



Cloud & Support

## Política de Seguridad de la Información ENS

Edición: 01

FECHA: 19/04/2024

Página 1 de 5

Conf.: Uso Externo

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ENS

## CONTROL DE REVISIONES

Versión	Modificados	Razón del Cambio	Fecha Aprobación
01	Sin modificación	Registro nuevo	19/04/2024

Sercom Informática, como empresa dedica a la integración de infraestructura tecnológica y provisión de servicios en la nube, asume su compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de esta, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

Por todo lo anteriormente expuesto, la Dirección establece los siguientes objetivos de seguridad de la información:

1. Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz ante situaciones críticas de seguridad
2. 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
3. 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 las actividades de la empresa
4. Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información

Para poder lograr estos objetivos es necesario:

- ✓ Mejorar continuamente nuestro sistema de seguridad de la información
- ✓ Cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que la empresa suscriba 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
- 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-ley 6/2022, de 29 de marzo de 2022
- Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre
- REGLAMENTO (UE) 910:2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS)

- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE)
- RD-ley 13/2012 de 30 de marzo, ley de cookies
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad
- 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
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Las líneas de trabajo en materia de seguridad de la información son:

- Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, pudieran causar
- Preservar los intereses de las principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor
- Trabajar de forma conjunta con los 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 la 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 los 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

- Estructurar el sistema de gestión de forma que se fácil comprender siguiendo la estructura siguiente:



La gestión de nuestro sistema se encomienda al responsable de Gestión y el sistema estará disponible en nuestro sistema de información en un repositorio, accesible según los perfiles de acceso concedidos en base al procedimiento en vigor de gestión de los accesos.

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 Integrada de Sistemas de Gestión.

Los roles o funciones de seguridad definidos en ESRI son:

Función	Deberes y responsabilidades
Responsable de la información	✓ Tomar las decisiones relativas a la información tratada
Responsable de los servicios	✓ Coordinar la implantación del sistema ✓ Mejorar el sistema de forma continua
Responsable de la seguridad	✓ Determinar la idoneidad de las medidas técnicas ✓ Proporcionar la mejor tecnología para el servicio
Responsable del sistema	✓ Coordinar la implantación del sistema ✓ Mejorar el sistema de forma continua
Dirección	✓ Proporcionar los recursos necesarios para el sistema ✓ Liderar el sistema



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 de seguridad. El comité para la gestión y coordinación de la seguridad 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 se acuerdan por este comité.

Los miembros del comité de seguridad de la información son:

- Responsable del sistema: Jordi Bermejo
- Responsable de los servicios: Marc Granados
- Responsable de la seguridad: Jordi Carbó
- Responsable de la información: David Carbó
- Dirección Empresa (socios-administradores): Jordi Carbó

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos. El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de nuestra empresa. Esta política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión.

En Barcelona, a 19 de abril de 2024

Jordi Carbó Guiral

CEO