Procedimiento:	**Política de Seguridad de la Información Agència Valenciana de la Innovació (IVACE +I)**
Código:	PR.09
Número de versión:	V4.2
Servicio/s que lo elabora:	Comité de Seguridad
Fecha de elaboración:	13/12/2024
Subdirección/es general que lo revisa:	Subdirección General de Programas de Innovación
Fecha de revisión:	10/03/2025
Cargo que lo aprueba:	Vicepresidencia ejecutiva
Fecha de aprobación:	14/03/2025
Se notifica a:	Personal de la AVI
Servicio/s que propone el procedimiento/cambio:	Comité de Seguridad
Motivo de la propuesta:	Actualización de la Política de seguridad

Título:	Política de Seguridad
Tipo de documento:	Marco Normativo
Nombre del Fichero:	ENS_POL_Politica_de_seguridad.docx
Clasificación:	Interno

Revisión y aprobación		**Fecha**
Revisado por:	Responsable de Seguridad	09/12/2024
Aprobado por:	Comité de Seguridad	13/12/2024

Control de Cambios

Fecha	**Versión**	**Revisión**	**Cambios Realizados**	**Autor**
30/10/2020	1	7	Versión inicial.	CPM
13/05/2021	2	1	Modificación y firma por el VE	CPM
26/05/2021	2	2	Cambios miembros Comité	CPM
10/01/2023	3	1	Adaptación Real Decreto 951/2015 y Cambios miembros Comité	CPM
13/12/2024	4	1	Nueva edición renovada	CPM
10/03/2025	4	2	Ampliación información pie de firma	CPM

Contenido

1 Introducción

La Agència Valenciana de la Innovació (AVI) es una entidad de derecho público de la Generalitat, con personalidad jurídica propia y plena capacidad jurídica para el cumplimiento de sus fines, de las previstas en el artículo 155.1 de la Ley 1/2015, de 6 de febrero, de la Generalitat, de Hacienda Pública, del Sector Público Instrumental y de Subvenciones e integrada en el sector público instrumental de la Generalitat. Está adscrita a la conselleria con competencia en materia de Innovación.

La AVI está facultada para ejercer potestades administrativas y realizar actividades prestacionales y de fomento destinadas al desarrollo del Sistema Valenciano de Innovación. Creada por Ley 1/2017, de 1 de febrero, de la Generalitat, se rige por derecho privado, excepto en la formación de la voluntad de sus órganos, el ejercicio de potestades administrativas que tenga atribuidas y en los aspectos específicamente regulados por la Ley 1/2015, de 6 de febrero, de la Generalitat, y la legislación presupuestaria.

Su objeto general es la mejora del modelo productivo valenciano mediante el desarrollo de su capacidad innovadora para la consecución de un crecimiento inteligente, sostenible e integrador.

La Agència Valenciana de la Innovació, depende de los sistemas TIC (Tecnologías de la Información y las Telecomunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada o los servicios prestados y estando siempre protegidos contra las amenazas o los incidentes con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada y los servicios prestados.

Para hacer frente a estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), así como realizar un seguimiento continuo de los niveles de prestación de los servicios, monitorizar y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los ciberincidentes para garantizar la continuidad de los servicios prestados.

De este modo, todas las unidades administrativas del Agencia Valenciana de la Innovació tienen presente que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por tanto, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, con la aplicación de las medidas que se relacionan a continuación.

Se ha de comentar que en el RD ENS 311/2022 se indica en múltiples puntos “Política de Seguridad de la organización”. Debe de atenderse y evaluarse en cada caso cuándo se trata o se refiere al documento de “Política de Seguridad de la Organización” y cuándo al argot técnico utilizado como “Políticas de seguridad”, dónde este último se refiere como “Política de Seguridad” a aquella configuración de software o hardware que establezca unas normas o pautas a seguir, para que se cumpla en unos determinados casos de uso en concreto.

2 Misión y servicios prestados

La Agència Valenciana de la Innovació, para la gestión de sus intereses, y en el ámbito de sus competencias y como Administración pública, sirve con objetividad los intereses generales y actúa de acuerdo a los principios de eficacia, jerarquía, descentralización y coordinación, promueve toda clase de actividades y presta los servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de los ciudadanos, fomentando la innovación, el desarrollo tecnológico y la competitividad del tejido empresarial. Para ello, impulsa iniciativas que favorecen la colaboración entre organismos públicos, empresas y centros de investigación, promoviendo un ecosistema innovador que potencie el crecimiento económico y el bienestar social en la Comunitat Valenciana.

La agencia, presta los servicios que se regulan en la LEY 1/ 2017, de 1 de febrero, de la Generalitat, por la que se crea la Agència Valenciana de la Innovació.

La presente Política de Seguridad aplica a las diferentes actividades en las que participa la Entidad a través de medios electrónicos, en concreto:

Las relaciones de carácter jurídico-económico entre la ciudadanía y la Entidad.

La consulta por parte de la ciudadanía de la información pública administrativa y de los datos administrativos que estén en poder de la Entidad.

La realización de los trámites y procedimientos administrativos incorporados para su tramitación en la Sede Electrónica de la Entidad, de conformidad con lo previsto en la normativa reguladora.

El tratamiento de la información obtenida por la Entidad en el ejercicio de sus potestades.

3 Principios básicos

Los principios básicos son directrices de seguridad a tener en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

- Seguridad como proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.

- Diferenciación de responsabilidades.

Y por ello, y se desarrollará 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 seguridad
- Mínimo privilegio
- Integridad y actualización del sistema
- Protección de la información almacenada y en tránsito
- Prevención ante otros sistemas de información interconectados
- Registros de la actividad y detección de código dañino
- Incidentes de seguridad
- Continuidad de la actividad
- Mejora continua del proceso de seguridad

4 Objetivos de la seguridad de la información

La organización, establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información. Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- Gestión de activos de información: Los activos de información de la organización se encontrarán inventariados y categorizados y estarán asociados a un responsable.
- Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

- Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.
- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.
- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

5 Alcance

Esta Política se aplicará a los sistemas de información de la Agència Valenciana de Innovació, relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos. Todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue al personal afectado.

6 Marco Normativo

El marco normativo que aplica es aquel que está regido a través de todas aquellas normas que integren la seguridad de la información en el ámbito del servicio que presta la organización, en especial el Esquema Nacional de Seguridad (ENS) y cualquier norma que derive o esté tratada en este, indicado en el documento en formato Excel “Registro de Normas Jurídicas del Marco Legal y Regulatorio”.

7 Organización de la seguridad de la información

7.1 Criterios de la seguridad de la información

La organización, teniendo en cuenta los artículos que describe el ENS, establece las siguientes acciones para organizar la Seguridad de la Información:

Designará roles de seguridad: Responsables unificados de Servicios y de la Información, Responsable de la Seguridad, Responsable del Sistema y Delegado de Protección de Datos.

Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano se denominará Comité de Seguridad de la Información.

7.2 Definición de Roles y Responsabilidades asociados al ENS

7.2.1 Responsables de Información y de los Servicios (RS)

Responsable de la información

Se designa Responsable de la Información a la Vicepresidencia Ejecutiva u órgano en quien delegue, a quien le corresponden las siguientes funciones:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los tratamientos de datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Responsable último del uso que se haga de una cierta información y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Determinar los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del ENS.
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta al Responsable de la Seguridad y la opinión del Responsable del Sistema.
- Establecer los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) y 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 la información y los servicios.
- Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información, en su próxima reunión.

- Tiene la responsabilidad última del uso que se haga de determinados servicios e información y, por tanto, de su protección.

Responsable del servicio

Se designan responsables del Servicio a cada uno de los responsables de unidades funcionales (Jefes de servicio y jefes de unidad, según relación que se incluirá a continuación), a quienes les corresponde las siguientes funciones:

- En cuanto al RGPD, se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión de los tratamientos de datos personales que se realizan en su áre.
- Establecer los requisitos de cada servicio/unidad en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Responsable de garantizar la protección en los servicios prestados
- Responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta al Responsable de la Seguridad y oír la opinión del Responsable del Sistema.
- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

Responsables de los servicios:

- Gestión Económica y Presupuestaria: Jefatura del servicio.
- Régimen Jurídico: Jefatura del servicio.
- Contratación, Personal, Asuntos Generales e Informática: Jefatura de servicio.
- Prensa y Comunicación: Jefatura de unidad.
- Auditoría Interna: Jefatura de servicio.
- Promoción del Conocimiento del Talento: Jefatura del servicio.
- Cooperación entre Agentes del SVI: Jefatura del servicio.
- Proyectos Estratégicos de Innovación: Jefatura del servicio.
- Innovación en el Sector Público y Compra Pública de Innovación: Jefatura del servicio.
- Programación, Prospectiva y Estudios: Jefatura del servicio.
- Evaluación y Coordinación de Programas: Jefatura del servicio.

7.2.2 Responsable de la Seguridad de la información (RSEG)

Se designa al Responsable de la Seguridad de la Información (en adelante, Responsable de Seguridad) al Jefe de Unidad de Informática, a quien le corresponden las siguientes funciones:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias y elaborar documentación del sistema.
- Aprobar la Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad TIC.
- 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.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, la Política de Seguridad de la Información, para su aprobación por Dirección.
- Actuará como Secretario del Comité de Seguridad de la Información, realizando las siguientes funciones:
    - Convocar las reuniones del Comité de Seguridad de la Información.
    - Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
    - Elaborar el acta de las reuniones.
    - Es responsable de la ejecución directa o delegada de las decisiones del Comité.

7.2.3 Responsable del Sistema (RSIS)

Se designa al Responsable del Sistema al Técnico/a de Informática, a quien le corresponden las siguientes funciones:

- 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 Comité de Seguridad de la Información 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.
- Coordinar las funciones del administrador de la seguridad del sistema:
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

7.2.4 Administrador de la seguridad del sistema

Se designa como Administrador de la Seguridad del Sistema al Técnico/a de Informática, al que, como tal, le corresponden las siguientes funciones:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la política de seguridad establecida por la Organización.
- Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los Procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de información y los mecanismos y servicios de seguridad requeridos.

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Aprobar los cambios en la configuración vigente del Sistema de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Monitorizar el estado de la seguridad del sistema.

En caso de que ocurra algún incidente de seguridad de la información, deberá:

- Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
- Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
- Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos
- Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.

7.2.5 Delegado de Protección de datos (DPD)

Corresponde a la SUBDELEGACIÓN DE PROTECCIÓN DE DATOS DEL SECTOR PÚBLICO INSTRUMENTAL, velar por el cumplimiento de las siguientes funciones:

- Informar y asesorar a la organización, y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben 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 la organización, 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.

- El Delegado de Protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:
- Recabar información para determinar las actividades de tratamiento.
- Analizar y comprobar la conformidad de las actividades de tratamiento.
- Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
- Recabar información para supervisar el registro de las operaciones de
- tratamiento.
- Asesorar en el principio de la protección de datos por diseño y por defecto.
- Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
- Priorizar actividades en base a los riesgos.
- Asesorar al Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

7.2.6 Comité de Seguridad de la Información

7.2.6.1 Estructura y composición del Comité de Seguridad de la Información

- Presidencia: Persona titular de la Secretaría General Técnica de la AVI
- Secretario: Persona Responsable de Seguridad de la Información
- Vocales:
    - Persona titular de la Subdirección General de Programas de Innovación.
    - Jefatura del servicio de Promoción del Conocimiento y del Talento.
    - Jefatura del servicio de Evaluación y Coordinación de Programas.
    - Jefatura del servicio de Cooperación entre agentes del SVI.
    - Jefatura del Servicio de Contratación, Personal, Asuntos Generales e Informática
    - Jefatura de Sección de Gestión Económica Administrativa 3

A requerimiento del Comité podrá convocarse a las reuniones cualesquiera otros Jefes de Servicio, Unidad y responsables cuya intervención sea precisa por ser afectados por el Esquema Nacional de Seguridad y por el RGPD.

7.2.6.2 Atribuciones del Comité de Seguridad de la Información

Serán funciones del Comité de Seguridad:

- Atender las inquietudes de la Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.

- Elaborar la estrategia de evolución en lo que respecta a la seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar documentación de seguridad de la información.
- Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
- Estar permanentemente informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.
- Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que su presidente, deberá dar cumplida respuesta.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Atender las inquietudes, en materia de Seguridad de la Información, informando regularmente del estado de la seguridad de la información a la Dirección.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
- Revisar la Política de Seguridad de la Información previa aprobación por la vicepresidencia ejecutiva.
- Aprobar el Plan de Adecuación para la implantación del ENS.

7.2.6.3 Periodicidad de las reuniones y adopción de acuerdos

El Comité de Seguridad de la Información se reunirá, al menos, una vez al año, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.

En cualquier caso, las reuniones se convocarán por su Presidencia, a través del Secretario, a su iniciativa o por mayoría de sus miembros permanentes.

Las decisiones se adoptarán por consenso de los miembros.

7.2.6.4 Designación y resolución de conflictos

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política, se reflejará en acta.

Los roles nombrados se renovarán anualmente de forma automática. Las bajas o modificaciones en los roles designados, se comunicarán al Comité y se seguirán los cauces establecidos para la designación del nuevo miembro.

Tal y como se regula en el artículo 13.3 del RD del ENS, se estipula que no puede existir dependencia jerárquica entre el RSEG y el RSIS, salvo excepciones justificadas, lo que conllevará a disponer de medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades.

8 Datos personales y riesgos que se derivan del tratamiento

Para la adecuación y cumplimiento de la LOPD-GDD y RGPD, se publicará el registro de actividades de su tratamiento y se realizará la gestión de riesgos a través de Análisis de Riesgos y la Evaluación de Impacto en la Protección de Datos en el caso que fuese necesario esta, en la organización.

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal. El Registro de Actividades del Tratamiento (RAT) detalla los tratamientos afectados y los responsables correspondientes, así como las medidas adoptadas derivadas de las evaluaciones de impacto realizadas sobre los tratamientos. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado RAT.

Todos los sistemas afectados por la presente Política de Seguridad están sujetos a un análisis de riesgos periódico, con revisión anual, con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del RD del ENS.

9 Obligaciones del personal

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo, que interactúe con el sistema de información y que intervenga en los procesos de la organización, constituyendo su incumplimiento infracción grave a efectos laborales.

Todos los miembros de la organización tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

9.1 Contratación

Los contratos firmados con las entidades que prestarán servicios para la Organización deberán recoger en su clausulado la obligación de aceptación de normativa de seguridad, y cualquier otra documentación que sea requerida por el responsable de

seguridad, para el intercambio de información, retirada del material por terceros, supervisión y revisión de acuerdos, etc.

10 Documentación complementaria

La presente Política de Seguridad de la Información será complementada con documentos más precisos (normas, guías y procedimientos de seguridad) que ayudan a llevar a cabo lo propuesto.

El cuerpo normativo se desarrollará en tres niveles:

- Primer nivel normativo: constituido por la presente Política de Seguridad de la Información.
- Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores con el objetivo de indicar el uso correcto de aspectos concretos del sistema de gestión de seguridad de la información.
- Tercer nivel normativo: constituido por procedimientos de seguridad, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde a la Vicepresidencia Ejecutiva u órgano en quien delegue la aprobación de la Política de Seguridad de la Información, tal y como se establece en el artículo 12 del RD ENS. Siendo el Comité de Seguridad de la Información el órgano responsable de la aprobación y difusión de los restantes documentos propios de la organización.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

11 Terceras partes

En caso que la organización preste servicios a otros organismos o maneje información de otros organismos, se les hará participe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la organización, utilice servicios de terceros o ceda información a terceros, se les hará participe de esta Política de Seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se

incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Para cualquier relación con terceras partes se utilizarán los canales de comunicación habituales.

12 Aprobación y entrada en vigor

Esta Política de Seguridad de la Información, será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Estando vacante el puesto de la Vicepresidencia Ejecutiva de la AVI, le corresponde a la persona titular de la Secretaría General de la AVI, ejercer por suplencia las funciones atribuidas a esa Vicepresidencia Ejecutiva, en virtud de lo dispuesto en el artículo 17.4 del Reglamento de organización y funcionamiento de la AVI, aprobado por Decreto 106/2017, de 28 de julio, del Consell.

Asimismo, estando vacante el puesto de la Secretaría General de la AVI, le corresponde a la persona titular de la Secretaría General Técnica de la AVI, ejercer por suplencia las funciones atribuidas a esa Secretaría General, en virtud de lo dispuesto en la Resolución del vicepresidente ejecutivo de la AVI, de 19 de septiembre de 2022.

Firmat per Joaquín Martínez Gómez, el 14/03/2025 13:54:37
Càrrec: Secretari General Tècnic (AVI)

El secretario general técnico