Sistema de Gestión de la Seguridad de la Información y Esquema Nacional de Seguridad

POLÍTICA INTEGRADA DE SEGURIDAD DE LA INFORMACIÓN

Información del Documento

Título	POLÍTICA INTEGRADA DE SEGURIDAD DE LA INFORMACIÓN
Clasificación	PUBLICO
Archivo	CZFB -Politica Integrada de Seguridad Informacion.docx

Lista de distribución

Área	Colaborador
Corporativa	Todos los empleados, usuarios, proveedores y terceras partes.

ÍNDICE

1. INTRODUCCIÓN 5
1.1 PREVENCIÓN 6
1.2 DETECCIÓN 6
1.3 RESPUESTA 6
1.4 RECUPERACIÓN 6
2. ALCANCE 7
3. ORGANIZACIÓN DE LA SEGURIDAD 7
3.1 LIDERAZGO DE LA DIRECCIÓN 7
3.2 ROLES, RESPONSABILIDADES Y FUNCIONES 7
3.2.1 Comité de seguridad de la información 8
3.2.2 Responsable de la Información 10
3.2.3 Responsable del servicio 11
3.2.4 Responsable de SEGURIDAD 12
3.2.5 Responsable del sistema 15
3.2.6 Delegado de protección de datos 16
3.3 PROCEDIMIENTO DE DESIGNACIÓN 18
4. OBJETO DE LA POLÍTICA DE SEGURIDAD 18
5. DESARROLLO DE LA PÓLITICA DE SEGURIDAD 19
6. REVISIÓN DE LA POLÍTICA DE SEGURIDAD 19
7. MANTENIMIENTO DEL SGSI 20
8. GESTIÓN DEL RIESGO 20

9. MARCO NORMATIVO 21
10. DATOS DE CARÀCTER PERSONAL 22
11. OBLIGACIONES DEL PERSONAL 22
12. FORMACIÓN Y CONCIENCIACIÓN 23
13. TERCERAS PARTES 23
14. SUPERVISIÓN Y EVALUACIÓN 24
15. DOCUMENTO DE SEGURIDAD 24
16. APROBACIÓN Y ENTRADA EN VIGOR 25

1. INTRODUCCIÓN

La **Política Integrada de Seguridad de la información** se elabora en cumplimiento de los requisitos de la Norma ISO 27001:2022 y de las exigencias del Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), que en su artículo 12 establece la obligación de disponer de una Política.

El Consorci de la Zona Franca de Barcelona depende de los sistemas TIC (Tecnología de Información y Comunicación) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que deben aplicarse las medidas de seguridad exigidas por la norma ISO 27001:2022 en base al riesgo, y también por el **Esquema Nacional de Seguridad** en base a la categorización de los diferentes sistemas. Debe realizarse un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

El Consorci de la Zona Franca de Barcelona debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida de los sistemas, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación asociadas deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.
La Organización debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

El CZFB desea potenciar el uso de las nuevas tecnologías tanto internamente como en sus relaciones con la ciudadanía. Los principales objetivos que se persiguen son, entre otros, los siguientes:

- Mejorar la calidad de los servicios públicos.
- Mejorar la seguridad de la información tratada por CZFB.
- Fomentar la relación electrónica de la ciudadanía con CZFB, creando la confianza necesaria entre ciudadano y la organización.
- Hacer transparente la actividad de CZFB.
- Fomentar la participación y colaboración.

1.1 PREVENCIÓN

La Organización 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 debe 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 según se dispone en la norma ISO 27001:2022 y en el marco operacional del propio ENS. 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, la Organización debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

1.2 DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios 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.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

1.3 RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos 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).

1.4 RECUPERACIÓN

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

2. ALCANCE

Consorci de la Zona Franca de Barcelona tiene la voluntad de conseguir que los principios de la Política de Seguridad formen parte de la cultura de la Organización para lo cual ha implementado un Sistema de Gestión de la Seguridad de la Información (SGSI) en base a un estándar reconocido internacionalmente.

El alcance de la Política de Seguridad de la Información coincide con el alcance del SGSI que se establece en el documento de **"CZFB - Contexto de la Organización**" y consta en el certificado de registro, siendo "*El SGSI para la provisión de servicios corporativos TIC como: - Mantenimiento de redes – Desarrollo de aplicaciones – Atención al usuario por el Área de Serveis de sistemes de la Informació del Consorci de la Zona Franca de Barcelona, en las Oficinas Centrales (Avinguda Parc Logistic 2-10 08040-BARCELONA), de acuerdo con la Declaración de Aplicabilidad vigente",* sin perjuicio del alcance del ENS que abarca todos aquellos sistemas que soportan la prestación de servicios a la ciudadanía por medios electrónicos.

Todo el personal de la Organización, incluyendo colaboradores, usuario y la dirección, debe conocer y cumplir esta política, que se desarrollará mediante normativa, procedimientos, instrucciones operativas, guías, manuales y todos aquellos instrumentos organizativos considerados útiles para alcanzar sus objetivos. Especial consideración merece el documento "**CZFB - Manual de Seguridad del usuario**", que contiene normas de uso de los sistemas de información de la Organización, cuyas disposiciones son de obligado cumplimiento.

Esta Política Integrada de Seguridad de la Información, además, estará a disposición de todas las otras partes interesadas que lo requieran, focalizando en usuarios, proveedores y clientes.

3. ORGANIZACIÓN DE LA SEGURIDAD

3.1 LIDERAZGO DE LA DIRECCIÓN

La Dirección del *Consorci de la Zona Franca de Barcelona* (CZFB) se compromete a liderar el mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI), así como las disposiciones indicadas en el RD 311/2022, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad**.

3.2 ROLES, RESPONSABILIDADES Y FUNCIONES

La organización de la seguridad de la información se organiza en torno a un Sistema de Gestión de Seguridad de la Información y a una serie de comités y roles, relevantes para el SGSI y el cumplimiento de las disposiciones del ENS, descritos en el documento "**CZFB - Roles, responsabilidades y autoridades**".

La implantación de la Política de Seguridad en CZFB requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) El Comité de Seguridad de la Información

b) Responsables del Servicio

c) Responsables de la Información

d) Responsable de la Seguridad de la Información

e) Responsable del Sistema de Información

f) Delegado de Protección de datos

3.2.1 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información coordina la seguridad de la información en la Diputación del Común. Estará constituido por:

- Presidenta/e
- Secretaria/o
- DPD / DPO
- Vocales:
    - Responsables de las unidades organizativas serán convocados en función de los temas a tratar (si afectan a su área).

Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas.

El Comité se deberá reunir con carácter ordinario al menos una vez al año y con carácter extraordinario por razones de urgencia y causa justificada o cuando lo decida su Presidencia.

El Comité podrá recabar del personal técnico propio o externo la información pertinente para la toma de sus decisiones, así como invitar a dicho personal a las reuniones con voz y sin voto.

El Comité ajustará su funcionamiento a las previsiones contenidas en el capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

La/El Director/a General actuará como presidente/a del Comité de Seguridad de la Información

El Responsable de la Seguridad de la Información, actuará como Secretario, con voz y voto, y como tal:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Levantará actas de las reuniones del Comité de Seguridad.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- 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 en función de las necesidades del Comité de Seguridad de la Información.

Las **funciones** del Comité de Seguridad son las siguientes:

a) Elaborar los borradores de modificación y actualización de la PSI.
b) Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
c) Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
d) 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.
e) Aprobar las Normas de Seguridad TIC (documentación de segundo nivel normativo).
f) Asegurar la coordinación de las diferentes áreas implicadas en la gestión de incidentes de seguridad de la información.
g) Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
h) Aprobar planes de mejora de la seguridad de la información de La Diputación del Común. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
i) Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
j) 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.
k) Impulsar el cumplimiento y difusión de la PSI, promoviendo las actividades de concienciación y formación en materia de seguridad para el personal de la organización.
l) Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de CZFB.

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.

3.2.2 RESPONSABLE DE LA INFORMACIÓN

Conforme a los artículos 11 y 41 del ENS, el Responsable de la Información es la persona que establece las necesidades de seguridad de la información que se maneja y efectúa las valoraciones del impacto que tendría un incidente que afectara a su seguridad. Tiene, además, la potestad de modificar el nivel de seguridad requerido para la misma (Anexo II.5.7.2 del ENS).

Serán personas con alto cargo en la dirección de la organización y pertenecientes al comité directivo del mismo. Este cargo tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestione cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestione.

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

Son **funciones** del Responsable de la Información, dentro de su ámbito de actuación, las siguientes:

a) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información (artículo 41 del ENS). Para ello, puede recabar el asesoramiento del Responsable de Seguridad de la Información y del Responsable del Sistema.
b) Es el responsable, junto al Responsable del Servicio, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control. Esta tarea podrá delegarla, de acuerdo con el Responsable del Servicio, en el Responsable de Seguridad de la Información y en el Responsable del Sistema.
c) 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.
d) Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
e) El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
f) 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.

g) 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.
- 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 del Sistema, ni siquiera cuando se trate de organizaciones de reducida dimensión que funcionen de forma autónoma.

3.2.3 RESPONSABLE DEL SERVICIO

Conforme al artículo 13 del ENS, el Responsable del Servicio es la persona que determina los requisitos de seguridad del servicio prestado.

Respecto al proceso de gestión del riesgo, el Responsable del Servicio es el encargado, junto al Responsable de la Información, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control. Esta tarea podrá delegarla, de acuerdo con el Responsable del Servicio, en el Responsable de Seguridad de la Información y en el Responsable del Sistema.

El responsable del servicio 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, Responsable de Seguridad de la Información y Responsable de Sistemas, antes de ser ejecutada.

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:

a) 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.
b) Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.

c) El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
d) Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
e) 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.
f) 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 general de la organización no dependa de la unidad a la que pertenece el Responsable de la Información.
- Este rol no podrá coincidir con el de Responsable de Seguridad, salvo en organizaciones de reducida dimensión que funcionen de forma autónoma.

3.2.4 RESPONSABLE DE SEGURIDAD

Conforme al artículo 13 del ENS, el Responsable de Seguridad de la Información es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y del servicio.

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.

Tal como se describe en la Guía CCN-STIC-801: “La figura del “Responsable de la Seguridad” aparece en ambas normativas (Privacidad) 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 de la Información a efectos de cumplimiento de la normativa en materia de protección de datos de carácter personal.

Serán funciones del Responsable de Seguridad de la Información las siguientes:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información, con la responsabilidad y autoridad para asegurarse de que el Sistema de Gestión de la Seguridad de la Información cumple con los requisitos del Esquema Nacional de Seguridad.
b) Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas.
c) Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables del Servicio y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS, declarando la aplicabilidad de dichas medidas.
d) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
e) Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación al Esquema Nacional de Seguridad, en colaboración con el Responsable de Sistemas.
f) Realizar con la colaboración del Responsable del Sistema, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable del Sistema, podrá aceptar los riesgos residuales calculados en el análisis de riesgos cuando el Responsable de la Información y el Responsable del Servicio hayan delegado en él esta tarea.
g) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y analizar los informes de auditoría, elaborando las conclusiones a presentar al Responsable del Sistema, a los Responsables del Servicio y los Responsables de la Información para que adopten las medidas correctoras adecuadas.
h) Coordinar el proceso de Gestión de la Seguridad, en colaboración con el Responsable de Sistemas.
i) Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema (artº. 28 y Anexo II.2 del ENS).
j) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el Responsable de Sistemas.
k) Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS.
l) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
m) Preparar los temas a tratar en las reuniones del Comité de Seguridad, en coordinación con el Responsable del Sistema, aportando información puntual para la toma de decisiones.
n) Responsable de la ejecución directa o delegada de las decisiones del Comité de Seguridad.
o) Colaborar estrechamente con el Delegado de Protección de Datos en relación a las obligaciones y disposiciones del Reglamento General de Protección de Datos y la LOPDGDD.
p) 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.
q) 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).

r) Elaborará, junto al Responsable de Sistema, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
s) 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.
t) Aprobará las directrices propuestas por el Responsable 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 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 de la Información Delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reportan.

Respecto a la documentación, y apoyándose en el Responsable del Sistema, son funciones del Responsable de Seguridad:

a) Proponer al Comité de Seguridad para su aprobación la documentación de seguridad de segundo nivel (Normas de Seguridad TIC y Procedimientos Generales del Sistema de Gestión de la Seguridad de la Información –SGSI–) y firmar dicha documentación.

b) Aprobar la documentación de seguridad de tercer nivel y firmar dicha documentación.

c) Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

Para el desarrollo de cualquiera de sus funciones el Responsable de Seguridad de la Información podrá recabar la colaboración del Responsable del Sistema.

3.2.5 RESPONSABLE DEL SISTEMA

Serán **funciones** del Responsable del Sistema las siguientes:

a) Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
c) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
d) Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.
e) Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.
f) Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el Responsable de Seguridad.
g) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
h) Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de dicha información o servicio y con el Responsable de Seguridad.
i) Realizar con la colaboración del Responsable de Seguridad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable de Seguridad, podrá aceptar los riesgos residuales calculados en el análisis de riesgos cuando el Responsable de la Información y el Responsable del Servicio hayan delegado en él esta tarea
j) Elaborar en colaboración con el Responsable de Seguridad de la Información, la documentación de seguridad de tercer nivel.
k) 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 de la Información.
l) Elaborar los Planes de Continuidad del Sistema para que sean validados por el Responsable de Seguridad de la Información de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.

m) Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
n) 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 de la Información para su aprobación.

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

a) Planificará la implantación de las salvaguardas en el sistema.
b) 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.

3.2.6 DELEGADO DE PROTECCIÓN DE DATOS

Siguiendo lo indicado en el RGPD y la LOPDGDD, el Delegado de Protección de Datos tendrá como mínimo las siguientes **funciones**:

a) Asesorar y supervisar el cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.

b) Asesorar y supervisar que se han definido plazos de conservación para los datos y que existen y se aplican procedimientos correctos para su destrucción cuando corresponda.

c) Supervisar que los tratamientos disponen de bases jurídicas o legitimación

d) Asesorar sobre la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

e) Asesorar sobre la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.

f) Asesorar y supervisar el diseño e implantación de medidas de información a los afectados por los tratamientos de datos (cláusulas).

g) Asesorar y supervisar que existen mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.

h) Supervisar las solicitudes de ejercicio de derechos por parte de los interesados.

i) Supervisar la diligencia en la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.

j) Asesorar y supervisar sobre los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.

k) Asesorar y supervisar el diseño e implantación de políticas de protección de datos.

l) Revisar los controles y auditorías de Seguridad y protección de datos y reportar conclusiones a la Dirección.

m) Supervisar la primera versión de los registros de actividades de tratamiento, así como los cambios que se realicen en los mismos.

n) Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre la protección de datos.

o) Asesorar, revisar y validar los análisis de riesgo y Evaluaciones de Impacto realizados.

p) Asesorar y supervisar la 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.

q) Asesorar y supervisar en la Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.

r) Supervisar los procedimientos de gestión de violaciones 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 supervisión y a los afectados.

s) Comunicar las violaciones de seguridad a las autoridades e interesados cuando se requiera.

t) Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre la protección de datos.

u) Supervisar las evaluaciones de impacto sobre la protección de datos.

v) Mantener las relaciones con las autoridades de supervisión.

w) Mantener el contacto con los interesados.

x) Asesorar y supervisar en el diseño de programas de formación, concienciación y sensibilización de usuarios.

y) Reportar periódicamente a la Junta de Gobierno sobre el estado de cumplimiento en la materia y las acciones que haya que acometer, así como reportar ante incidencias y circunstancias que se produzcan puntualmente

El delegado de protección de datos está nombrado formalmente y comunicado a la Agencia Española de Protección de Datos, pudiéndose comunicar los ciudadanos en el correo **dpd@zfbarcelona.es.**

3.3 PROCEDIMIENTO DE DESIGNACIÓN

La creación del Comité de Seguridad, el nombramiento de sus integrantes y la designación del Responsable de Seguridad de la Información, del Responsable de la información y del Responsable del Sistema, serán propuestos y aprobados por la Dirección General del CZFB.

La estructura y organización se revisará, al menos, cada 2 años o cuando por circunstancias organizativas sea necesario.

Se designan las siguientes responsabilidades:

- Responsables del Servicio
- Responsable de Información
- Responsable de Seguridad de la Información
- Responsable del Sistema
- Delegado de Protección de datos

4. OBJETO DE LA POLÍTICA DE SEGURIDAD

Los motivos para la creación de esta Política de Seguridad por parte del responsable de Seguridad del SGSI y la Dirección, son varios:

- El principal es garantizar a los usuarios el acceso a la información con la cantidad y calidad que se requiere para el desempeño profesional, así como evitar serias pérdidas de información y accesos no autorizados a la misma. Los principios que deben respetarse son los siguientes:

  - **Confidencialidad**: la información perteneciente a *El Consorci de la Zona Franca de Barcelona* debe ser conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.

  - **Integridad**: la información de *El Consorci de la Zona Franca de Barcelona* debe de ser completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.

- **Disponibilidad:** la información de *El Consorci de la Zona Franca de Barcelona* está accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.

- **Autenticidad:** El origen de la información de los ciudadanos tratada por *El Consorci de la Zona Franca de Barcelona* debe ser confiable, es decir, garantizando que quien la proporcione sea realmente quien dice ser.

- **Trazabilidad:** Garantizar que pueda determinarse en todo momento la trazabilidad respecto a los tratamientos efectuados por *El Consorci de la Zona Franca de Barcelona, respecto a la información* de los ciudadanos para la que sea relevante su conocimiento.

Adicionalmente, dado que cualquier Sistema de Gestión de la Seguridad de la Información debe cumplir con la legislación vigente, se atenderá al siguiente principio:

- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta *El Consorci de la Zona Franca de Barcelona*, especialmente lo dispuesto por el ENS y en materia de protección de datos personales.

- Establecer anualmente objetivos de seguridad de la información para la organización y protección de los activos de información de *El Consorci de la Zona Franca de Barcelona*. Dichos objetivos se alcanzarán a través de una serie de medidas organizativas y técnicas, junto a normas concretas y claramente definidas.

- Esta Política de Seguridad será mantenida, actualizada y adecuada a los fines y obligaciones de la organización.

- El resultado de esta Política se plasma en un Sistema de Gestión de Seguridad de la Información

5. DESARROLLO DE LA PÓLITICA DE SEGURIDAD

Esta Política se desarrollará por medio de normativa de seguridad y procedimientos que afronten aspectos específicos.

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

6. REVISIÓN DE LA POLÍTICA DE SEGURIDAD

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de modificación o mantenimiento de la misma. La Política será aprobada por este y difundida para que la conozcan todas las partes afectadas.

Esta Política se desarrollará por medio de normativa de seguridad que aborde aspectos específicos. Esta normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y de comunicaciones.

La normativa de seguridad (Manual) estará disponible en la intranet del organismo.

7. MANTENIMIENTO DEL SGSI

El mantenimiento actualizado del Sistema de Gestión de Seguridad de la información se fundamenta en:

- Estudio y conclusiones de los indicadores definidos.
- Resultado de las auditorías técnicas y de cumplimiento.
- Inputs de terceras partes.

8. GESTIÓN DEL RIESGO

La gestión de la Seguridad de la Información en la Organización está basada en el riesgo, de conformidad con la Norma internacional ISO/IEC 27001:2022 y el ENS.

Se articula mediante un proceso general de apreciación y tratamiento del riesgo, que potencialmente pueden afectar a la seguridad de la información de los servicios prestados, consistente en:

- **Identificar los riesgos**, que aprovecharán vulnerabilidades de los Sistemas de Información que soportan, o de los que depende, la seguridad de la información.
- **Analizar los riesgos**, en base a la consecuencia de materializarse y de la probabilidad de ocurrencia.
- **Evaluar los riesgos,** según un nivel previamente establecido y aprobado de riesgo ampliamente aceptable, tolerable e inaceptable.
- **Tratar los riesgos** inaceptables, mediante los controles o salvaguardas adecuadas.

Dicho proceso es cíclico y debe llevarse a cabo de forma periódica, como mínimo una vez al año, y basada en una metodología concreta que produzca resultados comparables. Para cada riesgo identificado se asignará un propietario, pudiendo recaer múltiples responsabilidades en una misma persona o comité.

La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos (artículo 7 del ENS) y reevaluación periódica (artículo 10 del ENS).

El Responsable de Seguridad de la Información junto al Responsable de Sistemas, son los encargados de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

El Responsable de la Información y el del Servicio son los responsables de los riesgos sobre la información y sobre el servicio, respectivamente, y por tanto de aceptar los riesgos residuales calculados en el análisis y de realizar su seguimiento y control sin perjuicio de la posibilidad de delegar esta tarea

La Empresa tiene el derecho a auditar el uso de todos los activos de la organización, incluyendo servidores, PC's, PC's portátiles, tablet's, smartphone's, … con el objetivo de analizar el uso debido de los mismos.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse cada año por parte del Responsable de Seguridad de la Información con la colaboración del Responsable del Sistema, que elevarán un informe al Comité de Gestión de la Seguridad de la Información.

9. MARCO NORMATIVO

Son de aplicación las leyes y normativas del ordenamiento jurídico español, especialmente con relación al **Esquema Nacional de Seguridad**, protección de datos personales, propiedad intelectual y uso de herramientas telemáticas. Por todo ello, *El Consorci de la Zona Franca de Barcelona* podrá ser requerida por los órganos administrativos pertinentes a proporcionar los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

El marco normativo al que la Organización está sujeta, debido al desarrollo de sus actividades, está descrito en el documento "**CZFB - Contexto de la Organización**".

Se toma como referencia básica en materia de Seguridad de la Información la normativa siguiente:

- 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 (Reglamento General de Protección de Datos).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- 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.
- Ley 34/2002, de 11 de junio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Reglamento (UE) nº 910/2014: relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

10. DATOS DE CARÀCTER PERSONAL

Consorci de la Zona Franca Barcelona realiza tratamientos en los que hace uso de datos de carácter personal. El Documento de Seguridad de Protección de Datos de la Organización se puede encontrar en las dependencias del *Delegado de Protección de Datos*. Dicho documento recoge los ficheros afectados y tratamientos correspondientes.

Todos los sistemas de información de *Consorci de la Zona Franca de Barcelona* se ajustarán a los niveles de seguridad requeridos por la normativa, en función de la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

11. OBLIGACIONES DEL PERSONAL

Todos los miembros de la Organización tienen la obligación de conocer y cumplir esta Política Integrada de Seguridad de la Información y el Manual de Seguridad del Usuario desarrollado a partir de ella, siendo responsabilidad de la Dirección disponer de los medios necesarios para que la información llegue a los afectados, teniendo en cuenta siempre las disponibilidades presupuestarias de *El Consorci de la Zona Franca de Barcelona*. Todos los trabajadores de la Organización atenderán a una acción de concienciación en materia de seguridad TIC al menos una vez al año.

Se establecerá un programa de acciones en concienciación continua para atender a todos los miembros de *El Consorci de la Zona Franca de Barcelona*, en particular a los de nueva incorporación, teniendo en cuenta siempre las disponibilidades presupuestarias de la Organización. 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 cualquier responsabilidad en la Organización, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Los accesos se gestionarán des del principio de reglas basadas en la premisa del mínimo privilegio, es decir, "Todo está generalmente prohibido a menos que esté expresamente permitido", en lugar de la regla más débil, "Todo está generalmente permitido a menos que esté expresamente prohibido". Además, a los usuarios sólo se le concede acceso a la información que necesita para realizar sus tareas (diferentes tareas o funciones implican diferentes necesidades de saber o conocer la información y, por tanto, diferentes perfiles de acceso).

12. FORMACIÓN Y CONCIENCIACIÓN

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

Todos los miembros del CZFB. asistirán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros del CZFB., 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.

13. TERCERAS PARTES

Cuando *Consorci de la Zona Franca de Barcelona* preste servicios o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Para ello, se establecerán canales para informe y coordinación de los respectivos Roles o Comités de Coordinación del ENS y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad. Cuando ***El Consorci de la Zona Franca de Barcelona*** utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política Integrada 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 la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de informe 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. Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. El informe debe ser aprobado por los responsables de la información y los servicios afectados antes de seguir adelante.

Los accesos se gestionarán des del principio de reglas basadas en la premisa del mínimo privilegio, es decir, "Todo está generalmente prohibido a menos que esté expresamente permitido", en lugar de la regla más débil, "Todo está generalmente permitido a menos que esté expresamente prohibido". Además,

a las terceras partes sólo se le concede acceso a la información que necesita para realizar sus tareas (diferentes tareas o funciones implican diferentes necesidades de saber o conocer la información y, por tanto, diferentes perfiles de acceso).

14. SUPERVISIÓN Y EVALUACIÓN

Con una periodicidad mínima anual se revisará esta Política de Seguridad para adecuarla a los posibles cambios en ***Consorci de la Zona Franca de Barcelona***, y se analizarán las incidencias y no conformidades encontradas en el sistema elaborando, si procede, una lista de acciones a emprender y ejecutar durante el año siguiente, como objetivos para garantizar la Seguridad de la Información y la protección y buen uso de los recursos de la Organización que la soportan.

Esta Política de Seguridad, la normativa y procedimientos que la desarrollan, y los manuales de seguridad de usuario y administrador deberán además seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: variaciones significativas en la plantilla de personal, cambios en la infraestructura, desarrollo de nuevos servicios, entre otros.

Esta Política de Seguridad debe ser difundida a todo el personal, colaboradores externos y usuarios de la red en general, involucrados en la relación con *El Consorci de la Zona Franca de Barcelona* que manejen, o puedan llegar a manejar, información y recursos pertenecientes a la misma.

15. DOCUMENTO DE SEGURIDAD

Esta Política de Seguridad de la Información se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Las normas y procedimientos contemplarán, al menos, los siguientes aspectos:

- Protección de datos de carácter personal: se implantarán medidas técnicas y organizativas que permitan cumplir los requisitos normativos en esta materia.
- Gestión de activos de información: los activos de información se encontrarán inventariados, categorizados y estarán asociados a un responsable.
- Seguridad ligada a los recursos humanos: la seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios, para lo que se implantarán los mecanismos que permitan a los usuarios conocer sus responsabilidades y cómo cumplir con ellas.
- Seguridad física: las instalaciones del CZFB. mantendrán una correcta seguridad física para evitar los accesos no autorizados así como cualquier otro tipo de daño o interferencia externa.

- Seguridad lógica: se establecen medidas organizativas y técnicas para el control de accesos, la protección frente a códigos dañinos, la seguridad de las comunicaciones, la realización de copias de seguridad…
- Gestión de incidentes de seguridad: se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad

El cuerpo normativo sobre seguridad de la información será de obligado cumplimiento y se desarrollará en cuatro niveles según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior: Política de Seguridad de la Información, políticas específicas y normas de seguridad, procedimientos operativos e instrucciones técnicas y registros/evidencias.

16. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Seguridad han sido elaborados mediante las aportaciones de los abajo firmantes y han sido aprobados por la Dirección, con vigencia a partir de la fecha de su firma.

Todos los abajo firmantes asumen y aceptan plenamente el contenido de esta Política y se comprometen a aplicarla en sus respectivos ámbitos para conseguir el correcto funcionamiento del Sistema de Gestión de la Seguridad de la Información.

Esta Política Integrada de Seguridad de la Información es efectiva desde la fecha de su firma y hasta que sea reemplazada por un nuevo texto de la misma. Este texto anula a cualquier otro aprobado con anterioridad.