POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

HISTORIAL DE MODIFICACIONES

Fecha	Versión	Aprobado por	Motivo
20/04/2023	00	D. Miguel Tarragona Piñol	Creación inicial
30/05/2023	01	D. Miguel Tarragona Piñol	Corrección miembros del Comité de Seguridad

Política de Seguridad de la Información

INTRODUCCIÓN

En la actualidad, las tecnologías de la información se enfrentan a un número creciente de amenazas que mutan y evolucionan constantemente. Ello comporta la necesidad de las Empresas de destinar parte de sus recursos materiales y personales a la de gestión de riesgos con la finalidad de reducir vulnerabilidades de sus sistemas.

El presente documento constituye la Política de Seguridad de la Información de SERVICIOS DE TRANSPORTES DE AUTOMÓVILES Y MERCANCÍAS, S.A. (en lo sucesivo SETRAM) en la que se establecen el posicionamiento de la Empresa respecto a la seguridad de la información, los criterios generales que deben regir su actividad y el conjunto de medidas que deben adoptarse para preservar la confidencialidad, integridad y disponibilidad de la información.

Dicha Política de carácter general está a su vez cumplimentada con Políticas y Protocolos de uso interno para el personal propio y técnico cuya premisa principal es el deber de proteger todos los activos de la Empresa frente a cualquier amenaza con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios, y la necesidad de lucha conjunta para defenderse de aquellas con la mayor urgencia, eficacia y resiliencia.

OBJETIVO

El objetivo de la presente Política es definir los principios y las reglas básicas para la gestión de la seguridad de la información.

ALCANCE

Esta política se aplica a todos los sistemas TIC de SETRAM y a todos los miembros de la misma, sin excepciones.

LA EMPRESA

SETRAM fue constituida en el año 1982 por empresarios del sector de la automoción, con amplia experiencia en la logística, y con el objeto de cubrir las necesidades creadas por el incremento del mercado y la implantación en España de nuevos centros de producción.

En la actualidad, SETRAM es un operador logístico multimodal del sector de la automoción, que dispone de una flota de más de 270 conjuntos porta vehículos, con la que transporta más de 400K unidades al año, y una red de terminales logísticas marítimas e interiores, con servicios de valor añadido y donde gestiona casi 500K unidades al año. Además del transporte y la logística de campas y puertos, ofrecemos a nuestros clientes el servicio de in-plant handling, en las campas del fabricante, donde gestiona 650K unidades al año.

Las actividades de campas interiores, puertos, campas del fabricante, transporte por carretera, ferrocarril y barco, así como las actividades logísticas asociadas, diferencian a SETRAM como un Operador Logístico Integral en el sector de la automoción.

Dentro de las cualidades que diferencian a SETRAM del resto de operadores, destaca la calidad del servicio, la cercanía y flexibilidad de su equipo de trabajo y su constante oferta de valores añadidos a los servicios contratados.

Política de Seguridad de la Información

Como empresa de renombre en el Sector, SETRAM es sinónimo de calidad y seguridad de servicio, tanto en transporte como almacenamiento de vehículos y estándar de modernidad y adaptación a los cambios del mercado, innovando en flota de camiones de bajo impacto medioambiental, energías renovables, mejoras digitales, como el CMR digital, y mejora continua de sus recursos industriales y humanos.

CONTENIDO

Política de Seguridad de la Información

1. Principios de la Política de Seguridad de la Información.

La presente Política responde a las recomendaciones de la ISO 27001 así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a SETRAM.

Con dicha Política SETRAM se compromete a implantar todas las medidas necesarias para cumplir con la normativa aplicable en materia de seguridad, relativa a la política informática, a la seguridad de edificios e instalaciones y al comportamiento de empleados y de terceras personas relacionadas con la Empresa en el uso de sistemas informáticos.

Además, SETRAM establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- Seguridad integral: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, debiéndose considerar como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.

- Gestión de riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles de riesgos se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.

- Prevención y recuperación de sistemas: La seguridad del sistema deberá contemplar los aspectos de prevención, detección y recuperación, para conseguir que las amenazas sobre el mismo no se materialicen o no afecten gravemente a los datos que manejan los sistemas de información o los servicios que prestan.

- Mejora continua: Las medidas de seguridad se revisarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

- Seguridad por defecto: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto y las funciones de Seguridad de la Información deberán quedar integradas en todos los niveles jerárquicos del personal.

2. Compromiso de la Dirección.

La Dirección de SETRAM consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- Promover en la Empresa las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre sus empleados.
- Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

3. Organización de la Seguridad.

La Dirección de SETRAM, con la finalidad de establecer normas relativas a la seguridad de la información en la entidad, creará un el Comité de Seguridad de la información como un medio para regular las medidas y políticas de seguridad de la información.

Las funciones del Comité de Seguridad de la Información serán las siguientes:

- Nombramiento al Responsable del Sistema de Gestión de Seguridad de la Información (SGSI) y aprobar sus funciones.
- Aprobación del inicio de la implantación del SGSI.
- Aprobación de la documentación que constituye el SGSI.
- Desarrollo, mantenimiento, revisión y aprobación de los programas y políticas.
- Aprobación de la Documentación del Sistema de Seguridad de la Información, así como de nuevas ediciones o modificaciones.
- Seguimiento de la implantación y funcionamiento del Sistema de Seguridad de la Información.
- Análisis de reclamaciones planteadas por los clientes.
- Evaluación periódica del grado de exposición a riesgos que afecten a los sistemas de información de la Empresa.
- Adopción, implantación y revisión de las medidas adoptadas para garantizar su adecuación de los sistemas de información, bases de datos, y procedimientos conforme a la legislación vigente sobre dicha materia.
- El Comité de Seguridad de la Información ejercerá la coordinación en materia de seguridad informática. A tal efecto, el Comité podrá convocar a las personas que estime oportunas para ejercer el seguimiento del grado de implantación de las normativas de seguridad de la información en su ámbito de aplicación, así como velar por el cumplimiento de estas.
- Seguimiento de los procesos del Sistema de Gestión.

El Comité de Seguridad de la Información y gestión del servicio estará constituido, al menos, por los siguientes miembros:

- Responsable del SGSI
- Responsable de Seguridad y de IT
- Director General
- Responsable de tráficos internacionales
- Director de Calidad (Logística y Automoción)

Las funciones del Responsable del Sistema de Gestión de Seguridad de la Información serán las siguientes:

- Implantación, desarrollo y mantenimiento del SGSI.
- Coordinación de la gestión de la seguridad de la información en toda la Empresa.
- Definición y desarrollo de un conjunto de procedimientos de gestión de seguridad y estándares que los soporten.
- Asesoramiento en todos los aspectos de la gestión de la seguridad de la información.
- Detección de cualquier problema que influya en la Seguridad de los productos y del servicio.
- Investigación de todos los incidentes de seguridad que sucedan.
- Ejecución de acciones para prevenir y/o corregir las no conformidades relativas a la seguridad de la información.
- Promoción de los requisitos del cliente en cuanto a seguridad de la información en todos los niveles de la Empresa implicados.

- Conservación y revisión del Manual de Seguridad de la Información, los Procedimientos Documentados y las Instrucciones de Trabajo.
- Información a la alta Dirección sobre el desempeño del sistema de gestión de la seguridad de la Información y cualquier necesidad de mejora.
- Desarrollo de programas de concienciación y formación en Gestión de la Seguridad para los empleados de la Empresa.
- Monitorización de la efectividad de los controles implantados para garantizar la seguridad de la información.
- Proposición de Planes de Mejora y solicitará la aprobación de las inversiones que posiblemente conlleven.

Asimismo, deberá proporcionar soporte a las siguientes actividades:

- Análisis de riesgos.
- Proyectos relacionados con la seguridad.
- Implementación y mantenimiento de los procesos necesarios para el sistema de gestión de la Seguridad.
- Auditorías.
- Incorporación de requerimientos de seguridad de la información en contratos y acuerdos.
- Desarrollo de planes de continuidad de negocio en la organización.
- Confección de un Plan Anual de Formación y concienciación, en función de las necesidades de la Empresa.
- Deberá mantenerse al día en novedades tecnológicas, nuevas amenazas o vulnerabilidades, estándares internacionales, legislación o regulación relacionada con la seguridad de la información; mantener contacto con consultores expertos en el sector y con proveedores.

4. Roles y responsabilidades.

Funciones y Obligaciones del Personal en Materia de Seguridad de la Información:

Dirección General	☑ Aprobar de la Política de Seguridad de la Información ☑ Designar el Representante de la dirección con autoridad para la implantación del Sistema de Gestión. ☑ Velar por la mejora continua del Sistema de Gestión
Responsable del Sistema de Gestión (SGSI – TISAX)	☑ Controlar los Documentos en Vigor, realizar la reproducción de las copias, así como efectuar y controlar su distribución ☑ Derogar y destruir los Documentos Obsoletos ☑ Elaborar los Planes y Programas ☑ Coordinar la documentación e investigación de las causas de las No Conformidades detectadas y el establecimiento de acciones correctivas y/o preventivas pertinentes. ☑ Controlar que se esté actuando según los documentos aprobados del SGSI (TISAX). ☑ Identificar juntamente con los responsables de departamento y/o áreas las necesidades formativas de los empleados de la empresa. ☑ Realizar análisis de riesgos ☑ Elaborar un Plan de tratamiento de riesgos ☑ Coordinador RGPD.
Responsable de IT	☑ Determinar las medidas de seguridad lógica ☑ Gestionar los controles lógicos

Responsables con personal a su cargo	☑ Conocer la Política de Seguridad de la Información ☑ Actuar según documentos del SGSI (TISAX) que apliquen ☑ Participar activamente en la adopción y realización de acciones correctivas y/o acciones preventivas ☑ Conocer y cumplir las políticas de seguridad de la información. ☑ Vigilar el cumplimiento de las políticas y procedimientos del SGSI (TISAX) de sus subordinados.
Todos los demás puestos de la empresa	☑ Conocer la Política de Seguridad de la Información ☑ Actuar según documentos del SGSI (TISAX) que apliquen ☑ Participar activamente en la adopción y realización de acciones correctivas y/o acciones preventivas ☑ Conocer y cumplir las políticas de seguridad de la información.

5. Datos de carácter personal.

La normativa vigente de Protección de Datos de Carácter Personal tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades y los derechos fundamentales de las personas físicas y, especialmente, su honor e intimidad personal y familiar, protegidas especialmente en la Constitución Española.

Por su parte, el Reglamento General de Protección de Datos (UE) 2016/679, establece la obligación de implantar una serie de medidas de seguridad de índole técnica y organizativa necesarias para salvaguardar la integridad y confidencialidad de los datos. Dichas medidas deben implantarse tanto en los sistemas de tratamiento como en los soportes, archivos, locales, equipos, programas y, en general, en todos los procedimientos en los que se manejen datos de carácter personal.

Conforme a lo anterior, SETRAM exigirá a todos sus empleados que intervengan en el tratamiento de datos o bien tengan acceso a información de cualquier tipo de dato carácter personal, el cumplimiento de dichas normas y del Manual de Empleados que les será facilitado por los Encargados de Seguridad y Atención a los Usuarios en Materia de Protección de Datos de la Empresa.

Dichos Encargados de Seguridad además se encargarán de coordinar, controlar, desarrollar y verificar el cumplimiento de las medidas, normativas y procedimientos implantados, siendo además los interlocutores con los usuarios ante cualquier suceso, duda o problema referente a Protección de Datos que puedan tener, detectar o sospechar. Cualquier tratamiento de datos de carácter personal que la Empresa realice deberá quedar debidamente recogido en el Registro de Actividades de Tratamiento.

Asimismo, SETRAM velará porque todos sus sistemas de información se encuentren ajustados a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el Manual de Seguridad para la protección de datos personales.

6. Información Confidencial.

De acuerdo con el artículo 5 del Estatuto de los Trabajadores, el Reglamento General de Protección de Datos 2016/679 (RGPD), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), Ley de Competencia Desleal 3/1991, incluyendo su modificación a través de la Ley 29/2009, y de la Ley Orgánica 5/2010 por la que se modifica el Código Penal de 1995, los trabajadores deben cumplir con la obligación de secreto profesional que les incumbe respecto de los datos y la información que manejen en el desarrollo de su actividad.

En base a ello, SETRAM establecerá normas de obligado cumplimiento para todo el personal sobre el uso de los recursos y componentes del sistema de información, automatizados y no automatizados (papel), así como sobre la forma de custodiar e intercambiar información y/o datos de carácter personal.

Asimismo, SETRAM deberá concienciar a sus Empleados de la importancia de la seguridad de la información y sus obligaciones en dicha materia.

La información que se considere reservada, confidencial o secreta deberá tratarse con especial cuidado, debiéndose definir medidas de seguridad extraordinarias o adicionales para el adecuado tratado de la información privilegiada.

Se exigirá a todo empleado la toma de medidas de control necesarias para asegurar, dentro de su ámbito de alcance, que dicha información no llegue a manos de personas no autorizadas. Para ello SETRAM suscribirá con sus empleados cláusulas de confidencialidad que les obliguen a guardar secreto profesional y a no difundir, transmitir o revelar a terceras personas cualquier información a la que tenga acceso como consecuencia del desempeño de su actividad laboral.

De la misma forma, SETRAM suscribirá con sus proveedores con acceso a los sistemas de información acuerdos de confidencialidad para velar por la protección de su información, así como contratos de Encargado de tratamiento de conformidad con el RGPD en caso de que además traten o accedan a datos de carácter personal.

7. Acceso a la información.

El control del acceso a la información de la Empresa es una barrera de protección, por lo que es esencial decidir quién debe tener permisos para acceder a la información y en qué circunstancias. Por ello, SETRAM deberá definir las reglas de accesos para sus sistemas, equipos, instalaciones e información conforme los requerimientos según puesto de trabajo y seguridad, y establecer quién, cómo y cuándo puede acceder a los activos de información de la Empresa.

Gracias a dicho control, la Empresa limitará el acceso a los sistemas de información exclusivamente a usuarios, procesos, dispositivos y sistemas de información únicamente autorizados.

A la hora de gestionar el control de acceso a los datos deberán tenerse en cuenta que la información, los servicios y las aplicaciones utilizadas no tienen por qué ubicarse de manera centralizada en las instalaciones, pudiéndose encontrar diseminadas en equipos y redes remotas propias o de terceros.

8. Gestión de Incidentes de Seguridad.

La Empresa deberá definir un procedimiento de gestión ante incidentes que permita detectar y corregir las posibles debilidades localizadas, dando a su vez respuesta ágil y firme a incidentes detectados.

En dicho procedimiento que deberá incluirse en la Guía de Seguridad deberá recogerse la obligación y responsabilidad de todos los empleados de identificación y notificación a la Empresa de cualquier incidente del que tengan constancia y que pudiera producirse al acceder al sistema, a un equipo, programa, carpeta etc., así como de cualquier acontecimiento que pueda suponer un ataque a la confidencialidad, integridad y disponibilidad de la información y/o que pudiera comprometer la seguridad de sus activos de información.

Las incidencias de seguridad deberán ser informadas directamente al Responsable de IT de la Empresa, quien a su vez será el encargado de comunicar lo acontecido al resto de Órganos internos y responsables implicados:

- El COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI) para que tenga conocimiento y proceda, de ser necesario, a reunirse para coordinar la mejor forma de solucionar el incidente de manera interna y/o con la colaboración de proveedores externos con probada experiencia en dichos supuestos.
- Los ENCARGADOS DE SEGURIDAD Y ATENCIÓN A LOS USUARIOS EN MATERIA DE PROTECCIÓN DE DATOS para que realicen las anotaciones en el Registro de incidentes y valoren si dicho incidente supone una vulneración de derechos y libertades en dicha materia y/o puedan derivar en la obligación de comunicación a los interesados y/o a la AEPD.
- Al ÓRGANO DE CONTROL de la RPE para su conocimiento y apertura de expediente en caso de que dicho incidente sea entendido como supuesto de responsabilidad penal corporativa.

Todo incidente deberá gestionarse de manera urgente y dentro de la más estricta confidencialidad, siendo obligación del Responsable de IT documentar y registrar el incidente junto con todas las pruebas recogidas y acciones realizadas para solucionarlo en el correspondiente Registro de Incidentes.

Dicho procedimiento deberá ser revisado y actualizado semestralmente.

9. Continuidad de Negocio.

SETRAM deberá disponer de un Plan de Continuidad de Negocio como parte de su estrategia para garantizar la continuación de los servicios y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para que la Empresa actúe en caso de ser necesario.

Este Plan de Continuidad deberá ser actualizado y aprobado periódicamente.

10. Gestión de Riesgos.

La Empresa deberá realizar un análisis de riesgos sobre todos los sistemas sujetos a la presente Política, con la finalidad de evaluar las amenazas y los riesgos a los que están expuestos.

La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles de riesgo se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los servicios prestados y además, dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas.

La gestión de riesgos quedará documentada en el informe de Análisis y gestión de riesgos.

11. Gestión de Vulnerabilidades.

La gestión de vulnerabilidades es el proceso de identificación, evaluación y priorización de vulnerabilidades en los sistemas informáticos y aplicaciones de una organización.

La Empresa deberá establecer un procedimiento de gestión de vulnerabilidades para identificar las vulnerabilidades, rastrear las soluciones y reducir las amenazas para la seguridad de la red interna/externa, proporcionando, además, una protección continua contra las amenazas.

El objetivo de dicho procedimiento es la gestión de vulnerabilidades para prevenir posibles ataques informáticos al detectar y solucionar las vulnerabilidades antes de que sean explotadas por los atacantes. Las vulnerabilidades frente a las cuales deberán protegerse los sistemas de información y la información que traten, dependerán en gran medida de la naturaleza de estos; siendo un factor intrínseco a nuestros activos.

Para su detección, la Empresa deberá realizar una vez al año una auditoría de seguridad interna y externa con proveedores externos.

12. Obligaciones de los usuarios.

Todo miembro de la Empresa tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad de la Información disponer de los medios necesarios para que la información llegue a los afectados.

Por su parte, el personal de SETRAM deberá ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, así como que ellos mismos son una pieza esencial para el mantenimiento y mejora de la seguridad. Para ello, SETRAM elaborará y entregará una Guía de Seguridad del Empleado con todas las políticas de seguridad de la información de obligado cumplimiento y establecerá un calendario de formación y de concienciación continua.

13. Relación con terceras partes.

Siempre que SETRAM preste servicios o maneje información de terceros, el responsable de esa relación les hará partícipe de la presente Política de Seguridad. Con la comunicación de dicha Política, el tercero quedará sujeto a las obligaciones y medidas de seguridad establecidas en la misma.

Asimismo, se exigirá a dichos terceros que dispongan y den cumplimiento a políticas de seguridad basadas en estándares auditables que permitan controles y revisiones de terceros que certifiquen el cumplimiento de aquellas.

En caso de ser necesario, se abrirán canales de comunicación y coordinación entre los respectivos Comités de Seguridad de la Información, y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Respecto de la relación con los proveedores, SETRAM deberá controlar que se realiza siempre bajo la más estricta legalidad, y con aquellos que además tengan acceso a información aquella deberá protegerse con la suscripción de los correspondientes acuerdos y contratos.

14. Desarrollo de la Política de Seguridad de la Información.

La presente Política de Seguridad de la Información será la base para el desarrollo de políticas y protocolos de seguridad internos que, en su conjunto, conformarán la Normativa de Seguridad de la Empresa.

La Normativa de Seguridad estará a disposición de todos los miembros de la Empresa que necesiten conocerla y en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

15. Vigencia y aceptación de la Política de Seguridad de la Información.

Esta política estará vigente desde su aprobación.

El Responsable de Seguridad será el encargado de difundir la presente Política a todos los niveles de la Empresa que corresponda, debiendo ser conocida también por cada nuevo empleado que se incorpore.

16. Revisión y Aprobación

La presente Política de Seguridad de la Información será revisada, al menos, cada dos años en las revisiones del Sistema, para asegurar su continua adecuación y eficacia.

Se tendrán en cuenta cambios significativos en el marco legal y de negocio, resultados de auditorías, así como análisis de riesgos y sugerencias de mejora.

La presente Política de Seguridad de la Información ha sido modificada por Dirección General el día 30 de mayo de 2023.

D. Miguel Tarragona Piñol
Director General
SERVICIOS DE TRANSPORTES DE AUTOMÓVILES
Y MERCANCÍAS, S.A.