POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CONFEDERACIÓN HIDROGRÁFICA DEL SEGURA, O.A

Edición	Fecha	Motivo del cambio	Elabora	Revisa	Aprueba
1.0	27/11/2023	Inicial	RSI	CRSI	Titular del Organismo
1.1	15/02/2024	Cambios Menores	RSI	CRSI	Titular del Organismo

Tabla de contenido

1. Objetivo. 5
2. Alcance. 5
3. Responsabilidades. 5
4. Determinación del alcance del Sistema de Gestión de Seguridad de la Información. 6
5. Misión de la Organización. 6
6. Marco Normativo. 7
7. Directrices para la estructura documental del Sistema de Gestión de la Seguridad de la Información. 7
8. Objetivos de seguridad. 8
9. Organización de la seguridad. 9
9.1. Máxima responsabilidad en materia de seguridad. 9
9.2. Roles: funciones y responsabilidades. 9
9.2.1. Responsable de Seguridad de la Información. 9
9.2.2. Responsable de Seguridad de la Información de Infraestructuras Críticas. 10
9.2.3. Responsable del Sistema. 10
9.2.4. Responsables de los Servicios. 11
9.2.5. Responsables de la Información. 12
9.2.6. Responsable de Seguridad y Enlace. 12
9.2.7. Delegado de Seguridad de Infraestructura Crítica. 12
9.2.8. Nombramientos. 13
9.3. Comité Responsable de Seguridad de la Información. 13
10. Protección de datos de carácter personal. 15
10.1. Figuras vinculadas a la protección de DCP. 15
10.1.1. Responsable del Tratamiento. 15
10.1.2. Delegado de Protección de Datos. 16
10.1.3. Personal de CHS con acceso a Datos de Carácter Personal. 19
10.1.4. Encargado de tratamiento. 19
11. Requisitos mínimos de seguridad. 20
12. Categorización del sistema. 22
13. Análisis y gestión de riesgos. 22
13.1. Criterios de evaluación del riesgo. 22
13.2. Actualización de la evaluación del riesgo. 22
14. Gestión de incidentes. 23

14.1. Prevención. 23
14.2. Monitorización y detección. 23
14.3. Respuesta. 23
14.4. Recuperación. 24
14.5. Conservación. 24
15. Obligaciones de personal. 24
16. Liderazgo. 24
17. Terceras partes. 25
18. Documentación complementaria. 26
19. Revisión y desarrollo de la Política de Seguridad de la Información. 26
20. Aprobación de la Política de Seguridad de la Información. 27

1. Objetivo.

El objetivo del presente documento es la definición de la Política de Seguridad de la Información (en adelante, PSI) de aplicación en la Confederación Hidrográfica del Segura, O.A. (en adelante, CHS) según lo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), formalizando así el reconocimiento estratégico de la información y los sistemas que la soportan.

Uno de los objetivos fundamentales de la presente PSI es establecer las directrices generales que garanticen la gestión de la seguridad de la información de manera íntegra y coordinada con los objetivos y líneas estratégicas del Organismo, la normativa aplicable y las directrices de seguridad internas de CHS.

Esta PSI asegura el compromiso manifiesto de CHS y sus máximos responsables por garantizar y supervisar el adecuado cumplimiento de las directrices necesarias que permiten el acceso seguro de los ciudadanos a los servicios de CHS, preservando sus derechos y minimizando los riesgos derivados de las amenazas existentes en cuanto a la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad de la información.

La protección frente a dichas amenazas, intencionadas o accidentales, requiere una estrategia que permita actuar tanto de forma preventiva como reactiva, supervisando y monitorizando todo el ciclo de vida de los sistemas con el fin de reaccionar de forma efectiva a los incidentes y dotar a CHS de los recursos necesarios para ello.

La presente PSI se complementa con Normas, Procedimientos y Guías de seguridad que definen las normas concretas de actuación.

2. Alcance.

Esta política se enmarca en el alcance del Sistema de Gestión de la Seguridad de la Información de CHS (en adelante, Sistema SGSI) definido por CHS en base a estándar de seguridad ISO 27001 y el ENS, siendo de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información, con independencia de cuál sea su destino, adscripción o relación con el mismo.

3. Responsabilidades.

Persona o comité	Responsabilidad
Titular del Organismo	• Revisa anualmente la PSI • Establece objetivos de seguridad
Comité Responsable de Seguridad de la Información (CRSI)	• Propone cambios en la PSI para revisión por el Titular del Organismo si procede
Responsable de Seguridad de la Información (RSI)	• Se encarga supervisar el cumplimiento de la PSI y habilitar los medios para que llegue al personal de CHS

Responsable del Sistema (RSIS)	• Se encarga de la operación del sistema de información
Responsable de Seguridad de la Información de Infraestructuras Críticas (RSI-IC)	• Coordina la protección de la información y medios de procesamiento en la infraestructura crítica
Responsable de Seguridad y Enlace (RSyE)	• Aplicar las políticas de la organización en los emplazamientos pertenecientes a CHS declarados como infraestructura crítica
Delegado de Protección de Datos (DPD)	• Proporcionar asesoramiento e información en materia de protección de datos al responsable o al encargado del tratamiento, supervisar el cumplimiento del RGPD
Otros	• Responsables del Servicio, Responsables de la Información, delegados de Seguridad y Personal de CHS que intervienen en la operativa conforme a la PSI en base a funciones definidas

4. Determinación del alcance del Sistema de Gestión de Seguridad de la Información.

El alcance de la presente PSI queda delimitado a los sistemas de información y recursos que dan soporte a los siguientes servicios e información:

a) Gestión de la Información Hidrológica de la cuenca.
b) Gestión del Plan Hidrológico de la cuenca.
c) Gestión de expedientes de Dominio Público Hidráulico, de calidad de las aguas y aprovechamientos de uso de agua.
d) Gestión y explotación de las obras hidráulicas para la gestión de recursos hídricos.
e) Gestión administrativa, económica y jurídica de CHS.

Todo ello, conforme a la declaración de aplicabilidad vigente y la valoración en vigor.

La ubicación de los sistemas y recursos humanos que intervienen en la gestión de estos procesos se encuentra se encuentran en la sede central situada en el Palacio de Fontes e instalaciones de CHS declaradas como infraestructura crítica.

5. Misión de la Organización.

La misión principal de CHS objeto de análisis y protección de la información que se trata en los servicios se relaciona a continuación:

- La elaboración del Plan Hidrológico de cuenca, así como su seguimiento y revisión.
- La administración y control del dominio público hidráulico.
- La administración y control de los aprovechamientos de interés general o que afecten a más de una Comunidad Autónoma.
- El proyecto, la construcción y explotación de las obras realizadas con cargo a los fondos propios de CHS, y las que les sean encomendadas por el Estado.

- Las que se deriven de los convenios con Comunidades Autónomas, Corporaciones Locales y otras entidades públicas o privadas, o de los suscritos con los particulares.

Estas actividades se encuadran dentro de un contexto de amenazas, riesgos de ciberseguridad y expectativas de las partes interesadas que se han desarrollado y muestran con más detalle en documento interno del SGSI definido.

6. Marco Normativo.

El marco normativo de las actividades está compuesto por diferentes normas y con el objeto de realizar un adecuado seguimiento del cumplimiento legal y regulatorio, de cara a la mejora de estas actividades, CHS dispone de un documento específico dentro de su Sistema SGSI que contempla toda la normativa aplicable y sobre el cual se realizan los seguimientos y actualizaciones correspondientes. Entre esa legislación y regulaciones, se destacan las de mayor relevancia en materia de ciberseguridad:

- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley de Protección de Infraestructuras Críticas (Ley PIC 8/2011)
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

7. Directrices para la estructura documental del Sistema de Gestión de la Seguridad de la Información.

El cuerpo normativo del Sistema SGSI se encuentra en repositorio interno gestionado por el Responsable de Seguridad de la Información (RSI) y validado por el Comité Responsable de la Seguridad de la Información (CRSI). El acceso será en función de la "necesidad de conocer" del personal que realiza tareas relacionadas con seguridad de la información. En este sentido, la autorización de acceso la dará el Responsable de Seguridad de la Información (RSI) y se guardará registro de auditoria (si es por aplicación, correo electrónico o cualquier otro medio).

8. Objetivos de seguridad.

A través de la presente PSI, CHS establece los siguientes objetivos globales de seguridad de la información que deberán implantarse y consolidarse como base para toda actuación en materia de ciberseguridad:

- Establecer un marco de referencia y actuación para la protección de los activos de los sistemas de información frente a amenazas, internas o externas, deliberadas o involuntarias, con la finalidad de garantizar la seguridad de la información independientemente del soporte y/o formato en que ésta se encuentre (bases de datos, documentos en papel, imágenes, dispositivos de almacenamiento, etc.).
- Definir e implantar, en el ámbito organizativo, operativo, técnico y/o humano, las correspondientes políticas, instrucciones, medidas, controles, etc. de seguridad como resultado de la metodología corporativa de gestión de riesgos aplicada sobre los activos de los sistemas de información.
- Gestionar de forma eficaz la respuesta frente a incidentes de seguridad o situaciones de emergencia con objeto de asegurar la continuidad de los sistemas de información críticos.
- Identificar e inventariar los repositorios y tratamientos de información con objeto de dotar a CHS de un sistema de clasificación de esta, permitiendo establecer y definir distintos escenarios de control en función de los criterios que se establezcan (formato, volumen, contenido, grado de actualización, etc.).
- Controlar los procesos de intercambio/comunicación de información con terceros (proveedores, organismos oficiales, empresas colaboradoras, etc.).
- Alinear la PSI y el cuerpo normativo de seguridad de la información con la legislación aplicable, estándares, *"best practices"* y criterios internacionales de reconocido prestigio.
- Fomentar una cultura corporativa de seguridad de la información a través de la concienciación y formación del personal, tanto interno como externo, mediante la realización de acciones formativas, campañas de divulgación, etc. en materia de seguridad de la información.

Estos objetivos se caracterizarán por:

- Estar alineados con la política.
- Ser medibles.
- Basados en análisis de riesgos.
- Comunicados a los implicados.

Anualmente, el Comité Responsable de Seguridad de la Información (CRSI) establecerá, documentará y aprobará un marco de referencia para establecer objetivos específicos de ciberseguridad aplicando los principios de mejora continua.

9. Organización de la seguridad.

9.1. Máxima responsabilidad en materia de seguridad.

Según la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el Titular del Organismo de CHS ostenta la máxima responsabilidad en el desarrollo de las competencias de la entidad, incluidas las de seguridad de la información. Es por tanto el máximo responsable de la implantación del ENS.

9.2. Roles: funciones y responsabilidades.

La PSI debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de CHS.

El Comité Responsable de Seguridad de la Información (Comité CRSI) será encargado de asignar responsabilidades nominativas para cada función de seguridad que serán formalmente nombrados conforme a la presente PSI.

9.2.1. Responsable de Seguridad de la Información.

Se nombrará formalmente como tal a una única persona en CHS. El rol no podrá ser desarrollado por un órgano colegiado, ni podrá haber más de una persona asumiendo el rol en CHS, aunque pueda delegar parte de sus funciones en otras personas.

Sus funciones serán las siguientes:

- Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información de CHS.
- Promover la formación y concienciación en materia de seguridad de la información.
- Elaborar y proponer para aprobación de CHS las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciber incidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del RDL 12/2018 y de su Reglamento de Desarrollo.

- Constituir el punto de contacto especializado para la coordinación con el CCN-CERT como CSIRT de referencia de la Administración General del Estado.
- Notificar a la autoridad competente, a través del CCN-CERT y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CCN-CERT, a su solicitud o por propia iniciativa.
- Actuar como secretario del Comité Responsable de Seguridad de la Información (CRSI).

9.2.2. Responsable de Seguridad de la Información de Infraestructuras Críticas.

Se nombrará formalmente como Responsable de Seguridad de la Información de Infraestructuras Críticas (RSI-IC) a una única persona en CHS, debiéndose nombrar también a un RSI-IC suplente. El rol no podrá ser desarrollado por un órgano colegiado, ni podrá haber más de una persona asumiendo el rol en CHS.

Sus funciones serán las siguientes:

Actuar como punto de contacto con la autoridad competente para supervisar los requisitos de seguridad de las redes y sistemas de información y como punto de contacto especializado para coordinar la gestión de incidentes con el CNPIC.

- Supervisar y desarrollar la aplicación de las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo controles periódicos de seguridad.
- Remitir a la autoridad competente, a través del CNPIC y sin dilación indebida, las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicios conforme legislación.
- Contar con personal con conocimientos especializados y experiencia en materia de ciberseguridad, desde los puntos de vista organizativo, técnico y jurídico, adecuados al desempeño de sus funciones.
- Ostentar una posición en la organización que facilite el desarrollo de sus funciones, participando de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad, y manteniendo una comunicación real y efectiva con la alta dirección.
- Mantener la debida independencia respecto de los responsables de las redes y los sistemas de información.

9.2.3. Responsable del Sistema.

Se nombrará formalmente como tal a una única persona. El rol no podrá ser desarrollado por un órgano colegiado, aunque pueda delegar parte de sus funciones en otras personas.

Sus funciones serán las siguientes:

- Basándose en el análisis de riesgos, establecerá las medidas de seguridad físicas y/o lógicas necesarias para proteger los activos de información
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por el Comité Responsable de Seguridad de la Información (CRSI) de CHS, debe ser acordada con los responsables de la información y los servicios afectados y el RSI.

El Responsable del Sistema (RSIS) tendrá la facultad de nombrar Responsables del Sistema Delegados. En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, cada organización podrá designar cuantos Responsables del Sistema Delegados considere necesarios. La designación corresponde al Responsable del Sistema, que delega funciones, no responsabilidad.

Por otro lado, el Responsable del Sistema (RSIS) podrá proponer, junto con el Responsable de Seguridad de la Información (RSI), al Titular del Organismo el nombramiento de Administradores de Seguridad para la implementación, gestión y mantenimiento de determinadas medidas de seguridad aplicables a una parte del sistema de información.

9.2.4. Responsables de los Servicios.

Los Responsables del servicio son las personas que determinan los requisitos de seguridad de sus servicios.

Sus funciones serán las siguientes:

- Establecer los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Tener la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección. El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Determinar los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del ENS. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta al Responsable de Seguridad de la Información (RSI) y conviene que escuche la opinión del Responsable del Sistema (RSIS).
- Atender a los requisitos de seguridad de la información que maneja en los servicios prestados, de forma que pueden heredarse los requisitos de seguridad de la información,

añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

9.2.5. Responsables de la Información.

Los Responsables de la Información son las personas que determinan los requisitos de la información objeto de su tratamiento.

Sus atribuciones y funciones serán las siguientes:

- Tener la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. El Responsable de la Información es el 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 de seguridad ENS corresponda al Responsable de la Información, podrá recabar una propuesta al Responsable de Seguridad de la Información (RSI) y conviene que escuche la opinión del Responsable del Sistema (RSIS).

9.2.6. Responsable de Seguridad y Enlace.

Se nombrará formalmente como Responsable de Seguridad y Enlace (RSyE) a una única persona en CHS, debiéndose nombrar también a un RSyE suplente.

El Responsable de Seguridad y Enlace (RSyE) representará y servirá de enlace ante la Secretaría de Estado de Seguridad en todas las materias de seguridad de sus infraestructuras y los diferentes planes especificados en este reglamento. Elaborará el Plan de Seguridad del Operador (PSO).

También canalizará las necesidades operativas e informativas que surjan entre el operador crítico y el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).

9.2.7. Delegados de Seguridad de Infraestructura Crítica.

Los Delegados de Seguridad de Infraestructura Crítica serán las personas designadas por el operador esencial como enlace operativo y el canal de información con las autoridades competentes en todo lo referente a la seguridad concreta de una infraestructura crítica, debiéndose nombrar también a un Delegado de Seguridad de Infraestructura Crítica suplente.

Los Delegados deberán velar por la correcta ejecución de los diferentes Planes de Protección Específicos (PPE) y tendrán facultades de inspección en el ámbito de la protección de infraestructuras críticas. Además, se considerará que serán los encargados de canalizar las necesidades operativas e informativas que surjan, a nivel infraestructura, entre el operador y las autoridades competentes.

9.2.8. Nombramientos.

Es función del Titular del Organismo de CHS nombrar formalmente:

- A los Responsables de la Información, que pueden ser un cargo unipersonal.
- A los Responsables de los Servicios, que, pudiendo ser el mismo que el Responsable de la Información, también puede ser un cargo unipersonal.
- Al Responsable de Seguridad de la Información (RSI), que debe reportar directamente al Comité Responsable de Seguridad de la Información (CRSI).
- Al Responsable del Sistema, que, en materia de seguridad, reportará al Responsable de Seguridad de la Información (RSI).
- Al Responsable de Seguridad de la Información de Infraestructuras Críticas (RSI-IC), y suplente, que debe reportar directamente al Comité Responsable de Seguridad de la Información (CRSI).
- Al Responsable de Seguridad y Enlace (RSyE), y suplente, que debe ser un cargo unipersonal.
- A las personas Delegados de Seguridad (DS), y suplentes, que deben ser un cargo unipersonal.

El procedimiento de nombramiento, por parte del Titular del Organismo, de los responsables mencionados en la relación anterior debe constar en un Apéndice de la PSI, y revestir carácter formal.

El Apéndice de nombramientos será mantenido y actualizado por el CRSI, reflejando en acta y bajo aprobación, cualquier cambio en los puestos y/o cargos asociados a los nombramientos. Estas situaciones tendrán carácter provisional y se dispondrán por el CRSI de cargos temporales hasta su aprobación por parte del Titular del Organismo en el momento de revisión de la presente PSI.

9.3. Comité Responsable de Seguridad de la Información.

El Comité Responsable de Seguridad de la Información (CRSI) es el órgano que coordina tanto la seguridad de la información como otros aspectos generales de seguridad (por ejemplo, la seguridad física y de las instalaciones de CHS).

La composición y funcionamiento del Comité Responsable de Seguridad de la Información (CRSI) será regulada a través de un documento estatutario aprobado por el titular del Organismo de CHS. En este sentido, estará constituido por representantes de las áreas afectadas por el ENS entre los que se encontrarán, al menos, los siguientes:

- El Responsable de Seguridad de la Información (RSI), que actuará como Secretario del Comité Responsable de Seguridad de la Información (CRSI).
- El Responsable del Sistema (RSIS).
- Responsable de Seguridad de la Información de Infraestructuras Críticas (RSI-IC).
- El Responsable de Seguridad y Enlace (RSyE).

- El Delegado de Protección de Datos de carácter personal (DPD).

Además, En relación con la asistencia, podrán ser invitados al Comité Responsable de Seguridad de la Información (CRSI), en función de las circunstancias:

- Responsables de Servicio o de Información.
- Personal relevante de CHS implicado en alguno de los aspectos relativos a la seguridad de la información, y siempre y cuando el secretario del Comité Responsable de Seguridad de la Información (CRSI) lo considere adecuado.

El Responsable de la Seguridad de la Información (RSI) será el secretario del Comité Responsable de Seguridad de la Información (CRSI), y como tal:

- Convoca las reuniones del Comité Responsable de Seguridad de la Información (CRSI).
- Prepara los temas a tratar en las reuniones del Comité Responsable de Seguridad de la Información (CRSI), aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité Responsable de Seguridad de la Información (CRSI).

Las funciones del Comité Responsable de Seguridad de la Información (CRSI) serán, al menos, las siguientes:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar anualmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del Sistema SGSI.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la presente PSI para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de CHS en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.

- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas del organismo, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Otras funciones que se definieran por añadido y/o actualización estatutaria bajo aprobación del Titular del Organismo.

Se incide que el Comité Responsable de Seguridad de la Información (CRSI) no es un comité exclusivamente técnico y deberá recabar regularmente de personal técnico, propio o externo, la información pertinente para la toma de decisiones o asesoramiento.

10. Protección de datos de carácter personal.

CHS, en el marco de su actividad, trata datos de carácter personal, es decir, información sobre una persona física identificada o identificable. Dichos tratamientos se encuentran detallados en el Registro de Actividades del Tratamiento, reflejando la información requerida por el 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 y por el que se deroga la Directiva 95/46/CE (en adelante, "RGPD") y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, "LOPDGDD").

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 (en adelante, "DCP") recogidos en el mencionado Registro de Actividades del Tratamiento.

La normativa sobre protección de datos identifica varias figuras vinculadas a la protección de DCP, debiendo ser conocidas estas junto con sus funciones por todos los miembros de CHS.

10.1. Figuras vinculadas a la protección de DCP.

10.1.1. Responsable del Tratamiento.

El Responsable del Tratamiento es la persona física o jurídica, autoridad pública, servicio u organismo que determina los fines y medios del tratamiento. Es por ello por lo que se ha atribuido la condición de Responsable del Tratamiento a CHS, debido a que determina los fines y medios del tratamiento de los DCP que obran en sus sistemas de información y que derivan de la prestación de los servicios públicos atribuidos a nivel de competencias. Por otra parte, cabe decir

que la consideración de Responsable del Tratamiento no debe ser asociada a persona física representante de CHS, en calidad del cargo o puesto.

Las funciones del Responsable del Tratamiento son, entre otras y en los términos establecidos en el RGPD y la LOPDGDD:

- Informar a los titulares sobre el tratamiento de sus datos;
- Mantener un registro de actividades de tratamiento efectuadas bajo su responsabilidad;
- Cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados;
- Cumplir con los principios relativos al tratamiento: determinando la licitud de los tratamientos, definiendo los plazos de conservación de los datos, etc.;
- Adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los DCP y eviten su alteración, destrucción, pérdida, o la comunicación o acceso no autorizado a estos;
- Documentar y notificar, si procede, violaciones de seguridad de los DCP a la autoridad de control y a los interesados;
- Realizar análisis de riegos y evaluaciones de impacto relativas a la protección de datos de las actividades de tratamiento y, en su caso, efectuar consultas previas a la autoridad de control;
- Regir la relación con los encargados de tratamiento mediante un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable;
- Aplicar las medidas técnicas y organizativas adecuadas para garantizar la protección de datos desde el diseño y por defecto.

10.1.2. Delegado de Protección de Datos.

El Delegado de Protección de Datos de carácter personal (DPD) es la figura que supervisa y asesora sobre el adecuado cumplimiento de la normativa sobre protección de datos en CHS, pudiendo ser este una persona física, jurídica u órgano colegiado.

El Delegado de Protección de Datos de carácter personal (DPD) tendrá como mínimo las siguientes funciones:

- Informar y asesorar al Responsable o al Encargado del Tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del Responsable o del Encargado del Tratamiento 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 supervisar su aplicación de conformidad con el artículo 35;
- Cooperar con la Autoridad de Control;

- Actuar como punto de contacto de la Autoridad de Control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

El responsable y el encargado del tratamiento respaldarán al Delegado de Protección de Datos de carácter personal (DPD) en el desempeño de las funciones mencionadas, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los DCP y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

El responsable y el encargado del tratamiento garantizarán que el Delegado de Protección de Datos de carácter personal (DPD) participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de DCP.

El Delegado de Protección de Datos de carácter personal (DPD) desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Para ello deberá ser capaz de:

- Recabar información para determinar las actividades de tratamiento y para supervisar el Registro de Actividades del Tratamiento;
- Analizar y comprobar la conformidad de las actividades de tratamiento;
- Informar, asesorar y emitir recomendaciones al Responsable o el Encargado del Tratamiento sobre las obligaciones de estos relativas a la protección de datos;
- Priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos;
- Asesorar al Responsable del Tratamiento sobre:
    - La evaluación de impacto relativa a la protección de datos,
    - Qué áreas deben someterse a auditoría de protección de datos interna o externa,
    - Qué actividades de formación internas proporcionar al personal o a los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos;
    - La aplicación del principio de la protección de datos por diseño y por defecto.
- Con relación a la evaluación de impacto relativa a la protección de datos, asesorar sobre:
    - Si se debe llevar a cabo o no una evaluación de impacto relativa a la protección de datos,
    - Qué metodología debe seguirse al efectuar una evaluación de impacto relativa a la protección de datos,
    - Si se debe llevar a cabo la evaluación de impacto relativa a la protección de datos con recursos propios o con contratación externa.,
    - Qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos de intereses de los afectados.,

- Si se ha llevado a cabo correctamente o no la evaluación de impacto relativa a la protección de datos, y
- Si las conclusiones de la evaluación de impacto relativa a la protección de datos (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes al RGPD.

El Delegado de Protección de Datos de carácter personal (DPD) deberá reunir conocimientos especializados en Derecho y la práctica en materia de protección de datos. Se han identificado, en consecuencia, aquellos conocimientos, habilidades o destrezas necesarias que tiene que saber o poseer el Delegado de Protección de Datos de carácter personal (DPD) para llevar a cabo una de las funciones propias de su puesto.

Estas funciones genéricas del Delegado de Protección de Datos de carácter personal (DPD) se pueden concretar en tareas de asesoramiento y supervisión, entre otras, en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos;
- Identificación de las bases jurídicas de los tratamientos;
- Valoración de la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos;
- Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos;
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos;
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados;
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados;
- Contratación de Encargados del Tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación Responsable-Encargado;
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia;
- Diseño e implantación de políticas de protección de datos;
- Auditoría de protección de datos;
- Elaboración y gestión de los registros de actividades de tratamiento;
- Análisis de riesgos de los tratamientos realizados;
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos;
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos;
- Establecimiento de procedimientos de gestión de brechas de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las Autoridades de Control y a los afectados;

- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos;
- Realización de evaluaciones de impacto relativas a la protección de datos;
- Relaciones con las Autoridades de Control;
- Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

10.1.3. Personal de CHS con acceso a Datos de Carácter Personal.

Todo el personal de CHS que tenga acceso a Datos de Carácter Personal (DCP) debe cumplir con las obligaciones que se detallan en la documentación sobre protección de datos y seguridad de la información dirigida al personal de CHS.

10.1.4. Encargado de tratamiento.

El Encargado del Tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate DCP por cuenta del Responsable del Tratamiento. Es decir, el Encargado del Tratamiento tiene como misión realizar las tareas ordinarias para el desarrollo efectivo de las funciones para las que ha sido creado el tratamiento por cuenta del Responsable del Tratamiento.

El Encargado del Tratamiento deberá aplicar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los DCP y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Las funciones del Encargado del Tratamiento son, entre otras:

- Mantener un registro de actividades de tratamiento de todas las categorías de actividades de tratamiento efectuadas por cuenta de CHS;
- Tratar los DCP siguiendo instrucciones documentadas del responsable;
- Garantizar que las personas autorizadas para tratar DCP se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;
- Asistir al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados;
- Ayudar al responsable a garantizar el cumplimiento de las obligaciones establecidas en RGPD;
- Poner a disposición del responsable toda la información necesaria para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable;
- Aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo con relación a los tratamientos de los DCP y eviten su alteración, pérdida, destrucción, o la comunicación o acceso no autorizado.

En consecuencia, CHS deberá realizar un documento actualizado donde identificarán a los encargados de tratamiento que prestan servicios en la Administración y la indicación de la formalización del contrato con estos prestadores de servicios con acceso a datos.

11. Requisitos mínimos de seguridad.

Atendiendo al cumplimiento del ENS, se garantizará el cumplimiento de los siguientes requisitos mínimos:

- Organización: diseño e implantación del proceso de seguridad de la información.
- Análisis y gestión de los riesgos: tratamiento adecuado de los riesgos de ciberseguridad.
- Gestión de personal: implantando seguridad en los procesos de incorporación y baja del personal, así como acciones relativas a formación y concienciación.
- Profesionalidad: la seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida (instalación, mantenimiento, gestión de incidentes y desmantelamiento). El personal de CHS recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios.
- Seguridad por terceros: CHS exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados. Además, se estará a lo dispuesto en el ENS relativo a contratación de terceros.
- Autorización y control de los accesos: el acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.
- Protección de las instalaciones: los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas permanecerán cerradas y dispondrán de un control de llaves.
- Adquisición de productos de seguridad y contratación de servicios de seguridad: se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de Seguridad de la Información (RSI).
- Seguridad por defecto mínimo privilegio: los sistemas se diseñarán y configurarán de manera que garanticen la seguridad por defecto y mínimo privilegio:
    - El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias y se asegurará que solo las pueden acceder las personas, o desde emplazamientos o equipos autorizados, pudiendo exigirse restricciones de horario y puntos de acceso facultados.

- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
- Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.
- Se garantizará que el uso ordinario del sistema sea sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
- Integridad y actualización del sistema: todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. En todo momento se conocerá el estado de seguridad de los sistemas, según las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo ante el estado de seguridad de estos.
- Protección de la información almacenada y en tránsito: en la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, tabletas, asistentes personales (PDA), teléfonos móviles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.
- Soporte Papel: toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el ENS, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.
- Prevención ante otros sistemas de información interconectados: el sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.
- Registro de actividad y detección de código dañino: con la finalidad exclusiva de lograr el cumplimiento del objeto del ENS con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de DCP, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa , así como facilitar la denegación de acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

- Gestión de incidentes de seguridad y Continuidad de la actividad: los sistemas de CHS dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.
- Mejora continua del proceso de seguridad: el proceso integral de seguridad implantado será actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

12. Categorización del sistema.

La categorización del sistema se establece en función de la valoración de servicios e información que hacen cada uno de los responsables de estos.

Para la valoración de servicios e información se seguirán las indicaciones del Real Decreto 311/2022, Anexo I punto 1 Fundamentos para la determinación de la categoría de seguridad de un sistema de información que establece que para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

- Las dimensiones de seguridad relevantes en el sistema a proteger.
- La categoría de seguridad del sistema de información a proteger.

13. Análisis y gestión de riesgos.

Todos los sistemas sujetos a esta PSI deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el ENS.

13.1. Criterios de evaluación del riesgo.

La metodología para la evaluación del riesgo es MAGERIT 3 implementada mediante la herramienta PILAR y recomendada por el Centro Criptológico Nacional.

13.2. Actualización de la evaluación del riesgo.

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.

- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

14. Gestión de incidentes.

14.1. Prevención.

Se debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. A tal fin, los sistemas, al menos deben estar:

- Autorizados formal y adecuadamente antes de entrar en operación.
- Evaluados regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Revisados periódicamente por parte de terceros con el fin de obtener una evaluación independiente.

14.2. Monitorización y detección.

Dado que los servicios se pueden degradar rápidamente debido a incidentes que van desde una disminución hasta el cese del nivel de prestación, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa basadas en mecanismos de detección, análisis y reporte que puedan informar a los responsables tanto regularmente como cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

14.3. Respuesta.

Con relación a la respuesta sobre los incidentes, se deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar puntos de contacto para las comunicaciones con respecto a incidentes detectados en otras unidades o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

14.4. Recuperación.

Para garantizar la disponibilidad de los servicios críticos, las unidades deben desarrollar Planes de Continuidad de los sistemas informáticos y de telecomunicaciones como parte de su Plan General de Continuidad de Negocio y actividades de recuperación.

14.5. Conservación.

Sin merma de los restantes principios básicos y requisitos mínimos establecidos, los sistemas de información de CHS garantizarán la conservación de los datos e información en soporte electrónico.

De igual modo, los sistemas mantendrán disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

15. Obligaciones de personal.

Todos los miembros de CHS afectados por el alcance tienen la obligación de conocer y cumplir esta PSI y la Normativa de Seguridad, siendo responsabilidad del CSRI disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de CHS atenderán a una sesión de concienciación en materia de seguridad informática al menos una vez cada tres años. Se establecerá un programa de concienciación continua para atender a todos los miembros de CHS, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas informáticos y de telecomunicaciones recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El cumplimiento de la presente PSI es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos de CHS, constituyendo su incumplimiento infracción grave a efectos laborales.

16. Liderazgo.

El Titular del Organismo de CHS se compromete a liderar el mantenimiento del Sistema SGSI. Para ello, se compromete a impulsar las siguientes acciones dentro de un sistema de mejora continua:

- Revisar anualmente del estado del Sistema SGSI para garantizar que se cumple la PSI de CHS, sus objetivos y que éstos están alineados con la dirección estratégica de CHS.

- Requerir en los nuevos proyectos que afronte CHS para que dispongan, desde su nacimiento, de una visión global de la seguridad de la información. A tal fin, se validará que todos los nuevos proyectos críticos para CHS cuenten con el correspondiente informe de seguridad por parte del Responsable de Seguridad de la Información (RSI).
- Estudiar la asignación de recursos económicos para la consecución de los objetivos del Sistema SGSI. Si por motivos presupuestarios esto no fuera posible, se estudiarán medidas alternativas tendentes a minimizar el riesgo. Así mismo se elevará a los organismos competentes las revisiones de seguridad que justifiquen la inversión necesaria.
- Mantener el espíritu de seguridad en la Organización mediante el impulso campañas de concienciación del personal.
- Apoyar la labor del Comité Responsable de Seguridad de la Información (CRSI) y del Responsable de Seguridad de la Información (RSI), así como del resto de implicados para garantizar las funciones establecidas en la presente PSI.
- Implantar un proceso de mejora continua con la propuesta documentada de acciones y objetivos tras la revisión por el Titular del Organismo del Estado de la Seguridad que será presentado, al menos, anualmente por el Comité Responsable de Seguridad de la Información (CRSI).

17. Terceras partes.

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipes de esta PSI, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios o ceda información a terceros, se les hará partícipes de esta PSI y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. A tal fin, se exigirá, al menos, lo siguiente:

- 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 PSI.

Cuando algún aspecto de la PSI no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información (RSI) 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.

18. Documentación complementaria.

La PSI se complementará con documentos más precisos que ayuden a implementar las directrices propuestas. Para ello se utilizarán los siguientes marcos de referencia:

- Controles de seguridad ISO 27001:2022.
- Recomendaciones del CCN en su guía *"821 Esquema Nacional de Seguridad – Guías de Seguridad".*

A nivel práctico, estos documentos se implementarán internamente en:

- Normas de seguridad (*security standards*): uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.
- Procedimientos de seguridad (*security procedures*): afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.
- Guías de seguridad (*security guides*): tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos.

Toda la documentación del Sistema SGSI se encontrará documentada y gestionada bajo un sistema de control de acceso basado en la "necesidad de conocer".

19. Revisión y desarrollo de la Política de Seguridad de la Información.

El Comité Responsable de Seguridad de la Información (CRSI) revisará la PSI a intervalos planificados, que deberán ser inferiores a dos años o siempre que se produzcan cambios significativos, para asegurar que se mantenga su idoneidad, adecuación y eficacia.

Dada la naturaleza de CHS, es imprescindible tener en cuenta y velar por la coherencia de la PSI de CHS, con la equivalente del Ministerio para la Transición Ecológica y el Reto Demográfico.

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

20. Aprobación de la Política de Seguridad de la Información.

En virtud de la función de la Secretaría General de supervisión y coordinación de la informática en materia administrativa, según el artículo 6.g del Real Decreto 984/1989, de 28 de julio, por el que se determina la estructura orgánica dependiente de la Presidencia de las Confederaciones Hidrográficas, la aprobación de la PSI por parte del titular del organismo es propuesta por la Secretaria General.

En Murcia, a fecha de la firma electrónica.

PROPONE LA APROBACIÓN DE LA PSI:

LA SECRETARIA GENERAL

MÓNICA GONZALO MARTÍNEZ

RESUELVE LA APROBACIÓN DE LA PSI:

EL PRESIDENTE,

MARIO ANDRÉS URREA MALLEBRERA

(firmas electrónicas)