Política de Seguridad de la Información

Introducción

Esta Política de Seguridad de la Información se establece para proteger la confidencialidad, integridad y disponibilidad de los activos de información de DEDICATED TRANSPORT, S.L. (la "Empresa"). Cumple con los estándares ISO/IEC 27001 y se aplica a todos los empleados, contratistas y terceros que accedan o utilicen los activos de información de la Empresa.

Propósito

El propósito de esta política es garantizar la protección de los activos de información contra todas las amenazas, ya sean internas o externas, intencionadas o accidentales.

Esta política busca asegurar el cumplimiento de todas las leyes, regulaciones y obligaciones contractuales aplicables, estableciendo un marco para la definición, revisión y logro de objetivos de seguridad de la información.

Además, la política tiene como objetivo promover la concienciación, educar a los empleados y guiar los procesos de toma de decisiones relacionados con la seguridad de la información dentro de la organización.

Alcance

DEDICATED TRANSPORT, S.L. , presta servicios logísticos de transporte y reparto de mercancías a nivel nacional, operando como intermediario entre empresas de sectores como el retail, el mobiliario o el equipamiento deportivo ("Clientes") y los particulares que reciben los envíos ("Destinatarios"), con el apoyo de una red de contratistas y transportistas autónomos, y ha decidido implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para mejorar los servicios prestados a sus clientes.Esta política se aplica a todos los activos de información

que sean propiedad de, alquilados, manejados o controlados por METHOD, incluyendo los datos personales que trate en el desarrollo de su actividad. En particular, esta política cubre:

- Información almacenada en medios físicos o electrónicos.
- Información transmitida a través de redes o canales de comunicación.
- Información procesada o manejada por empleados, contratistas o terceros.

Objetivos

Los principales objetivos de esta política son:

- Proteger la confidencialidad de la información para evitar divulgaciones no autorizadas.
- Garantizar la integridad de la información para prevenir modificaciones no autorizadas.
- Asegurar la disponibilidad de la información para los usuarios autorizados cuando la necesiten.
- Cumplir con las leyes, regulaciones y obligaciones contractuales aplicables.
- Mejorar continuamente el SGSI.

Organización y Responsabilidades de Seguridad

La Dirección de la Empresa es responsable de proporcionar liderazgo y compromiso con la seguridad de la información. Debe garantizar la disponibilidad de los recursos necesarios para la implementación y mantenimiento del SGSI, así como aprobar políticas y procedimientos de seguridad.

El Responsable del SGSI es el encargado de desarrollar, implementar y mantener el SGSI. Sus funciones incluyen:

- Realizar evaluaciones de riesgos.
- Implementar controles de seguridad adecuados.
- Informar a la alta dirección sobre la efectividad del SGSI.

Los empleados, contratistas y terceros son responsables de:

- Cumplir con esta política y los procedimientos de seguridad de la información.
- Reportar cualquier incidente de seguridad o vulnerabilidad detectada.
- Participar en programas de formación y concienciación en seguridad de la información.

Medidas de Seguridad

Para proteger los activos de información, se han establecido medidas de seguridad en diversas áreas:

- **Seguridad de Recursos Humanos**: Se implementan medidas para garantizar que los empleados, contratistas y terceros conozcan sus responsabilidades y protejan los activos de información.
- **Seguridad Física**: Se aplican controles físicos para evitar accesos no autorizados, daños o interferencias con los activos de información.
- **Gestión de Activos**: Se identifican, clasifican y protegen todos los activos de información a lo largo de su ciclo de vida.
- **Control de Accesos**: El acceso a los activos de información está limitado solo a usuarios autorizados mediante mecanismos de autenticación y autorización adecuados.
- **Seguridad en Redes**: Se implementan medidas para proteger la infraestructura de red contra accesos no autorizados, brechas y amenazas de seguridad.
- **Seguridad en Operaciones**: Se establecen procedimientos para mantener la integridad de los procesos operativos y garantizar la ejecución segura de las actividades diarias.
- **Gestión de Configuración**: Se aplican controles para gestionar, documentar y supervisar la configuración de los sistemas de información.
- **Desarrollo Seguro**: Se integran prácticas de seguridad en el ciclo de desarrollo de software para garantizar que las aplicaciones sean diseñadas, desarrolladas y mantenidas de forma segura.
- **Gestión de Cambios**: Se establecen procedimientos para controlar y documentar los cambios en los sistemas de información y la infraestructura tecnológica.
- **Gestión de Riesgos**: Se realizan evaluaciones regulares de riesgos para identificar y mitigar amenazas a los activos de información.
- **Gestión de Datos**: La información es clasificada y protegida de acuerdo con su nivel de sensibilidad y criticidad.
- **Gestión de Incidentes**: Se establece un procedimiento para detectar, responder y recuperarse de incidentes de seguridad de la información.

- **Continuidad del Negocio**: Se desarrollan y prueban planes de continuidad para garantizar la operación de funciones críticas en caso de una interrupción.
- **Gestión de Terceros**: Se definen y aplican requisitos de seguridad para proveedores y socios comerciales, asegurando su cumplimiento con los estándares de seguridad de la organización.
- **Cumplimiento**: Se llevan a cabo auditorías y revisiones periódicas para verificar el cumplimiento con las regulaciones y normativas aplicables.
- **Concienciación y Comunicación**: Se realizan programas de formación continua para empleados, contratistas y terceros sobre políticas, procedimientos y buenas prácticas en seguridad de la información.

Mejora Continua en Seguridad

La Empresa está comprometida con la mejora continua en la gestión de la seguridad de la información. Se realizan evaluaciones y revisiones periódicas para identificar áreas de mejora en el SGSI.

- Se evalúan auditorías, informes de incidentes y sugerencias de los empleados para implementar mejoras.
- Se monitorean métricas e indicadores de desempeño para medir la efectividad de los controles de seguridad y detectar oportunidades de optimización.
- Se realizan ajustes en el SGSI para adaptarse a nuevas amenazas y cambios en la estrategia organizacional.

Cumplimiento

La Empresa se reserva el derecho de auditar y monitorear las actividades de los empleados y la información manejada a través de los sistemas de información.

Todos los empleados deben cumplir con la Política de Seguridad de la Información y con las Políticas Específicas de Seguridad.

El incumplimiento de estas políticas resultará en medidas disciplinarias proporcionales a la infracción cometida.

Revisión

Esta política se revisa y actualiza anualmente o según sea necesario

Gestión de cambios

Versión	Fecha	Descripción	Creado por	Revisado por	Aprobado por
1.0	02/09/2026	Definición de la política	RocaJunyent	DPO Method - Bea Rodriguez	Dirección de la Empresa (DEDICATED TRANSPORT, S.L.)