ID Documento:	Aprobado por:	Fecha actualización:	Clasificación documento:
POL-SI-001	Dirección	16/10/2025	**PÚBLICO**

POL-SI-001 – Política del Sistema de Gestión de Seguridad de la Información (SGSI)

Defisoft es una empresa joven española que lleva más de 10 años ofreciendo soluciones digitales de vanguardia a empresas de diversos sectores. Durante esta década de actividad, la organización se ha focalizado en el desarrollo de software para la gestión de negocios, además, en la creación de páginas web y tiendas online customizadas. Todo ello, con un servicio de consultoría adaptado al cliente, siempre en el centro de nuestro día a día.

La Dirección de Defisoft S.L. asume de forma explícita su compromiso con la protección de la información, estableciendo un **Sistema de Gestión de Seguridad de la Información (SGSI) que permita garantizar la confidencialidad, integridad y disponibilidad de los activos críticos en todos los niveles de la organización**.

En este marco, Defisoft adopta los siguientes principios:

1. Establecer, implementar, mantener y mejorar un **SGSI conforme a los requisitos de la norma ISO/IEC 27001:2023**, asegurando su adecuación, eficacia y mejora continua.
2. Definir una **estructura organizativa clara, con roles, responsabilidades y recursos asignados**, que favorezca la aplicación práctica de las medidas de seguridad.
3. **Fomentar la mejora continua como foco central del sistema**, integrando auditorías, indicadores y planes de acción en la operativa diaria.
4. **Cumplir con los requisitos contractuales, legales, regulatorios y de partes interesadas** relacionados con la seguridad de la información.
5. **Garantizar los recursos necesarios** (económicos, técnicos y humanos) para el despliegue y sostenimiento del SGSI.
6. Impulsar una **cultura de concienciación y compromiso**, mediante formación, comunicación interna y refuerzo de buenas prácticas en todos los niveles.
7. Aplicar un **enfoque basado en riesgos**, mediante una identificación, análisis y tratamiento sistemático de las amenazas que puedan comprometer la seguridad de los activos.
8. Ejecutar **revisiones periódicas del sistema**, estableciendo planes de mejora cuando se detecten desviaciones o nuevas necesidades.
9. Promover la **implicación activa de todo el personal**, haciendo que cada persona, desde su rol y responsabilidades, contribuya al correcto funcionamiento del SGSI.

Esta política es aprobada por la Dirección de Defisoft S.L., difundida internamente, y está disponible para todos los miembros de la organización. Su cumplimiento es obligatorio y será objeto de revisión anual o cuando se produzcan cambios relevantes en el entorno.

En Campo de Criptana, a 30 de julio de 2025

Fdo.: Dirección General – Defisoft S.L.

POL-SI-002- Política de Seguridad de la Información

1. Finalidad

El objetivo de esta política es **establecer los principios, directrices y responsabilidades para garantizar la seguridad y la gestión adecuada de la información y de los activos de Defisoft S.L.**, en cumplimiento con los requisitos de seguridad establecidos en la norma ISO/IEC 27001:2023.

Esta política tiene como finalidad **asegurar la confidencialidad, integridad y disponibilidad de la información, así como fomentar el uso responsable y seguro de todos los activos de información dentro de la organización**.

Definiciones clave:

- **Información**: datos que tienen un significado y un propósito para los procesos de negocio o los servicios de la organización.

- **Activo de información**: cualquier recurso, componente o elemento (ya sea físico, lógico o humano) que permite el procesamiento, almacenamiento, manipulación o transmisión de dicha información. Esto incluye, entre otros, a los sistemas informáticos, redes, software, bases de datos, usuarios, procedimientos y documentación.

- **Sobre la gestión del inventario de activos**: La gestión de los activos de información implica los siguientes pasos fundamentales:

    - Registro y documentación formal de los activos.
    - Clasificación según su valor estratégico para el negocio y el nivel de criticidad asociado.
    - Creación y mantenimiento de un inventario actualizado y estructurado.
    - Aplicación de etiquetas identificativas y políticas de clasificación.
    - Implementación de medidas técnicas y organizativas para su protección según su categoría.

2. Alcance

Esta política aplica a toda la información gestionada por Defisoft S.L., a los sistemas que la soportan, y a todas las personas que acceden o tratan datos, incluyendo empleados, colaboradores externos y proveedores autorizados.

3. Responsabilidades

- **Dirección**: Es responsable de liderar el compromiso con la seguridad, aprobar esta política y asignar los recursos necesarios.

- **Responsable del SGSI:** Es responsable de desarrollar, coordinar y supervisar la implementación del SGSI.

- **Propietarios de activos**: Son responsables de velar por la protección de los activos bajo su responsabilidad.

- **Usuarios**: Son responsables de cumplir con las políticas y notificar cualquier incidente o anomalía de seguridad detectada.

4. Clasificación de la información

- **Inventario**: Se mantendrá un inventario actualizado que incluya hardware, software, datos, documentación y otros activos relevantes.

- **Clasificación**: Los activos se clasificarán con base en su nivel de confidencialidad, integridad y disponibilidad.

- **Etiquetas**: Se utilizarán etiquetas como “Pública”, “Privada” y “Confidencial” para marcar su sensibilidad y requerimientos de protección.

5. Tratamiento de la información

- **Procesamiento seguro**: Todo tratamiento de información debe hacerse bajo controles de acceso, cifrado, seguridad de dispositivos y formación del personal.

- **Compartir información**: Solo podrá compartirse información con partes autorizadas. Será obligatorio establecer acuerdos de confidencialidad y utilizar canales seguros. Se deben respetar políticas asociadas a protección de datos, evaluación de riesgos y cumplimiento legal.

6. Acceso y control

- **Autenticación**: Se exigirá autenticación individual segura antes de acceder a sistemas o datos.

- **Control de acceso**: El acceso estará limitado a quienes tengan necesidad legítima, bajo el principio de mínimo privilegio.

- **Privacidad**: Se protegerán los datos personales conforme a legislación vigente.

- **Auditoría**: Se mantendrán registros de todas las actividades de accesos y uso de información sensible.

7. Retención y eliminación

- **Retención**: Se definirán y aplicarán plazos adecuados para conservar la información, según requisitos legales y operativos.

- **Eliminación segura**: Los activos de información obsoletos o innecesarios serán eliminados mediante métodos seguros, conforme a las pautas internas.

8. Gestión de Riesgos

- **Evaluación**: Se realizarán análisis periódicos para identificar riesgos relacionados con la seguridad de la información.

- **Tratamiento**: Se establecerán controles para mitigar los riesgos y un protocolo para la gestión de incidentes.

9. Seguridad física y ambiental

- **Protección física**: Se garantizará el control de accesos físicos a instalaciones, equipos y recursos críticos.

- **Ambiente seguro**: Se mantendrán condiciones adecuadas (climatización, energía, protección contra incendios, etc.) en los entornos tecnológicos.

10. Continuidad del negocio

- **Planes de continuidad**: Se desarrollarán planes para asegurar la operatividad ante interrupciones.

- **Backups**: Se realizarán copias de seguridad regulares de los datos críticos, almacenadas de forma segura y verificable.

11. Auditoría y monitoreo

Se realizarán auditorías internas y revisiones técnicas para comprobar la eficacia del SGSI y el cumplimiento de esta política conforme a la ISO/IEC 27001:2023.

12. Capacitación y concienciación

Todo el personal recibirá formación sobre clasificación, tratamiento y protección de la información. Se reforzará mediante campañas de sensibilización y materiales de apoyo.

13. Cumplimiento legal y regulatorio

Defisoft S.L. cumplirá con toda la legislación y normativa aplicable en materia de seguridad de la información, protección de datos, ciberseguridad y propiedad intelectual.

14. Revisión y mejora

Esta política será revisada al menos una vez al año, o antes si se producen cambios significativos en el SGSI, en los riesgos de seguridad, en la normativa aplicable o como resultado de auditorías internas, revisiones por la Dirección o incidentes de seguridad.

La revisión y actualización será responsabilidad del responsable del SGSI, con aprobación final por la Dirección de Defisoft SL.