Política de Seguridad de la Información de la Disciplina Capacidades Digitales de Sener

Sener Mobility

SR/SI/PO-220001/0

www.group.sener

PÚBLICO

Registro de cambios

Rev	Fecha	Autor	Sección afectada	Cambios
0	2023-09-07	Comité Seguridad Información	-	Edición Inicial

CONTENIDO

1 INTRODUCCIÓN

La Disciplina de Capacidades digitales de Sener, especializada en el desarrollo de soluciones digitales, ratifica mediante esta política su firme compromiso de garantizar la seguridad de la información en todas las actividades, productos y servicios que desarrolla. Esta política está establecida en el marco de actividades del ámbito digital de la compañía, con el propósito de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

2 ALCANCE

Aunque en Sener existe un manual y políticas de seguridad cuyo alcance afecta a todos los sistemas, trabajadores y proveedores que tengan relación con la compañía, la presente política aplica a todos los sistemas, personas, y proveedores que intervienen dentro de las actividades relativas al desarrollo, la comercialización y la consultoría de soluciones digitales, actividades que se encuentran dentro del ámbito de la disciplina de Capacidades digitales.

3 OBJETIVOS

Para materializar este compromiso, se suscriben los siguientes objetivos en relación con la seguridad de la información:

- Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.
- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.
- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

4 PRINCIPIOS Y DIRECTRICES

Sener suscribe los siguientes principios como base para alcanzar estos objetivos:

- **Mejorar continuamente** nuestro sistema de gestión de la seguridad de la información.
- Proveer los recursos materiales, económicos y humanos necesarios para llevar a cabo las tareas relacionadas con la seguridad de la información.
- Cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscriba Sener, además de los compromisos adquiridos con los clientes, así como la actualización continua de los mismos. El marco legal y regulatorio en el que desarrollamos nuestras actividades es:
  - 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, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

  - Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
  - Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual.
  - Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, en el caso de materializarse, puedan causar.
- Preservar los intereses de sus principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.
- Trabajar de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.
- Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.
- Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- Seguir las directrices establecidas en el sistema de gestión de Sener de acuerdo con lo establecido en el marco de la búsqueda de la excelencia en la calidad. Nuestro sistema de gestión tiene la siguiente estructura general:

5 ORGANIZACIÓN DE LA SEGURIDAD

La gestión de nuestro sistema se encomienda al Responsable del Sistema, que en coordinación con el Área Sistema de Gestión y Certificaciones, vela por su correcta aplicación y adecuación. La documentación correspondiente se encuentra debidamente estructurada en el gestor documental de Sener, al cual se puede acceder según los perfiles de acceso establecidos.

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la presente política de seguridad de la información. En consecuencia, la Dirección promueve la composición de un Comité de Seguridad de la Información, en aras de establecer una vía definida y de apoyo a las iniciativas de seguridad.

El **Comité Seguridad Información** dentro de la Disciplina de Capacidades Digitales es el Órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad de la información que afectan a Capacidades Digitales se acuerdan por este comité.

El Comité Seguridad Información de la Disciplina de Capacidades Digitales es un Órgano autónomo, ejecutivo y con autonomía para la toma de decisiones dentro de su ambito y que no tiene que subordinar su actividad a ningún otro elemento de nuestra compañía dentro de sus responsabilidades.

El Comité Seguridad Información de la Disciplina de Capacidades Digitales colabora y se relaciona con el área de sistemas y con el Responsable de Seguridad de la Información a nivel corporativo.

Los miembros del Comité de Seguridad Información son:

- Responsable de Sistema
- Responsable del Servicio
- Responsable de la Información
- Responsable de Seguridad
- Responsable de Protección de datos personales

Estos miembros son designados por el mismo comité, único Órgano que puede nombrarlos, renovarlos y cesarlos.

El Responsable del Servicio actuará a su vez como Presidente del Comité de Seguridad Información que será el responsable último de las decisiones adoptadas y que dirigirá las reuniones del Comité de Seguridad, informando, proponiendo y coordinando las actividades y decisiones.

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

- Revisión de la Política de Seguridad de la Información y de las responsabilidades principales y propuesta de aprobación al Órgano de Gobierno.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
    - Principales incidencias en la Seguridad de la Información.
    - Elaboración y actualización de planes de continuidad.
    - Cumplimiento y difusión de las Políticas de Seguridad.

6 FUNCIONES Y RESPONSABILIDADES

Con el objetivo de garantizar la seguridad de los sistemas y servicios utilizados en Sener, así como proteger la información que manejan, se definen los principales roles y funciones de la Disciplina de Capacidades Digitales del siguiente modo:

Perfil Asociado	Funciones y responsabilidades
Responsable del Sistema	Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios. Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o demás miembros del Comité de Seguridad de la Información. Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
Responsable de Información	Establecer y elevar para su aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema. Dictaminar respecto a los derechos de acceso a la información. Aceptar los niveles de riesgo residual que afectan a la información. Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información de la que es responsable, especialmente la incorporación de nueva Información a su cargo.
Responsable de Servicio	Establecer y elevar para su aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema. Dictaminar respecto a los derechos de acceso a los servicios. Aceptar los niveles de riesgo residual que afectan a los servicios. Poner en comunicación del Responsable de Seguridad cualquier variación respecto a los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios a su cargo.
Responsable de Seguridad	Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información. Promover las actividades de formación y concienciación en materia de seguridad de la información dentro de la Disciplina de Capacidades Digitales. Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema. Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema.

	Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación. Gestionar las revisiones externas o internas del sistema. Gestionar los procesos de certificación. Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema. Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso. Analizar los informes de autoevaluación y de auditoría, así como elevar las conclusiones al Responsable del Sistema para que adopte las medidas correctivas adecuadas. Colaborar con el Responsable de Seguridad de la Información corporativo para establecer las medidas de seguridad dentro de la Disciplina de Capacidades Digitales de forma coordinada a nivel de la compañía.
Responsable de Protección de datos personales	Informar y asesorar de las obligaciones en virtud de la normativa vigente en materia de Protección de Datos. Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas de Sener en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes. Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación. Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.

Esta definición se completa en los perfiles de puesto y en los documentos del sistema.

El procedimiento para su designación y renovación será la ratificación en el Comité Seguridad Información.

Está política se complementa con el resto de las políticas, procedimientos, instrucciones de trabajo y demás normativa interna en vigor, así como los registros asociados que desarrollan el Sistema de Gestión de Seguridad de la Información, tanto a nivel de la Disciplina de Capacidades Digitales como dentro de todo el ámbito de Sener.

La Política de Seguridad de la Información es aprobada por la Dirección y su contenido, así como las normas y procedimientos que la desarrollan, son de obligado cumplimiento para todas las personas y activos dentro de la Disciplina de Capacidades Digitales de Sener y de aquellas que participan o colaboran en sus actividades.

Esta Política de Seguridad de la Información ha sido aprobada por el Director General de Sener Mobility, y tanto ésta como sus posteriores actualizaciones serán comunicadas a través de los canales corporativos definidos por la Sección de la Disciplina de Capacidades Digitales, estando disponible para las partes interesadas.