Política de Seguridad de la información

HISTORIAL DE REVISIONES				
Revisión	Fecha	Motivo	Elaboración	Aprobación
0	12/01/26	Inicial	Resp. De Seguridad	Comité de Seguridad

1 Objetivo y Misión

La presente política de seguridad tiene como objetivo establecer los criterios y directrices generales para la protección de la información en nuestra organización, de acuerdo con la normativa que establece en el Esquema Nacional de Seguridad (ENS).

La Dirección de SOSMATIC, consciente de la importancia de una buena gestión de la seguridad de la información para su negocio y la satisfacción del cliente, cuenta con un Sistema de Gestión de Seguridad de la Información.

SOSMATIC reconoce la importancia de proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, evitando la pérdida, la divulgación, modificación y utilización no autorizada de toda la información, incluyendo los datos personales, por lo que está comprometida con desarrollar, implantar, mantener y mejorar continuamente el SISTEMA de GESTIÓN DE LA SEGURIDAD.

2 Alcance

La Política de Seguridad de la información (ENS) se aplica a las siguientes actividades:

- ✓ *Los sistemas de información que soportan los procesos de negocio de soporte, mantenimiento, asistencia técnica y reparación in-situ y en remoto de sistemas de tecnologías de la información de puesto de usuario, redes, comunicaciones, servidores y equipos IOT de acuerdo a la declaración de aplicabilidad vigente, a fecha de emisión de la declaración.*

La política de seguridad es de obligado cumplimiento para todos los empleados, proveedores y colaboradores de SOSMATIC que tengan acceso a información y a los sistemas de información, electrónicos y físicos.

3 Roles y Comité. Funciones y responsabilidades

La seguridad de la información es responsabilidad de todos los miembros de la organización.
La implantación de la Política de Seguridad requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado.

Como parte de la Política de Seguridad de la Información, los principales roles y sus responsabilidades quedan identificados y detallados del modo siguiente:

- ✓ **Responsable de Seguridad de la información**
  Desarrollar, implementar y mantener políticas y procedimientos de seguridad de la información.
  Supervisar y gestionar la seguridad de los activos de información de la organización.
  Identificar y evaluar los riesgos de seguridad de la información y desarrollar estrategias para mitigarlos.
  Coordinar y participar en investigaciones de incidentes de seguridad de la información.
  Mantenerse actualizado sobre las últimas tendencias y amenazas en ciberseguridad y recomendar medidas para mejorar la postura de seguridad de la organización.

- ✓ **Responsable de la Información**

  Gestionar la información dentro de la organización y asegurar su integridad, disponibilidad y confidencialidad.
  Definir y aplicar políticas y procedimientos para la gestión de la información.
  Identificar y clasificar la información crítica de la organización.
  Implementar medidas de protección de la información, como cifrado y controles de acceso.
  Realizar auditorías internas y externas para garantizar el cumplimiento de las políticas de gestión de la información.

- ✓ **Responsable del Servicio**

  Gestionar y supervisar la entrega de servicios de seguridad de la información.
  Coordinar con otros equipos y proveedores para garantizar la disponibilidad y confiabilidad de los servicios de seguridad.
  Realizar evaluaciones periódicas de la calidad de los servicios de seguridad y proponer mejoras.
  Coordinar la respuesta a incidentes de seguridad y gestionar la comunicación con los usuarios afectados.
  Mantener actualizados los acuerdos de nivel de servicio (SLA) y garantizar su cumplimiento.

- ✓ **Responsable del Sistema de Gestión ENS**

  Implementar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI) basado en el estándar ENS (Esquema Nacional de Seguridad).
  Realizar evaluaciones de riesgos y establecer controles de seguridad adecuados.
  Coordinar y realizar auditorías internas y externas para verificar el cumplimiento de los requisitos de seguridad.
  Capacitar al personal en prácticas de seguridad y conciencia de la información.
  Mantener la documentación del SGSI actualizada y asegurar su accesibilidad.

- ✓ **Responsable de sistemas**

  Administrar y mantener los sistemas informáticos de la organización.
  Implementar medidas de seguridad para proteger los sistemas contra amenazas y ataques.
  Supervisar el rendimiento de los sistemas y tomar medidas para optimizar su funcionamiento.
  Realizar copias de seguridad y recuperación de datos en caso de incidentes o desastres.
  Mantenerse actualizado sobre las últimas tecnologías y tendencias en sistemas de información.

- ✓ **Persona de Contacto (POC)**

  Actuar como enlace principal entre diferentes equipos o partes interesadas en el contexto de la ciberseguridad.
  Recopilar y comunicar información relevante sobre incidentes de seguridad o problemas relacionados.
  Coordinar la resolución de problemas y la implementación de medidas correctivas.
  Proporcionar actualizaciones regulares y mantener una comunicación fluida entre todas las partes involucradas.

Servir como punto de contacto para consultas y solicitudes relacionadas con la ciberseguridad.

COMITÉ DE SEGURIDAD

El comité de Seguridad está compuesto por:

- Responsable de Seguridad
- Responsable de la Información
- Responsable del Servicio
- Responsable del Sistema de Gestión ENS
- Responsable de sistemas

El Comité de Seguridad tendrá las siguientes funciones:

• Asesorar y atender las inquietudes en materia de Seguridad de la Información, a todas las personas de SOSMATIC, siempre y cuando le sea requerido.
• Resolver los conflictos de responsabilidad que puedan aparecer entre los/as diferentes responsables y/o entre las diferentes áreas, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
• Recoger las funciones y obligaciones de los/as Responsables de la Información y los Servicios ENS, en aquellas acciones transversales, en las que le sea solicitado y/o se considere necesario.
• Promover la mejora continua del sistema de gestión de la Seguridad de la Información.

Las funciones del Comité y los Roles de Seguridad están desarrolladas y actualizadas en el manual de Funciones de SOSMATIC.

PROCEDIMIENTOS DE DESIGNACIÓN

SOSMATIC procederá a realizar la constitución del comité y de los distintos roles de Seguridad asignando las responsabilidades correspondientes.

Todos los nombramientos se revisarán cada 3 años o cuando los puestos queden vacantes.

RESOLUCIÓN DE CONFLICTOS

En el caso de presentarse conflictos entre las diferentes partes/áreas implicadas, el Comité de encargará de resolverlos, elevando a Dirección aquellos casos en los que no tenga suficiente autoridad para decidir.

4 Evaluación de riesgos

La organización llevará a cabo una evaluación de los riesgos de seguridad de la información y actualizará periódicamente esta evaluación para mantenerla actualizada.

5 Categorización

SOSMATIC dispone de una metodología de evaluación de impacto y riesgo en basado en el modelo Magerit Ver.3 y según aspectos descritos en la Guía CC-STIC 803 Valoración de los sistemas.

Para la determinación de la categoría de un sistema de información vinculado al alcance especificado, se definen tres categorías posibles: BÁSICA, MEDIA y ALTA.

- ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO (9 a 10 puntos del análisis de impacto).
- MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior (6 a 7 puntos del análisis de impacto).
- BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior (1 a 5 puntos del análisis de impacto).

6 Políticas y procedimientos de seguridad de la información

La organización establecerá políticas de seguridad de la información que incluirán las siguientes áreas:

- Identificación y autenticación de usuarios
- Control de acceso
- Gestión de contraseñas
- Gestión de parches y actualizaciones
- Copias de seguridad
- Gestión de incidentes de seguridad
- Política de seguridad de la información en el uso de servicios en la nube

Estas políticas de seguridad se desarrollarán aplicando los siguientes requisitos mínimos:

- ✓ Organización e implantación del proceso de seguridad.
- ✓ Análisis y gestión de los riesgos.
- ✓ Gestión de personal.
- ✓ Profesionalidad.
- ✓ Autorización y control de los accesos.
- ✓ Protección de las instalaciones.
- ✓ Adquisición de productos de seguridad y contratación de servicios de seguridad.
- ✓ Mínimo privilegio.
- ✓ Integridad y actualización del sistema.
- ✓ Protección de la información almacenada y en tránsito.
- ✓ Prevención ante otros sistemas de información interconectados.
- ✓ Registro de la actividad y detección de código dañino.
- ✓ Incidentes de seguridad.
- ✓ Continuidad de la actividad.
- ✓ Mejora continua del proceso de seguridad

7 Calificación de la documentación

Para facilitar el nivel de privacidad de los documentos del propio sistema de gestión de la seguridad (política, normativa, ...) se establecen 4 niveles de privacidad:

- Pública: información que se pode difundir libremente dentro y fuera del organismo y cuya divulgación no afecta a la institución en términos de pérdida de imagen y/o económica.
- Interna: información que, sin ser confidencial ni restringida, debe mantenerse en el ámbito interno de SOSMATIC y no debe estar disponible externamente, excepto la terceras partes involucradas previo compromiso de confidencialidad y conocimiento del propietario de la misma.
- Restringida: información sensible, interna a área o proyectos a los que debe tener acceso controlado un grupo reducido de personas y no toda la organización.
- Confidencial: información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidades de negocio, potencial de fraude o requisitos legales.

Cualquier información no clasificada se tratará por defecto como Interna, por lo que su divulgación deberá estar autorizada por su propietario.

8 Protección de datos personales

La organización cumplirá con las obligaciones establecidas en la normativa vigente en materia de protección de datos personales, garantizando en todo momento la confidencialidad, integridad y disponibilidad de los datos personales tratados.

9 Formación y concienciación

La organización proporcionará la formación y concienciación necesaria a todos los miembros de la organización para que conozcan y cumplan la política de seguridad de la información y la normativa aplicable.

10 Auditorías

La organización llevará a cabo auditorías internas periódicas para comprobar el cumplimiento de la política de seguridad de la información y la normativa aplicable.

11 Revisión de esta política de seguridad

La política de seguridad será revisada anualmente mediante la revisión del sistema por dirección, para asegurar que se adapta a las necesidades de la organización y a los cambios en la normativa aplicable.

12 Cumplimiento normativo

La organización cumplirá con la normativa aplicable en materia de seguridad de la información, incluyendo el Esquema Nacional de Seguridad (ENS).

Según la legislación vigente, las leyes aplicables en materia de Seguridad de la Información son:

- Real Decreto 311/2022, del 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- Ley Orgánica 3/2018 Protección de Datos Personales y garantía de los derechos digitales.
- RD 43/2021 de seguridad de las redes y sistemas de información.
- Ley 34/2002 servicios de la sociedad de la información y de comercio electrónico, que regula la Gestión de incidentes de ciberseguridad que afecten a la red de Internet

Comité de Seguridad de SOSMATIC, S.A.