Política de Seguridad

CCSAB-2501-27001_ENS

CCS Abogados

Ref.: CCSAB-2501-Política_Seguridad v. 1.0
29 de octubre de 2025
Documento de uso interno

ÍNDICE

1 OBJETO Y ALCANCE

La política del Sistema de Gestión de Seguridad de la Información (SGSI) tiene como propósito fijar el marco de actuación necesario para proteger los recursos de información frente a amenazas, internas o externas, deliberadas o accidentales y establecer las directrices y los principios generales para la protección de la información, que le permitan a CCS Abogados salvaguardar la confidencialidad, integridad y disponibilidad de la información de la Organización y de sus partes interesadas.

La política recogida en el presente documento deberá ser cumplida como requisito mínimo y sin perjuicio de tener políticas más restrictivas y mejorar la seguridad en la medida de lo posible. Será de aplicación sin excepciones a todos los sistemas TIC de la entidad y a todos los miembros de la organización, especialmente a aquellos implicados en Servicios y Proyectos destinados al sector público, que requieran la aplicación de ENS, y para todas las personas empleadas, contratistas, proveedores y terceros que tengan acceso a los sistemas y datos de CCS Abogados, aun cuando su relación con la compañía ya haya finalizado, así como a todos los servicios prestados por la Organización que se apoyen en las Tecnologías de la Información y las Comunicaciones.

El alcance de la presente Política cubre toda la información, independientemente de su formato o medio de almacenamiento, que sea propiedad de la Organización o que haya sido confiada a ella por terceros. Esta Política está implantada, mantenida al día y comunicada a toda la plantilla. Asimismo, está a disposición del público.

2 OBJETIVOS

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

- ➔ Cumplir con la normativa vigente en materia de los sistemas de 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.
- ➔ Promover la concienciación y formación en seguridad de la información.

3 MARCO NORMATIVO

Uno de los objetivos debe ser el de cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribimos además de los compromisos adquiridos con los clientes, así como la actualización continua de los mismos. Para ello, 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.
- ➔ Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- ➔ Real Decreto 311/2022, de 3 de Mayo, por el que se regula el Esquema Nacional de Seguridad.
- ➔ Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- ➔ Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- ➔ Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- ➔ 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. o 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. o 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.
- ➔ REGLAMENTO (UE) No 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 y por la que se deroga la Directiva 1999/93/CE

4 DESARROLLO

Para poder lograr estos objetivos es necesario:

- ➔ Mejorar continuamente nuestro sistema de seguridad de la información.
- ➔ Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, 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.
- ➔ Estructurar nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión tiene la siguiente estructura:
    - Políticas
    - Procedimientos
    - Registros

La gestión de nuestro sistema se encomienda al Responsable del Sistema y el sistema estará disponible en nuestro sistema de información en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos.

5 ORGANIZACIÓN DE SEGURIDAD

La responsabilidad esencial recae sobre la Dirección General de la organización, ya que esta es responsable de organizar las funciones y responsabilidades y de facilitar los recursos adecuados para conseguir los objetivos del ENS. Los directivos son también responsables de dar buen ejemplo siguiendo las normas de seguridad establecidas. Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándose y poniéndolos en público conocimiento a través de la presente Política de Seguridad

Los roles o funciones de seguridad definidos son:

Función	Deberes y responsabilidades
Responsable de la Información	· Tomar las decisiones relativas a la información tratada
Responsable del Servicio	· Establecer los requisitos del servicio en materia de seguridad - Determinar los niveles de seguridad de los servicios en función de las dimensiones definidas
Responsable de 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 de deberes y responsabilidades se completa en los perfiles de puesto y en los documentos del sistema Registro de responsables, roles y responsabilidades.

6 COMITÉ DE SEGURIDAD

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 de Información
- Responsable del Servicio
- Responsable de Seguridad
- Responsable del Sistema
- Representante del departamento de Derecho Público

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.
La organización de la Seguridad de la información se desarrolla en el documento complementario, entre sus funciones se deja resaltada las de velar por el ENS y entre sus tareas principales destaca la ***resolución de conflictos***, ya que las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité de seguridad y prevalecerá en todo caso el criterio de la Dirección General.
La organización de la Seguridad de la información se desarrolla en el documento complementario a esta Política de Organización de la Seguridad.
Esta política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión.

Paseo de la Castellana, 59
28046 **MADRID**
Tel. +34 910 888 000

Av. Linares Rivas 18-21, 2º
15005 **A CORUÑA**
Tel. +34 981 218363

Colón 36, 1º
36201 **VIGO**
Tel. +34 886 318970

www.ccsabogados.com