POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código: ISMS-POL-001
Fecha: 18/12/2025
Versión: 1.0-ES

RESPONSABLE	REVISADO	APROBADO
Corporate Head of Cybersecurity	Comité de Seguridad de la Información	Comité de Dirección

CONTROL DE VERSIONES

Edición	Descripción del cambio	Fecha
Versión 1.0	Aprobación del Comité de Dirección: implantación inicial del Sistema de Gestión de la Seguridad de la Información.	18/12/2025

CONTENIDO

1. OBJETO

La presente Política de Seguridad de la Información (en adelante, la "**Política**"), establece las directrices fundamentales para una gestión adecuada de esta, que garantice la protección de la información, los servicios, los sistemas, las comunicaciones y demás recursos corporativos tecnológicos (en adelante, los "**Activos de Información**") de PERSÁN S.A. y las sociedades filiales que conforman el Grupo Persán (en adelante "**PERSÁN**" y/o la "**Organización**").

La necesidad de proteger los Activos de Información responde a los siguientes factores:

- La obligación de garantizar la Seguridad de la Información (en adelante, también referida como "**Seguridad**"), asegurando que el acceso, uso y custodia de dichos activos se alinee con los requisitos del negocio.
- El cumplimiento del marco legal vigente, así como de las políticas internas, normativas, procedimientos e instrucciones de Seguridad, incluyendo las obligaciones derivadas del tratamiento de datos personales.
- La voluntad de reforzar el posicionamiento institucional de la Organización, demostrando madurez en la gestión de riesgos tecnológicos y la confianza ante terceros.

Esta Política está alineada con la estrategia empresarial y la gestión de riesgos de la Organización y establece las bases para el desarrollo del Sistema de Gestión de Seguridad de la Información (en adelante, "**SGSI**"). Se apoya en un proceso sistemático de apreciación de riesgos, que permite evaluar el impacto y la probabilidad de ocurrencia de las amenazas, facilitando decisiones coherentes sobre su tratamiento.

2. ALCANCE

El ámbito de aplicación de esta Política se extiende a todo el Sistema de Gestión de Seguridad de la Información (SGSI). Se incluyen expresamente los entornos internos, servicios externalizados, infraestructuras digitales críticas, así como las relaciones tecnológicas con terceros, garantizando la trazabilidad y cobertura de los activos vinculados a operaciones esenciales.

Todas las áreas de la Organización son responsables de promover, comunicar y facilitar el cumplimiento de esta Política. Para ello, la Dirección dotará los recursos humanos, técnicos y económicos necesarios para su aplicación efectiva, así como también, establecerá mecanismos formales de asignación de responsabilidades y seguimiento del cumplimiento que aseguren la adecuada aplicación de las medidas definidas.

Esta Política es de obligado conocimiento y cumplimiento para todo el personal de PERSÁN, incluyendo empleados, Dirección, proveedores, subcontratistas y colaboradores externos que, directa o indirectamente, accedan, traten o gestionen información de la Organización. Se promoverá la formación continua y la

concienciación de todas las partes implicadas, como condición necesaria para el cumplimiento efectivo de las disposiciones establecidas.

3. RESPONSABILIDAD

La definición, el establecimiento y la revisión de la Política de Seguridad de la Información y del SGSI requiere la participación coordinada de varios roles clave de la Organización. A continuación, se describen las funciones principales de los implicados:

- **Dirección de la Organización:** tiene la autoridad para aprobar la Política, asignar responsabilidades y dotar de los recursos necesarios. Debe asegurarse de que la Política esté claramente definida, comunicada y alineada con los objetivos estratégicos.
- **Comité de Seguridad de la Información ("CSI"):** revisa y recomienda ajustes a la Política y al SGSI antes de su aprobación formal por la Dirección, proponiendo mejoras y supervisando su vigencia.
- **Responsable del SGSI:** coordina la elaboración, implantación y actualización de la Política y del SGSI, asegurando el cumplimiento de los requisitos normativos, legales y estratégicos de la Organización.

4. ACRÓNIMOS Y DEFINICIONES

Los acrónimos y definiciones relevantes para la comprensión de la presente Política se encuentran recogidos en el documento global "***Glosario de Acrónimos y Definiciones del SGSI***", el cual toma como referencia la "***Guía de Seguridad CCN-STIC-401 (Glosario y Abreviaturas)***" y otras fuentes complementarias para aquellos casos no contemplados explícitamente en la citada Guía.

5. DESARROLLO

5.1. INTRODUCCIÓN

El objetivo de la Seguridad de la Información es garantizar la protección adecuada de los recursos, la calidad de la información y la continuidad del negocio, mediante un enfoque basado en la prevención de riesgos, la supervisión constante y la respuesta eficaz ante incidentes.

PERSÁN depende de forma crítica de los sistemas de tecnologías de la información y las comunicaciones para el desarrollo de sus actividades y la consecución de sus objetivos estratégicos. Estos sistemas gestionan información valiosa y soportan procesos clave, por lo que deben ser administrados con criterios de responsabilidad, eficacia y seguridad, adoptando las medidas necesarias para protegerlos frente a amenazas que puedan comprometer la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada y de los servicios prestados.

Dado que los riesgos tecnológicos evolucionan de forma continua, la Organización requiere una estrategia dinámica y adaptable, capaz de responder a cambios en el entorno, amenazas emergentes y vulnerabilidades técnicas. Para ello, todas las áreas de PERSÁN deben aplicar las medidas de seguridad establecidas, realizar un seguimiento proactivo de la prestación de los servicios, identificar y analizar vulnerabilidades, y preparar las capacidades necesarias para una respuesta oportuna ante incidentes.

Todas las áreas deben cerciorarse de que la Seguridad de la Información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación y en la solicitud de ofertas para proyectos de tecnologías de la información.

Las áreas deben estar preparadas para actuar con eficacia en tareas de prevención, detección, respuesta y recuperación ante incidentes, garantizando así el cumplimiento de los principios establecidos en esta Política y los compromisos adquiridos en materia de Seguridad de la Información.

5.2. MISIÓN

PERSÁN se dedica a la fabricación y comercialización de productos de limpieza, detergentes, suavizantes y productos para el cuidado personal. Opera en varios países, combinando la globalización de una multinacional con la cercanía de una compañía familiar.

La Seguridad de la Información aplica de forma transversal sobre las distintas áreas de actividad de la Organización protegiendo los datos y activos que soportan su funcionamiento, y asegurando la protección de la información crítica para el negocio.

Los principios clave sobre las que aplica esta Política son:

- **Fabricación y comercialización:** la Seguridad de la Información protege la propiedad industrial, las fórmulas de productos, los planes de producción, las previsiones de ventas, y los datos logísticos y comerciales para asegurar que la información sensible relacionada con procesos y productos no sea alterada, destruida o accedida sin autorización.
- **Expansión internacional:** la información intercambiada con terceros y socios debe mantenerse segura y trazable para proteger los datos comerciales, contratos, relaciones con clientes internacionales, y asegurar el cumplimiento de normativas de protección de datos y Seguridad de la Información en los distintos países de operación.
- **Sostenibilidad:** se deben proteger los indicadores medioambientales, informes de sostenibilidad y cualquier documentación técnica o de cumplimiento que pueda estar sujeta a verificación, auditoría o certificación externa.

- **Iniciativas sociales:** se deben proteger los datos personales de beneficiarios de programas de becas, formación o mentoría para garantizar el cumplimiento de la normativa de protección de datos y la confidencialidad de la información de carácter social o educativo.
- **Innovación:** se debe prevenir fugas de información, sabotajes o accesos no autorizados a entornos de prueba y conocimiento técnico para proteger la información relativa a proyectos de I+D, documentación técnica, software en desarrollo y otras iniciativas estratégicas.
- **Relación con proveedores:** se deben definir requisitos de seguridad para garantizar una gestión segura de la información contractual, operativa y financiera intercambiada con los proveedores críticos, y contemplar cláusulas de confidencialidad e indicadores de cumplimiento de los estándares acordados.

5.3. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La gestión de la Seguridad de la Información en PERSÁN se basa en el establecimiento, seguimiento y revisión periódica de objetivos, en coherencia con el marco definido por el Sistema de Gestión de Seguridad de la Información (SGSI) y la estrategia general de la Organización.

Los objetivos deben ser medibles, alcanzables, revisables y alineados con los requisitos aplicables, incluyendo los establecidos por la legislación vigente, las partes interesadas, las necesidades internas del negocio y los riesgos identificados en el análisis de riesgos.

Los objetivos estratégicos de Seguridad de la Información son:

- Alinear la Seguridad de la Información con la misión, visión y objetivos de PERSÁN, contribuyendo al fortalecimiento institucional y a la excelencia en la gestión.
- Cumplir con los requisitos legales, normativos y contractuales aplicables, con especial atención a la legislación sobre protección de datos personales y seguridad en las comunicaciones.
- Reducir y controlar los riesgos que afectan a los Activos de Información, especialmente aquellos relacionados con los procesos más críticos para la continuidad del negocio.
- Garantizar la Seguridad de la Información en la prestación de servicios, mejorando la confianza de clientes, colaboradores y terceros.
- Fomentar una cultura de seguridad entre los empleados, promoviendo la concienciación, la formación y la responsabilidad individual en el tratamiento de la información.
- Asegurar la continuidad operativa de los servicios esenciales, estableciendo mecanismos preventivos y capacidades de respuesta ante incidentes de seguridad.

- La evaluación periódica del cumplimiento de estos objetivos forma parte del ciclo de mejora continua del SGSI y será revisada por la Dirección, a fin de introducir ajustes cuando sea necesario.

5.4. COMPROMISO DE LA DIRECCIÓN

La Dirección de PERSÁN declara su compromiso firme con la protección de la información, asegurando que los objetivos de Seguridad de la Información estén integrados en los procesos de negocio, y que los requisitos de para ello, sean identificados y aplicados de forma coherente en toda la Organización.

Asimismo, la Dirección se compromete con la mejora continua del SGSI revisando su idoneidad, adecuación y eficacia, a través del análisis de:

- Oportunidades de mejora detectadas.
- Resultados del desempeño del SGSI (no conformidades, auditorías, indicadores, cumplimiento de objetivos).
- Comentarios y expectativas de las partes interesadas.
- Cambios en el contexto interno y externo relevante para el SGSI.
- Resultados de la apreciación de riesgos y evolución del plan de tratamiento.

Para garantizar la efectividad del sistema, la Dirección dotará al SGSI de los recursos necesarios y apoyará activamente a todo el personal en la consecución de los objetivos establecidos.

5.5. PRINCIPIOS

El compromiso de PERSÁN con la Seguridad de la Información es un componente esencial de su actividad y de su responsabilidad corporativa. Debido a esto, dicho compromiso se manifiesta en la adopción de medidas que garanticen la protección de la información, los servicios, los procesos y los activos tecnológicos frente a todo tipo de amenazas.

En este contexto, la presente Política se sustenta en los siguientes principios:

- **Eficacia:** la información gestionada debe ser adecuada, relevante y útil para el cumplimiento de la misión de PERSÁN, contribuyendo a la toma de decisiones y a la generación de valor.
- **Eficiencia:** el procesamiento de la información debe realizarse optimizando recursos y reduciendo costes, garantizando que el nivel de control y tratamiento aplicado sea proporcional a los riesgos y necesidades identificadas. De esta forma, se apoya una gestión ágil, sostenible y equilibrada.

- **Legalidad:** todas las actividades relacionadas con la información deben ajustarse al marco legal y normativo vigente. PERSÁN promueve el cumplimiento normativo, la protección de datos personales, la prevención del fraude y la integridad ética en su actuación.
- **Innovación:** se fomenta la mejora continua y la adopción de tecnologías seguras, que refuercen los controles existentes y mantengan a PERSÁN como un referente en su sector.

Además, PERSÁN adopta como marco de referencia las cinco dimensiones de Seguridad de la Información que permiten establecer criterios homogéneos para la valoración y tratamiento de los activos:

- **Confidencialidad:** la información solo debe estar disponible para aquellas personas debidamente autorizadas.
- **Integridad:** la información debe mantenerse completa, exacta y protegida frente a modificaciones no autorizadas.
- **Disponibilidad:** la información y los servicios deben estar accesibles cuando se necesiten, evitando interrupciones que afecten a la continuidad operativa.
- **Autenticidad:** se debe garantizar que la identidad de los usuarios, sistemas o fuentes de información es verídica, y que los datos provienen de quien dice ser.
- **Trazabilidad:** se debe poder conocer, en todo momento, quién accedió a qué información, cuándo y cómo, asegurando el registro y seguimiento de acciones relevantes.

5.6. REQUISITOS

Para garantizar una gestión eficaz de la Seguridad de la Información, PERSÁN establece un conjunto de requisitos mínimos que deben aplicarse en el desarrollo de todas las actividades, servicios y operaciones que impliquen el tratamiento de datos o el uso de Activos de Información:

- Establecer requerimientos de seguridad desde la fase de diseño de sistemas, aplicaciones, procesos, arquitecturas y cualquier otro Activo de Información (seguridad en el diseño).
- Configurar dichos Activos de Información para que, por defecto, se encuentren en el estado más seguro posible, aplicando el principio de mínima exposición y privilegios reducidos (seguridad por defecto).
- Prevención, detección, respuesta y conservación.
- Vigilancia continuada y reevaluación periódica.
- Diferenciación de responsabilidades.
- Organización e implantación del proceso de seguridad.

- Análisis y gestión de los riesgos.
- Gestión del personal.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Seguridad en la adquisición de productos y contratación de servicios.
- Mínimo privilegio.
- Integridad y actualización del sistema de información.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Gestión y Notificación de Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.
- Seguridad en la cadena de suministro.
- Confiabilidad, seguridad y resiliencia.

Estos principios se aplican de forma transversal a toda la Organización y son desarrollados mediante un marco normativo complementario, compuesto por normativas, procedimientos, instrucciones técnicas, guías y manuales, que permitirán alcanzar los objetivos definidos y asegurar un nivel de protección adecuado en todas las dimensiones de la Seguridad de la Información: confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad.

Toda la documentación que integra el SGSI, se gestiona, estructura y conserva conforme a los procesos documentados que PERSÁN ha desarrollado teniendo en cuenta los estándares nacionales e internacionales aplicables.

5.7. ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

PERSÁN establece una estructura organizativa basada en roles diferenciados y comités de seguimiento que facilita la toma de decisiones, la gestión del riesgo y los mecanismos de coordinación para garantizar una protección eficaz de los activos y el cumplimiento de los requisitos normativos y legales aplicables.

Los requisitos específicos sobre la asignación de funciones, así como la descripción de los distintos perfiles implicados en el SGSI, se recogen en la **Política de Roles y Responsabilidades del SGSI.**

5.8. COMUNICACIÓN, DIFUSIÓN Y FORMACIÓN

La Política de Seguridad de la Información de PERSÁN, junto con su desarrollo normativo asociado, constituye el marco de referencia obligatorio que todas las áreas de la Organización deben cumplir en el ámbito de sus competencias.

Aspectos fundamentales:

- **Comunicación y accesibilidad:** la Política será comunicada a todas las personas que desempeñan funciones para PERSÁN, tanto internas como externas, y estará disponible para todas las partes interesadas pertinentes.
- **Difusión y formación:** se establecerán mecanismos de formación, sensibilización y concienciación para asegurar la comprensión y aplicación de la Política por parte del personal.
- **Cumplimiento y seguimiento:** el grado de cumplimiento de la Política será evaluado periódicamente mediante auditorías internas, revisiones, controles de cumplimiento y otros mecanismos definidos dentro del SGSI.
- **Mejora continua:** la Política se enmarca en un proceso de mejora continua, garantizando su adecuación, eficacia y alineación con la estrategia de PERSÁN, sus objetivos de seguridad y el nivel de riesgo aceptado por la Organización.

La Política será aprobada formalmente por la Dirección y estará sujeta a revisión, al menos una vez al año, o cuando se produzcan cambios relevantes en el entorno tecnológico, organizativo, normativo o en los resultados del análisis de riesgos.

5.9. GESTIÓN Y NOTIFICACIÓN DE INCIDENTES

La Organización establecerá mecanismos formales para la detección, reporte, notificación y gestión de incidentes de Seguridad de la Información que puedan comprometer la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad de la información o los servicios críticos. Todo el personal, incluidos proveedores y colaboradores, deberá comunicar sin demora cualquier evento que pueda constituir un incidente, a través de los canales definidos en el **Código de Buenas Prácticas de Seguridad de la Información.**

Los incidentes se clasificarán según su impacto y alcance. Aquellos que afecten procesos críticos, impliquen la pérdida o alteración de información sensible, causen interrupciones relevantes en los servicios o generen efectos sobre terceros, serán tratados como incidentes significativos. En estos casos, se activará un

procedimiento estructurado que incluirá análisis técnico, contención, mitigación, registro detallado, evaluación de causas raíz y revisión de medidas preventivas.

Cuando el incidente supere los umbrales definidos internamente, o así lo exijan compromisos contractuales o normativos, se procederá a la comunicación formal a las entidades u organismos correspondientes en los tiempos establecidos, conforme al marco legal vigente.

5.10. RÉGIMEN DISCIPLINARIO

El incumplimiento de esta Política ya sea por acción u omisión, compromete la capacidad de la Organización para identificar riesgos, proteger los Activos de Información, detectar amenazas en tiempo oportuno, responder eficazmente a incidentes y recuperar los servicios con garantías de continuidad. Toda vulneración de los principios establecidos será considerada una falta grave a las responsabilidades funcionales en materia de seguridad de información.

Este tipo de incumplimientos puede manifestarse en la omisión de controles preventivos, la desatención de alertas, la falta de notificación de incidentes o la inacción ante situaciones que afecten la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad de la información. La Organización aplicará las medidas correctivas y disciplinarias que resulten proporcionales al impacto generado, incluyendo, cuando corresponda, la activación de procedimientos de investigación interna y la notificación a las autoridades competentes conforme a la normativa vigente.

6. REVISIÓN Y MEJORA

El Comité de Seguridad de la Información, en colaboración con el resto de los roles del SGSI, trabajará continuamente por la mejora de la idoneidad, adecuación y eficacia de la presente Política.

Las revisiones se realizan:

- Con periodicidad mínima anual, o con mayor frecuencia en caso de incidentes graves, cambios significativos o actualizaciones normativas.
- Mediante evaluaciones de conformidad con la normativa, políticas internas y estándares de referencia aplicables.

Las propuestas de mejora se documentarán y presentarán al Comité de Seguridad de la Información (CSI) del SGSI, incluyendo resultados de auditorías internas, revisiones por la Dirección y análisis de tendencias de amenazas.

Las acciones de mejora aprobadas se registrarán en el plan de trabajo del SGSI y se integrarán en el ciclo “Plan, Do, Check, Act (PDCA)” para garantizar la mejora continua del Sistema de Gestión de Seguridad de la Información.

7. REFERENCIAS

Para más información, consultar en el repositorio del SGSI (Mapa de Procesos PERSÁN: Gestión de la Ciberseguridad):

- Cuerpo Normativo del Sistema de Gestión de Seguridad de la Información (SGSI).