai Aramburu Gomez