Seguridad IT

Política del SGSI

Creado por	Última modificación	Clasificación Información
FS-X IT Security & Infrastructure	23/09/2025	Interna
Regulación núm.	**Versión**	**Estado**
01.02	2.0	Publicado

ÍNDICE

Lista de Figuras

I Propósito

El propósito de este documento es definir la política del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) del Grupo SEAT.

El propósito de este documento es describir y definir la política del Sistema de Gestión de Seguridad de la Información en Tecnologías de la Información de las empresas integrantes del Grupo SEAT.

Las Regulaciones de Seguridad IT comprenden todas las normativas y estándares de Seguridad IT.

Las Regulaciones de Seguridad IT están basadas en el cumplimiento de normas y estándares internacionales (por ejemplo, la ISO 27001) y tienen como objetivo establecerlas de manera firme en las empresas del Grupo SEAT.

II Alcance

El documento Política de SGSI se extiende a todas las empresas del Grupo SEAT (en adelante, Compañía o SEAT), quienes deberán adoptar e implementar las medidas recogidas en la presente política. El alcance del SGSI está delimitado a aquellas entidades enumeradas en anexo A.1.5, donde se establecen las empresas y unidades organizativas que se encuentran dentro del alcance del SGSI.

1 Sistema de Gestión de Seguridad de la Información

1.1 Objetivo

El Sistema de Gestión de la Seguridad de la Información, como parte del sistema de gestión general de la organización, se establece con el objetivo de asegurar una adecuada protección de los activos de información críticos de la Compañía, incluidos aquellos que son intercambiados con empresas externas. El SGSI permite, a través de una metodología sistemática, identificar, evaluar y gestionar los riesgos de seguridad de la información que puedan afectar a los activos de información, asegurando las siguientes propiedades en los mismos:

- **Confidencialidad:** La información que no sea explícitamente de interés público sólo debe ponerse a disposición de personal autorizado.
- **Integridad:** Debe asegurarse un procesado de la información libre de fallos, así como la protección frente a modificaciones no autorizadas.
- **Disponibilidad:** La información debe estar a disposición de las personas autorizadas en los plazos acordados.
- **Responsabilidad:** El acceso a la información que requiera protección debe ser no refutable.

La implementación de un SGSI es una decisión estratégica dentro de la Compañía que contribuye a proteger los activos de información eficazmente de una amplia variedad de amenazas, tanto internas como externas, mediante la introducción de controles y salvaguardas técnicas u organizativas apropiadas con el objetivo de:

- Asegurar la continuidad del negocio frente a amenazas.
- Minimizar los daños o pérdidas ocasionados por incidentes de seguridad de la información.
- Construir una ventaja competitiva y contribuir a alcanzar los objetivos estratégicos de la Compañía.
- Garantizar el cumplimiento de los requisitos legales o regulativos, preservando, de esta forma, la imagen corporativa.

La fijación de objetivos de seguridad de la información se realiza teniendo en cuenta las siguientes entradas:

- Informes del Responsable de Seguridad del Sistema de Gestión de la Seguridad de la Información, aprobados por la Dirección de SEAT.
- Oportunidades de mejora encontradas durante la operación del SGSI.

En la fijación de objetivos, se debe tener en cuenta que los mismos deben ser medibles y alcanzables, de ahí que la planificación para su consecución deba incluir:

- Lo que se va a hacer
- Los recursos necesarios
- Quién será el responsable
- El plazo para su consecución
- Cómo se evaluarán los resultados.
- Si procede, el indicador asociado a dicho objetivo.

La Dirección, junto con el Responsable de Seguridad del Sistema de Gestión de la Seguridad de la Información, se responsabilizará de definir los objetivos de seguridad de la información para SEAT. Éstos deben ser específicos y consecuentes con su Política de Seguridad de la Información, misión, visión y valores.

1.2 Alcance

El alcance del SGSI debe estar definido y documentado en cuanto a:

- Entidades que constituyen el SGSI. Por entidad se entiende: Departamento de una empresa del Grupo SEAT, empresa que forma parte del Grupo SEAT, actores externos como proveedores, concesionarios...
- Controles y medidas de seguridad aplicables para cada una de las entidades que constituyen las diferentes entidades que constituyen el SGSI.

El SGSI está influenciado por hechos externos al mismo que pueden hacer que el alcance sea variable en el tiempo. Aspectos que condicionan el alcance son:

- Incidencias de Seguridad IT reportadas por entidades que se encuentran fuera del SGSI.
- Cambios en el perfil de riesgos de la organización.
- Cambios por el nivel de protección de activos sensibles tratados por una entidad.
- Cambios intrínsecos motivados por la variación de los recursos que se disponen para la operación y monitorización del SGSI.

1.3 Visión

Una cultura empresarial orientada a la gestión continuada de riesgos y seguridad de la información es fundamental y necesaria para lograr los objetivos establecidos en el SGSI. Dicha visión se rige por los siguientes valores y principios:

I. RECURSOS/PERSONAL

1) Cada empleado de los departamentos incluidos en el alcance del SGSI deberá estar capacitado para analizar, identificar y reportar de forma sistemática riesgos de seguridad que contribuyen a prevenir incidencias de seguridad.

2) Cada gerente de los entes organizativos deberá ejercer con diligencia sus responsabilidades establecidas en el SGSI e incentivar a sus colaboradores/as a adoptar medidas adecuadas que protejan los activos de información más críticos de la organización.

II. PROCESOS Y SISTEMAS DE GESTIÓN

3) El sistema de gestión de riesgos empresarial (RMS: *Risk Management System*) contempla la identificación y tratamientos de gestión de riesgos de seguridad de la información.

4) La gestión de seguridad de la información está diseminada en toda la organización y todos los procesos de negocio mediante la integración del SGSI con el sistema de Gestión de Calidad (ISO 9001) de la compañía.

III. CONTROLES Y SALVAGUARDAS.

5) Todas las inversiones en controles y salvaguardas de seguridad de la información responden a riesgos o deficiencias identificados en el proceso de revisión de la efectividad del SGSI.

6) La elección de los controles de seguridad a implantar en el marco del SGSI se basa en criterios para maximizar la relación coste (inversiones / costes financieros) / beneficio (reducción del riesgo).

1.4 Estructura SGSI

El SGSI de la compañía está estructurado en diferentes áreas de acción (dominios) sobre las cuales exista una interdependencia. El SGSI debe evolucionar sistemáticamente para hacer frente a cambios en los riesgos identificados. A través de los diferentes procesos internos, el SGSI dictamina la forma como cada una de las áreas de acción se ve influenciada por el resto y, por lo tanto, su adaptación a cambios en factores internos (p.e. reducción de la efectividad de un control) o externos (cambios regulatorios). Ello constituye la base fundamental para garantizar una mejora continua en la gestión de la seguridad de la información.

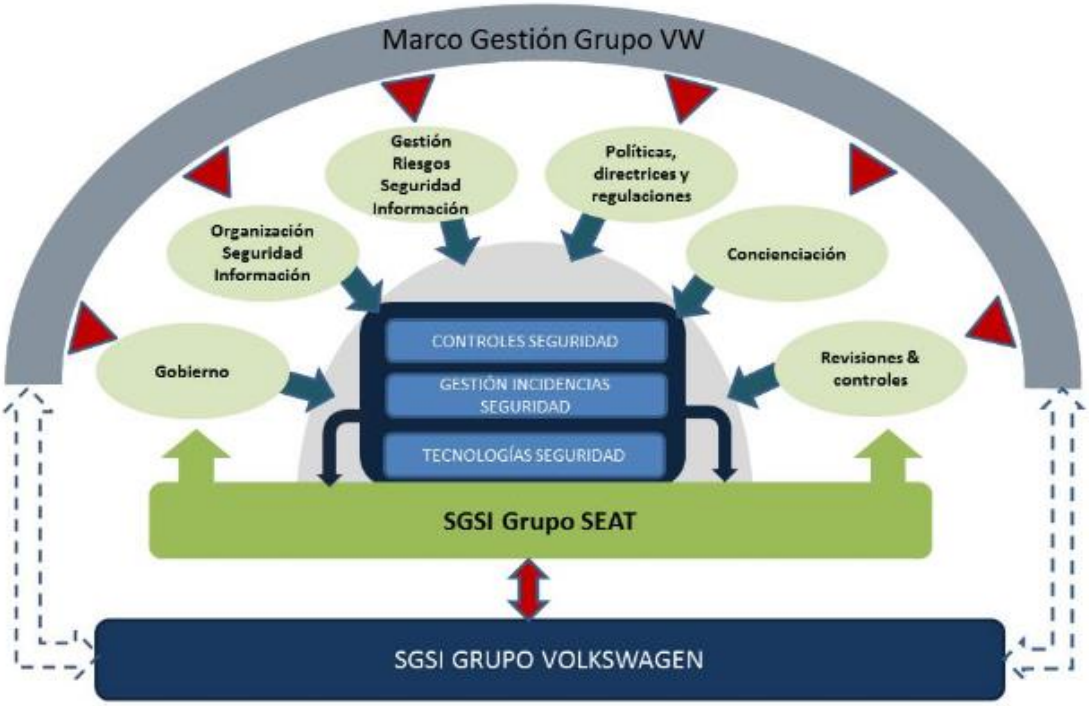

Figura 1: Estructura SGSI del Grupo SEAT e integración con K-SGSI

La descripción de los objetivos, actividades y responsabilidades de cada una de las áreas puede consultarse en el anexo A.1.4

1.5 Proceso del SGSI

1.5.1 Mejora continua

El proceso de gestión del SGSI se basa en la metodología PDCA (Plan - Do – Check – Act) o ciclo de Deming a lo largo de los diferentes procesos que constituyen el SGSI. Este proceso permite introducir progresivamente el sistema SGSI dentro de la organización y contribuye a su mejora continua. A continuación, se muestran los diferentes pasos en la definición, implantación y mejora continua del proceso:

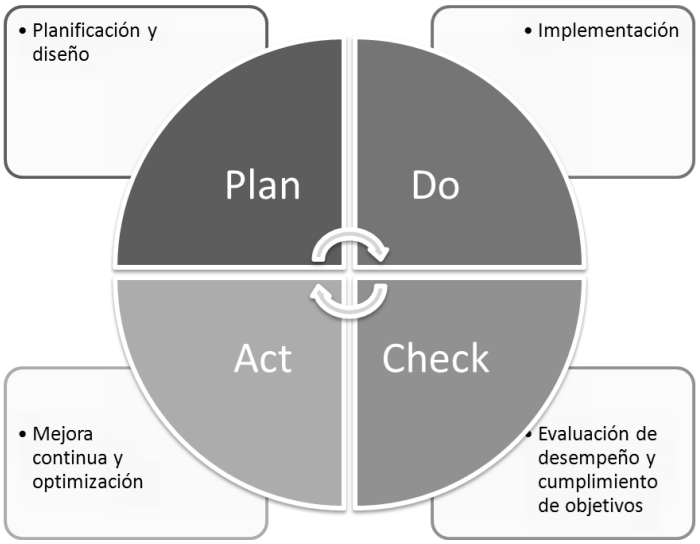

Figura 2: Mejora continua del SGSI

El CISO asume la responsabilidad de todo el proceso del SGSI, incluyendo la instauración de todos los comités necesarios para la implantación y seguimiento de la efectividad del SGSI.

1.5.2 Gestión de riesgos

Las entidades identificadas dentro del alcance del SGSI deben evaluar periódicamente los riesgos de Seguridad de la Información en su área de influencia.

La metodología para identificar y tratar los riesgos de Seguridad de la Información deriva del proceso de gestión de riesgos empresarial GRC.

Los riesgos residuales y los riesgos aceptados deben se r evaluados periódicamente para garantizar que se encuentra dentro de los umbrales de aceptación de riesgos establecidos por la organización.

El SGSI se ve influenciado por el Sistema de Gestión de riesgos de IT (ITRM).

1.5.3 Clasificación de la información y protección de activos de información

Cada entidad es responsable de clasificar la información de acuerdo con las instrucciones proporcionadas por la organización.

Los activos de información y los niveles de protección deben ser actualizados e informados de forma regular.

Todos los activos de información, los responsables de los mismos (propietarios de la información) y su clasificación deberá estar disponible para toda la organización en un Registro de Activos de Información.

1.5.4 Evaluación del desempeño

El desempeño del SGSI debe evaluarse, al menos, una vez al año en un Comité estratégico del Sistema de Gestión de Seguridad de la Información. Este proceso tiene como principales objetivos:

- Evaluar que los objetivos de Seguridad de la Información establecidos en la fase de diseño del SGSI se están cumpliendo
- Evaluar y tratar riesgos de Seguridad IT existentes y/o nuevos que se hayan identificado durante el proceso de evaluación.
- Identificar nuevas amenazas que deban ser consideradas dentro del alcance del SGSI (por ejemplo, cambios en las regulaciones o leyes aplicables).
- Establecer planes de acción correctivos para garantizar que se cumplen con los objetivos del SGSI.
- Dar a conocer y concienciar sobre los riesgos de seguridad existentes dentro de la organización.

Adicionalmente, se pueden constituir Comités específicos, vinculados en todo caso al comité estratégico, para coordinar la implantación y seguimiento de actividades resultantes del comité estratégico (p.e. Comité de implantación del SGSI).

Todas las gerencias incluidas dentro del alcance del SGSI deben ser informadas de los resultados obtenidos una vez finalizado el proceso de evaluación del desempeño.

Los comités que se constituyen para la implantación, operación y seguimiento del SGSI pueden consultarse en el apéndice B del presente documento.

1.6 Formación y concienciación

El Responsable de Seguridad del Sistema de Gestión de Seguridad de la Información debe garantizar que todo el personal involucrado en el SGSI conoce esta política, sus objetivos y procesos, a través de su divulgación, acciones formativas y acciones de concienciación.

También debe garantizar la distribución de los documentos que aplican a cada nivel, de acuerdo con los diferentes roles definidos en la compañía.

1.7 Auditoría

La Dirección General de SEAT debe garantizar y verificar, mediante auditorías internas y externas, el grado de cumplimiento de las directrices de esta Política y que éstas son operadas e implementadas correctamente, responsabilizándose del cumplimiento de las medidas correctivas que hayan podido determinarse con el fin de mantener la mejora continua.

1.8 Validez y actualización

Esta política es efectiva desde el momento de su publicación y se revisa como mínimo una vez al año.

El objetivo de las revisiones periódicas es adecuarla a los cambios en el contexto de la organización, con atención a las cuestiones externas e internas, analizándose las incidencias acaecidas de seguridad de la información y las No Conformidades encontradas en el SGSI. Todo ello armonizado con los resultados de los diferentes procesos de apreciación del riesgo.

Al revisar la Política también se revisará todas las Normas y demás documentos que la desarrollan, siguiendo un proceso de actualización periódica sujeto a los cambios relevantes que pudieran acontecer: crecimiento de la empresa y cambios organizacionales, cambios en la infraestructura, desarrollo de nuevos servicios, entre otros.

Como consecuencia se elaborará una lista de objetivos y acciones a emprender y ejecutar durante el año siguiente para garantizar la Seguridad de la Información y el buen uso de los recursos que la soportan y tratan en SEAT.

2 Sanciones

El incumplimiento de la Política de Seguridad de la Información y demás normativas y procedimientos que la desarrollen, tendrá como consecuencia la aplicación de sanciones, conforme a la magnitud y características del aspecto no cumplido, de acuerdo con la legislación laboral vigente.

III Responsabilidades

El Comité Ejecutivo del Grupo SEAT soporta el marco de gestión de la Seguridad de la Información a través de un SGSI, asigna recursos para la implantación de programas de Seguridad IT, aprueba la Política de Seguridad IT y decide sobre la estrategia de tratamiento de aquellos riesgos de seguridad de la información que pueden afectar a objetivos estratégicos corporativos.

El CISO del Grupo SEAT tiene la responsabilidad en la definición, implementación, monitorización y mejora continua del SGSI, así como constituir y liderar los diferentes comités de seguimiento e implementación del SGSI. El CISO informará regularmente sobre los riesgos y amenazas de seguridad que pueden afectar a los objetivos estratégicos de la organización. En función del alcance y de los requisitos específicos de cada una de las empresas y entidades que constituyen el Grupo SEAT, se podrán implantar SGSI aplicables.

Cada gerente del ente organizativo del Grupo SEAT que se encuentren dentro del alcance del SGSI tiene la responsabilidad de decidir sobre los controles y medidas de seguridad a implementar, dentro del ciclo de revisión periódico del SGSI, para garantizar un nivel aceptable de riesgo para la organización.

Apéndice

A General

A.1 Documentos Adicionales

A.1.1 Normativa de Seguridad IT núm. 01.01 Política de Seguridad.

A.1.2 Normativa de Seguridad IT núm. 03.01.15 Gestión de Riesgos de Seguridad de la Información.

A.1.3 SGSI – 01 – Alcance del SGSI

A.1.4 SGSI – 02 – Análisis del Contexto y Partes Interesadas

A.1.5 SGSI – 03 – Revisión por la Dirección

A.2 Listado de Abreviaturas

Abreviatura	Definición
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
DPO	Data Privacy Officer
GRC	Governance, Risk & Compliance
RMS	Risk Management System
SGSI	Sistema de Gestión de Seguridad de la Información
SI	Seguridad de la Información

A.3 Validez

Esta normativa entra en vigor en el momento de su publicación. Para nuevas compañías, el contenido de la regulación debe ser implementado en un intervalo de transición de seis meses.

Próxima fecha de revisión: Q3 de 2026

A.4 Historia del documento

Versión	Nombre	Unidad Organizativa	Fecha	Comentario
1.0	Jordi Trapero	FO-7/5	09 de Diciembre 2014	Publicación documento
1.0	Albert Zamora	EY para FS-X	06 de mayo de 2019	Actualización Departamental
1.0	Sergio Lorente	FS-X	20 de junio de 2021	Inclusión anexo C
2.0	IT Security & Infrastructure	FS-X	23 de septiembre de 2025	Nueva versión

B Estructura de Comités del SGSI

A continuación, se describe la estructura de Comités del SGSI, la independencia entre ambos y las principales funciones de cada uno de ellos. La descripción detallada de los objetivos, así como de la organización y funcionamiento pueden consultarse en el apéndice A.1.5

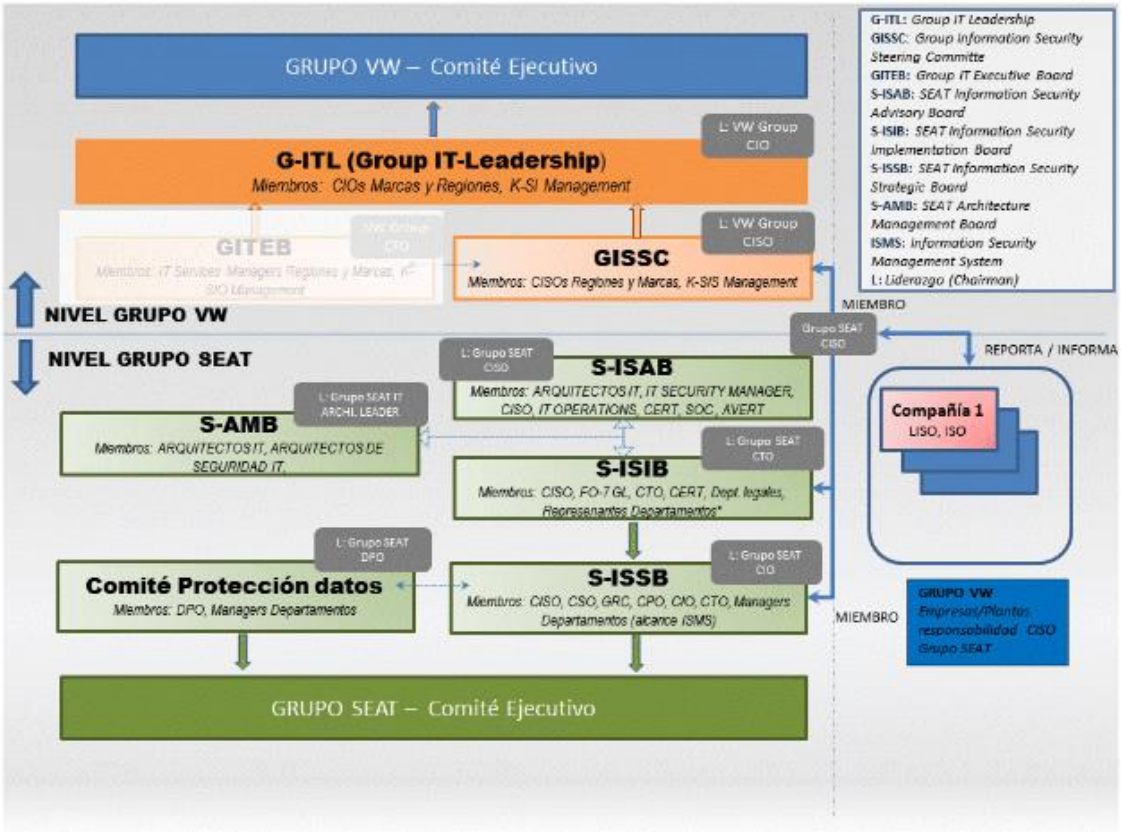

Figura 3: Estructura de comités del SGSI e independencias