POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FUNDACIÓ CANVI CLIMATIC

Adaptación al Esquema Nacional de Seguridad

ELABORADO POR:	REVISADO Y APROBADO POR:
Responsable Seguridad Información	**Responsable de la información**
Carlos Sánchez Cerveró	**Roberto Jaramillo Martínez**

HISTÓRICO DE MODIFICACIONES		
FECHA	**EDICIÓN**	**DESCRIPCIÓN DE CAMBIOS**
04/03/2019	00	Edición inicial.

ÍNDICE PG.:

1. OBJETO

El objeto del presente documento es la definición de la Política de Seguridad de la Información de la Fundació de la C.V. Observatori Valencià del Canvi Climàtic, dentro del alcance señalado en el Esquema Nacional de Seguridad, el Reglamento General Europeo de Protección de Datos y la Ley Orgánica de Protección de Datos de Carácter Personal.

Se ha implantado la presente Política atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de la Fundació de la C.V. Observatori Valencià del Canvi Climàtic que resulten de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

2. MISIÓN

La Fundació de la C.V. Observatori Valencià del Canvi Climàtic, para la gestión de sus intereses y de las funciones y competencias que tiene encomendadas, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y expectativas de la población y de todos los grupos de interés.

Para ello, pone a disposición de los mismos la realización de trámites online con el objetivo de impulsar la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen la eficacia de la acción pública.

Se desea potenciar por otro lado el uso de las nuevas tecnologías en la organización y en la propia ciudadanía.

Los principales objetivos que se persiguen son, entre otros, los siguientes:

- Fomentar la relación electrónica de la ciudadanía con la organización.
- Crear la confianza necesaria entre ciudadano y nuestra organización en esta relación.

3. ÁMBITO DE APLICACIÓN

Esta Política es de aplicación a todo el ámbito de actuación de la Fundació de la C.V. Observatori Valencià del Canvi Climàtic, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad de la Fundació de la C.V. Observatori Valencià del Canvi Climàtic.

La presente Política es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en Fundació de la C.V. Observatori Valencià del Canvi Climàtic, especialmente, los responsables de los Servicios de Explotación de los Sistemas de Información y los propios usuarios, como actores ambos, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de InformaciónSeguridad de la Información de la Fundació de la C.V. Observatori Valencià del Canvi Climàtic.

En el ámbito de la presente Política, se entiende por usuario cualquier empleado público perteneciente o ajeno a la Fundació de la C.V. Observatori Valencià del Canvi Climàtic, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la Fundació de la C.V. Observatori Valencià del Canvi Climàtic y que utilice o posea acceso a sus Sistemas de Información.

4. PRINCIPIOS Y DIRECTRICES

Los principios y directrices que deben de contemplarse a la hora de garantizar la seguridad de la información son **la prevención, la detección, la respuesta y la recuperación**, de manera que las amenazas existentes no se materialicen, o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan:

Prevención

La Fundació de la C.V. Observatori Valencià del Canvi Climàtic debe prevenir, y evitar, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad.

Para ello, sus órganos directivos deben implementar las medidas mínimas de seguridad determinadas por el Esquema Nacional de Seguridad (en adelante, ENS) regulado mediante Real Decreto 3/2010, de 8 de enero, 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.

Para garantizar el cumplimiento de la Política de Seguridad de la Información, los órganos directivos responsables deben:

- Autorizar los sistemas o los servicios antes de entrar en operación.

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica del cumplimiento del ENS por parte de terceros.

Detección

Dado que los sistemas y servicios pueden degradarse rápidamente debido a incidentes, que pueden ir desde una simple desaceleración hasta su detención, los órganos directivos responsables deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

En el supuesto de que la degradación sea atribuida a incidentes de seguridad, estos órganos directivos deberán establecer mecanismos de reporte que lleguen al responsable de seguridad.

Respuesta

Los órganos directivos responsables deben establecer mecanismos para responder eficazmente a los incidentes de seguridad.

Recuperación

Para garantizar la disponibilidad de los servicios críticos, los órganos directivos responsables deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

5. ACTUALIZACIÓN DEL DOCUMENTO

Cuando se produzca un cambio significativo en la estructura o en la operativa de la Fundació de la C.V. Observatori Valencià del Canvi Climàtic que afecte a esta Política, deberá producirse una modificación y actualización del mismo.

Se levantará acta de los cambios y modificaciones identificados, y éstos serán incluidos en una nueva versión del documento, así como en el apartado de control de cambios, como evidencia del proceso de actualización realizado y para mantener la trazabilidad entre distintas versiones.

Será el Responsable de Seguridad de la Información la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

6. REFERENCIAS

Las referencias tenidas en cuenta para la redacción de este Procedimiento han sido:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 (RGPD).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Documentos y Guías CCN-STIC.

7. DEFINICIONES

- **Documento**: Datos que poseen significado y su medio de soporte.
- **Proceso**: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.
- **Procedimiento**: Forma especificada, documentada o no, de llevar a cabo una actividad o un proceso.
- **Indicador**: Dato o conjunto de datos, que ayudan a medir objetivamente la ejecución o la evolución de un proceso o de una actividad.
- **Registro**: Documento que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas.

8. ROLES Y RESPONSABILIDADES

8.1. Roles de seguridad de la Información

Los Roles y Responsabilidades fundamentales en la Seguridad de la Información de la Fundació de la C.V. Observatori Valencià del Canvi Climàtic son los siguientes:

- **RESPONSABLE DE LA INFORMACIÓN**

El Responsable de la Información es habitualmente una persona que ocupa un alto cargo en la dirección de la organización. Corresponde al nivel de un órgano de gobierno de máximo nivel, constituido por la **Alta Dirección**, que entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde que éstos se alcancen.

Se decide que esta responsabilidad recaiga en el **Vicepresidente de la Fundación.**

La Guía CCN-STIC-801 permite que ambas figuras coincidan, y en todo caso, el Responsable de la Información estará supeditado al Responsable del Tratamiento.

Sus funciones pueden ser asignadas a personas individuales, o bien ser asumidas por el Comité de Seguridad de la Información.

La persona u órgano que lo asuma deberá ser identificada para cada Información que trate la organización.

Funciones asociadas

Sus funciones serán las siguientes:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los 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.
- Tiene 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.
- Establece 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.

- Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

Compatibilidad con otros roles

Este rol podrá coincidir con el del Responsable de Servicio y con el de Responsable de Tratamiento requerido por la Ley Orgánica de Protección de datos en organizaciones de tamaño reducido o intermedio que funcionen de forma autónoma.

Este rol no podrá coincidir con el de Responsable de Seguridad, salvo en organizaciones de reducida dimensión que funcionen de forma autónoma.

Este rol no podrá coincidir con el de Responsable de Sistema ni con el de Administrador de la Seguridad del Sistema, ni siquiera cuando se trate de organizaciones de reducida dimensión que funcionen de forma autónoma.

- **RESPONSABLE DEL SERVICIO**

Cuando sea distinto del Responsable de la Información, puede corresponder al nivel de un órgano de gobierno de máximo nivel, al igual que el Responsable de la Información, o bien al de una Dirección Ejecutiva o Gerencia, que entiende qué hace cada departamento, y cómo los departamentos se coordinan entre sí para alcanzar los objetivos marcados por la Dirección.

Se propone que esta condición recaiga en el **Vicepresidente de la Fundación.**

Sus funciones podrán ser asignadas a personas individuales, o bien ser asumidas por el Comité de Seguridad de la Información.

La persona u órgano que lo asuma deberá ser identificada para cada Servicio que preste la organización.

Funciones asociadas

Sus funciones serán las siguientes:

- Establece 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.

- Tiene la responsabilidad última del uso que se haga de determinados servicios 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 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 conviene que escuche 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.

Compatibilidad con otros roles

Podrá coincidir en la misma persona u órgano el rol de Responsable de la Información y del Responsable del Servicio, aunque generalmente no coincidirán cuando:

- El servicio gestione información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.

- La prestación del servicio no dependa de la unidad a la que pertenece el Responsable de la Información.

Este rol podrá coincidir con el del Responsable de Tratamiento requerido por la Ley Orgánica de Protección de Datos sólo en organizaciones de tamaño reducido o intermedio que funcionen de forma autónoma.

Este rol no podrá coincidir con el de Responsable de Seguridad, salvo en organizaciones de reducida dimensión que funcionen de forma autónoma.

Este rol no podrá coincidir con el de Responsable de Sistema ni con el de Administrador de la Seguridad del Sistema, ni siquiera cuando se trate de organizaciones de reducida dimensión que funcionen de forma autónoma.

- **RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN**

Corresponde al nivel de una Dirección Ejecutiva o Gerencia. Se nombrará formalmente como tal, por parte del órgano de gobierno, a una única persona en la organización.

El rol no podrá ser desarrollado por un órgano colegiado, ni podrá haber más de una persona asumiendo el rol en la organización, aunque pueda delegar parte de sus funciones en otras personas.

Se propone que las funciones de Responsable de Seguridad estén asignadas al **Director Gerente.**

Tal como se describe en la Guía CCN-STIC-801: "*La figura del "Responsable de la Seguridad" aparece en ambas normativas (ENS y LOPD) con un papel muy similar como persona que vela para que los sistemas de información efectivamente respondan a los requisitos establecidos. Las organizaciones harán bien en hacer coincidir estas responsabilidades en una única figura, recopilando todas las funciones en la Política de Seguridad"*.

Por tanto, se decide asimismo que el Responsable de Seguridad de la Información ejerza también de responsable de seguridad a efectos de cumplimiento de la normativa en materia de protección de datos de carácter personal.

Funciones asociadas

Sus funciones serán las siguientes:

- Coordinará y controlará las medidas definidas en el Documento de Seguridad y en general se encargará del cumplimiento de las medidas de seguridad que detalla el reglamento de desarrollo de la LOPD.
- Reportará directamente al Comité de Seguridad de la Información.
- Actuará como Secretario del Comité de Seguridad de la Información o persona delegada por él.
- Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.
- Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización.
- Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

- Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema.
- Realizará el Análisis de Riesgos.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
- Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Coordinará la elaboración de la Documentación de Seguridad del Sistema.
- 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.
- Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.
- Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.
- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.
- Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.
- Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

En caso de ocurrencia de incidentes de seguridad de la información:

- Analizará y propondrá salvaguardas que prevengan incidentes similares en un futuro.

Compatibilidad con otros Roles

Este rol únicamente podrá coincidir con la del Responsable de Servicio y el Responsable de Información en organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento.

Este rol no podrá coincidir con el de Responsable de Sistema y el de Administrador de Seguridad del Sistema, aunque se trate de organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento.

Delegación de Funciones

Para 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 de la Seguridad, se podrán designar los Responsables de Seguridad Delegados que se consideren necesarios.

La designación corresponde al Responsable de la Seguridad. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final seguirá recayendo sobre el Responsable de la Seguridad.

Los Responsables de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad, pudiendo ser, por ejemplo, la seguridad de sistemas de información concretos o de sistemas de información horizontales.

Cada Responsable de Seguridad Delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reportan.

- **RESPONSABLE DEL SISTEMA**

El responsable del sistema es la persona que se encarga de la explotación del sistema de información. Corresponde al nivel de una Dirección Operativa.

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

Se propone que las funciones de Responsable del Sistema estén asumidas por el **Técnico Ambiental.**

Funciones asociadas

Sus funciones serán las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
- Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- Elaborar los Planes de Continuidad del Sistema para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.
- Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.

- Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

En caso de ocurrencia de incidentes de seguridad de la información:

- Planificará la implantación de las salvaguardas en el sistema.
- Ejecutará el plan de seguridad aprobado.

Compatibilidad con otros roles

Este rol no podrá coincidir con el de Responsable de Información, con el de Responsable de Servicio ni con el de Responsable de Seguridad de la Información.

Este rol podrá coincidir con el de Administrador de Seguridad del Sistema en organizaciones de una dimensión reducida o intermedia que tengan una estructura autónoma de funcionamiento.

En grandes organizaciones no debería coincidir con el de Administrador de la Seguridad del Sistema, independientemente del tamaño del Sistema.

- **ADMINISTRADOR DE SEGURIDAD DEL SISTEMA**

Corresponde al nivel de un empleado cualificado en seguridad informática de sistemas.

Podrá nombrarse formalmente como tal varias personas para cada Sistema. El rol no podrá ser desarrollado por un órgano colegiado, ni podrá delegar parte de sus funciones en otras personas. En su caso, se nombrarían nuevos Administradores de la Seguridad del Sistema.

Se propone que las funciones de Administrador de la Seguridad del Sistema estén asumidas por el **Técnico de Energía.**

Funciones asociadas

Sus funciones serán las siguientes:

- 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 ocurrencia de incidentes de seguridad de la información:

- Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
- Ejecutar el plan de seguridad aprobado.
- 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 (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).
- 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.

Compatibilidad con otros roles

Este rol no podrá coincidir con el de Responsable de Información, con el de Responsable de Servicio ni con el de Responsable de Seguridad de la Información.

Este rol podrá coincidir con el de Responsable del Sistema en organizaciones de una dimensión reducida o intermedia que tengan una estructura autónoma de funcionamiento.

En grandes organizaciones no debería coincidir con el de Responsable del Sistema, independientemente del tamaño del Sistema.

Delegación de Funciones

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 sus funciones, se podrán designar Administradores de Seguridad del Sistema Delegados.

Los Administradores de Seguridad del Sistema Delegados serán responsables, en su ámbito, de aquellas acciones que delegue el Administrador de Seguridad del Sistema relacionadas con la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

El Administrador de Seguridad del Sistema Delegado será designado a solicitud del Administrador de Seguridad del Sistema, del que dependerá funcionalmente.

Su identidad aparecerá reflejada en la documentación de seguridad del sistema de información.

- **RESPONSABLE DE SEGURIDAD FÍSICA**

Cuando la seguridad física (de las instalaciones) esté segregada de la seguridad lógica, esta se ajustará a lo establecido por el ENS en materia de seguridad física de forma análoga a lo establecido en los puntos anteriores.

El Responsable de la Seguridad Física implantará las medidas de seguridad que le competan dentro de las determinadas por el Responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

Se propone que las funciones de Responsable de Seguridad Física estén asumidas por el **Director Gerente de Las Naves.**

- **RESPONSABLE DE GESTIÓN DE PERSONAL**

Los responsables de gestión del personal se ajustarán a lo establecido por el ENS en materia de personal de forma análoga a lo establecido en los puntos anteriores.

Los responsables de personal implantarán las medidas de seguridad que les competan dentro de las determinadas por el Responsable de Seguridad de la Información, e informarán a éste de su grado de implantación, eficacia e incidentes.

Se propone que las funciones de Responsable de Gestión de Personal estén asumidas por el **Director Gerente.**

- **DELEGADO DE PROTECCIÓN DE DATOS (DPO)**

El delegado de protección de datos tendrá como mínimo las siguientes funciones (contempladas en el art. 39 del Reglamento General de Protección de Datos.):

- 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 presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, 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 personales, 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, y realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos 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.

La designación para el desempeño de este rol se efectuará por el Comité de Seguridad siendo la persona designada un miembro de **la organización externa contratada para tal efecto** (ver acta de constitución del comité de seguridad de la información).

7.2 Comité de Seguridad

En el caso de los Sistemas de los Organismos Autónomos que queden fuera del ámbito de los servicios gestionados por la Fundació de la C.V. Observatori Valencià del Canvi Climàtic, el representante de dichos organismos en el Comité de Seguridad de la Información asumirá el rol de Responsable de Seguridad y Sistemas de dichos servicios.

Las políticas y roles de seguridad de protección de datos residen en el **Comité de Seguridad,** el cual estará constituido por los siguientes cargos y personas:

- Responsable de la Información/Responsable del Servicio
- Responsable de Seguridad de la Información / Responsable del tratamiento
- Delegado de Protección de Datos
- Secretaria del Comité
- Responsable del Sistema
- Administrador del sistema
- Responsable de Seguridad Física.
- Responsable de Gestión de Personal.

Sus funciones serán las siguientes:

- Atender las inquietudes de la Alta 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 de la Organización en lo que respecta a la 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, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada 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 respecto de ellos.
- 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 incidentes de 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 planes de mejora de la seguridad de la información de la Organización. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

- Velar para que 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 de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

En caso de ocurrencia de incidentes de seguridad de la información:

- Aprobará el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente.

El Comité de Seguridad de la Información no es un comité técnico, pero recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría interna y/o externa.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

El Responsable de la Seguridad de la Información es el secretario del Comité de Seguridad de la Información y como tal:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, 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.

Se convocará al resto de personas con responsabilidades en los roles del ENS según las necesidades del Comité de Seguridad de la Información.

De igual manera, se convocará a las personas responsables de Seguridad de ENS de cada área municipal en función de las necesidades del Comité de Seguridad de la Información.

Podrán convocarse reuniones extraordinarias cada vez que las necesidades o las circunstancias así lo exijan.

Funciones de las Responsabilidades asociadas al ENS

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de las figuras:

- La persona ***Responsable del Servicio***, determina los requisitos de seguridad de los servicios prestados dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad. Los Responsables de los Servicios, serán los responsables de cada área afectada por el ENS, y por lo tanto, se encargarán de velar por el cumplimiento del ENS en sus respectivas áreas.
- El ***Responsable de la Información***, determina los requisitos de seguridad de la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad ENS.
- El ***Responsable de Seguridad de la Información***, su función es planificar lo que se ha de hacer en materia de seguridad, así como supervisar que se haya hecho.
- El ***Responsable del Sistema***, es el encargado de las operaciones del sistema.

Funciones del Comité de Seguridad de la Información

El Comité de Seguridad tendrá las siguientes funciones:

- **Atender las inquietudes, en materia de Seguridad de la Información**, de la Organización y de los diferentes departamentos informando regularmente del estado de la Seguridad de la Información a la Alcaldía.
- **Asesorar en materia de Seguridad de la Información**, siempre y cuando le sea requerido.
- **Representar frente a terceros** (entidades privadas y otras Administraciones Públicas) l**a figura de responsable de seguridad en acciones transversale**s. La representación será avalada previo informe favorable del estado de la seguridad emitidos de manera solidaria por parte de los Responsables de Seguridad.
- **Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables** y/o entre diferentes Áreas/Departamentos de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- **Recoger las funciones y obligaciones de los Responsables de la Información y los Servicios, en aquellas acciones transversales**, en las que le sea solicitado y/o se considere necesario.

- **Promover la mejora continua del sistema de gestión de la Seguridad de la Información.** Para ello se encargará de:

- **Coordinar los esfuerzos** de las diferentes áreas/servicios en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- **Proponer planes de mejora** de la Seguridad de la Información de la Organización, con su dotación presupuestaria correspondiente, priorizando 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 desde su especificación inicial hasta su puesta en operación (**Privacy by Design**). 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.
- **Realizar un seguimiento de los principales riesgos** residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- **Realizar un seguimiento de la gestión de los incidentes de seguridad** y recomendar posibles actuaciones respecto de ellos.

- **Elaborar (y revisar regularmente) la Política de Seguridad de la Información** para su aprobación por el Órgano Superior de la Organización.
- **Elaborar la normativa de Seguridad de la Información** para su aprobación en coordinación con la Fundació de la C.V. Observatori Valencià del Canvi Climàtic.
- **Verificar la idoneidad de los procedimientos de seguridad de la información** y demás documentación.
- **Elaborar programas de formación destinados a formar y sensibilizar al personal** en materia de Seguridad de la Información y en particular de protección de datos de carácter personal.
- **Elaborar y aprobar los requisitos de formación y calificación de administradores,** operadores y usuarios desde el punto de vista de Seguridad de la Información.
- **Promover la realización de las auditorías periódicas** que permitan verificar el cumplimiento de las obligaciones de la Organización en materia de seguridad.

Procedimientos de designación

La Fundació de la C.V. Observatori Valencià del Canvi Climàtic procederá a realizar la constitución del comité y de las distintas responsabilidades. Todos los nombramientos se revisarán cada 4 años o cuando los puestos queden vacantes.

9. CONTENIDO

9.1. Generalidades

Un enfoque preventivo y garantista del cumplimiento no debe dejar pasar la oportunidad de establecer unos adecuados controles desde las primeras fases de diseño de un nuevo servicio o producto. Es necesario para ello conocer cuál es o será el ciclo vital de los datos desde que se recaben, se traten, se custodien o se cedan o cancelen.

Cada fase de esa vida tiene unas implicaciones legales, organizativas o técnicas más o menos fáciles de ver y bastante más complejas de ajustar a un equilibrio legal y de negocio.

Cuanto antes se identifiquen los requisitos de cumplimiento, antes se podrán tomar las decisiones más adecuadas y probablemente será menos intrusivo o complejo de garantizar el cumplimiento. Esto puede aplicarse en situaciones donde lo que está en proyecto es el diseño de esa aplicación móvil, un desarrollo cloud, una plataforma de venta o proceso de negocio.

Cuando esa previsión se hace desde la fase embrionaria de un proyecto, cuando se implican todos los roles que puedan estar afectados de una u otra forma a lo largo de la vida de éste (técnicos, desarrolladores, marketing, compras / ventas, jurídico, privacidad…), y cuando entre se establece un análisis inicial que determina todos los requisitos de cumplimiento, se está logrando el desarrollado de una herramienta óptima desde el punto de vista de la protección de datos y la privacidad.

El Reglamento General de Protección de Datos pretende ser el germen de una nueva cultura, más allá de las novedades legislativas y su régimen sancionador. Una forma de hacer las cosas más preventiva y responsable que reactiva, una cultura que bien implementada generará muchas más ventajas y oportunidades para el desarrollo global de cualquier negocio.

9.2. Principios básicos

Este término establece 7 principios básicos que deben orientar el diseño y desarrollo de sistemas y tecnologías que traten datos de carácter personal. Son los siguientes:

1. **Proactivo, no Reactivo; Preventivo no Correctivo.** El enfoque de Privacidad por Diseño (PbD por sus siglas en inglés) está caracterizado por medidas proactivas, en vez de reactivas. Anticipa y previene eventos de invasión de privacidad antes de que estos ocurran. PbD no espera a que los riesgos se materialicen, ni ofrece remedios para resolver infracciones de privacidad una vez que ya ocurrieron – su finalidad es prevenir que ocurran.

2. **Privacidad como la Configuración Predeterminada.** La Privacidad por Diseño busca entregar el máximo grado de privacidad asegurándose de que los datos personales estén protegidos automáticamente en cualquier sistema de IT dado o en cualquier práctica de negocios.
   Si una la persona no toma una acción, aun así, la privacidad se mantiene intacta. No se requiere acción alguna de parte de la persona para proteger la privacidad – está inter construida en el sistema, como una configuración predeterminada.

3. **Privacidad Incrustada en el Diseño.** La Privacidad por Diseño está incrustada en el diseño y la arquitectura de los sistemas de Tecnologías de Información y en las prácticas de negocios. No está colgada como un suplemento, después del suceso.
   El resultado es que la privacidad se convierte en un componente esencial de la funcionalidad central que está siendo entregada. La privacidad es parte integral del sistema, sin disminuir su funcionalidad.

4. **Funcionalidad Total.** Privacidad por Diseño busca acomodar todos los intereses y objetivos legítimos para todas las partes interesadas. Privacidad por Diseño evita las falsas dualidades, tales como privacidad versus seguridad, demostrando que sí es posible tener ambas al mismo tiempo.

5. **Seguridad Extremo-a-Extremo – Protección de Ciclo de Vida Completo.** Habiendo sido incrustada en el sistema antes de que el primer elemento de información haya sido recolectado, la Privacidad por Diseño se extiende con seguridad a través del ciclo de vida completo de los datos involucrados – las medidas de seguridad robustas son esenciales para la privacidad, de inicio a fin.
   Esto garantiza que todos los datos son retenidos con seguridad, y luego destruidos con seguridad al final del proceso, sin demoras.

Por lo tanto, la Privacidad por Diseño garantiza una administración segura del ciclo de vida de la información, desde la cuna hasta la tumba, desde un extremo hacia el otro.

6. **Visibilidad y Transparencia.** Privacidad por Diseño busca asegurar a todos los involucrados que cualquiera que sea la práctica de negocios o tecnología involucrada, está en realidad esté operando de acuerdo a las promesas y objetivos declarados, sujeta a verificación independiente. Sus partes componentes y operaciones permanecen visibles y transparentes, a usuarios y a proveedores.

7. **Respeto por la Privacidad de los Usuarios – Mantener un Enfoque Centrado en el Usuario.** Por encima de todo, la Privacidad por Diseño requiere que los arquitectos y operadores mantengan en una posición superior los intereses de las personas, ofreciendo medidas tales como predefinidos de privacidad robustos, notificación apropiada, y facultando opciones amigables para el usuario. Hay que mantener al usuario en el centro de las prioridades.

9.3. Datos de carácter personal

La Fundació de la C.V. Observatori Valencià del Canvi Climàtic solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido.

De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa vigente de Protección de Datos.

9.4. Obligaciones del personal

Todos los miembros de la Fundació de la C.V. Observatori Valencià del Canvi Climàtic, que se encuentran dentro del ámbito de aplicación del ENS serán objeto de sesiones presenciales o de concienciación en materia de seguridad en función de la periodicidad que el Comité de Seguridad de la Información establezca como necesario y razonable en base a las necesidades detectadas, y siendo en todo caso un programa de concienciación continua que aspira a atender a todos los miembros de la Fundació de la C.V. Observatori Valencià del Canvi Climàtic,

organismos autónomos y sociedades públicas incluidas en su perímetro, y 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.

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.

9.5. Gestión de riesgos

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando se modifique la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de análisis de riesgos comprenderá las siguientes fases:

1. Identificación escenarios de riesgo.
2. Análisis de riesgos.
3. Tratamiento: El Comité de Seguridad procederá a la selección de medidas de seguridad que se deben aplicar que deberán de ser proporcionales a los riesgos y estar justificadas. El riesgo se deberá mitigar o eliminar.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos se utiliza la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA).

9.6. Desarrollo

Esta Política de Seguridad de la Información será complementada por medio de diversas recomendaciones de seguridad (políticas, protocolos, procedimientos, instrucciones técnicas, etc.)

Del mismo modo, esta Política de Seguridad de la Información complementa las políticas de seguridad de la Fundació de la C.V. Observatori Valencià del Canvi Climàtic en materia de protección de datos de carácter personal.

La Normativa de Seguridad estará a disposición de todos los miembros de la Institución que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible para su consulta en la carpeta ***Seguridad de la Información***, ubicada en Drive.

9.7. Terceras partes

Cuando la Fundació de la C.V. Observatori Valencià del Canvi Climàtic preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe 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 Fundació de la C.V. Observatori Valencià del Canvi Climàtic utilice servicios de terceros o ceda información a terceros, se les hará partícipe 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 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 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.