Denominación	Política de Seguridad y Privacidad de la Información
Información documentada	Política (documento de primer nivel)
Referencia	PSP-00

Rev.	Autor	Fecha	Descripción
0.0	RSEG	31 oct 2024	Versión inicial
0.1	RSEG	11 sept 2025	Adaptación a nueva versión de guíaS CCN-STIC-801 y CCN-STIC 805 Inclusión de medidas en torno a la inteligencia artificial

*El presente documento tendrá efectos desde la fecha de su firma electrónica.

**El presente documento contiene información clasificada como de uso público, por cuanto será distribuida a través de los siguientes medios:

- ☑ Tablón de anuncios virtual/intranet corporativo
- ☑ Dirección de correo corporativo (indicar): todos.czfc@zonafrancacadiz.com
- ☑ Otro (indicar): sitios web/portales de transparencia corporativos

ÍNDICE

1. APROBACIÓN, ENTRADA EN VIGOR, PUBLICACIÓN Y REVISIÓN

A través del presente documento, el Consorcio de la Zona Franca de Cádiz (en adelante CZFC) aprueba su Política de Seguridad y Privacidad de la Información (PSP), siendo ésta efectiva desde la fecha de su firma por parte del máximo órgano de dirección de la entidad, y manteniendo su vigencia hasta la firma de una nueva política que la sustituya.

Su entrada en vigor tiene carácter normativo en el seno de la entidad, en virtud de lo cual será de obligado cumplimiento por todos los miembros del CZFC y será observada por cuantos grupos de interés se encuentren vinculados al sistema de información de la entidad.

Dada su calificación como información de uso público, esta política será objeto de publicación en la intranet y los sitios web corporativos o portales de transparencia de la entidad, sin perjuicio de su publicación en otros medios de difusión.

La presente Política será revisada por el Comité de seguridad de la información (CSEG) con carácter anual o cuando, atendiendo a circunstancias que impliquen modificaciones en el sistema de información o sobre las medidas técnicas y organizativas vinculadas a su seguridad, resulte preceptivo o aconsejable dicha revisión.

2. OBJETO Y ÁMBITO DE APLICACIÓN

Constituye el objeto del presente documento la aprobación de la PSP en el ámbito del CZFC, así como su marco organizativo y tecnológico.

Esta PSP, y las políticas específicas que se aprueben en su desarrollo, extienden su ámbito de aplicación a todos los activos de información del CZFC, y serán observadas por la totalidad de los miembros de la entidad, incluyendo todos sus órganos directivos, responsables de área y departamento, así como la totalidad de la plantilla que, de forma estable o con carácter temporal, preste servicios en el CZFC.

Asimismo, la PSP se extiende a toda persona que acceda tanto a los sistemas de información como a la propia información que sea gestionada por el CZFC, con independencia de cuál sea su destino, adscripción o relación.

3. MISIÓN DE LA ORGANIZACIÓN

El CZFC, siendo consciente de la importancia de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos y asumiendo su compromiso con la seguridad y privacidad de la información, somete dichos sistemas a su adecuación conforme a las normas de referencia, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

Estos sistemas serán administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a los atributos o dimensiones de **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad** de la información tratada y los servicios prestados, así como a la **privacidad** de los datos de carácter personal.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando adecuadamente ante los incidentes.

Los sistemas TIC deben estar protegidos frente a amenazas de rápida evolución con potencial para incidir en los mencionados atributos o dimensiones de seguridad, así como en el valor de la información y los servicios. Para ello, se requiere de una estrategia que se adapte a los cambios en las condiciones del entorno a fin de garantizar la prestación continua de los servicios. Esto implica que las organizaciones deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS) para la categoría del sistema, así como realizar un seguimiento continuo de los niveles de prestación de servicios, analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las organizaciones deben cerciorarse de que la seguridad y privacidad de la información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y privacidad, así como las necesidades de su financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC o en los que tenga especial relevancia la información.

Todas las áreas integradas en el seno de la entidad deben estar preparadas para prevenir, vigilar, detectar, reaccionar y recuperarse ante incidentes y brechas de seguridad, de acuerdo con el Artículo 8 del RD 311/2022, de 3 de mayo, por el que se aprueba el Esquema Nacional de Seguridad (ENS).

4. ALCANCE Y ESTRUCTURA

Esta política se aplica a todos los sistemas TIC de la entidad y a todos los miembros del CZFC implicados en procesos, proyectos y servicios que requieran la aplicación del ENS, sin excepciones; así como a los servicios prestados por la organización en calidad de entidad perteneciente al sector público. Asimismo, debe ser observada por los prestadores de servicios o proveedores de soluciones TIC del CZFC.

La presente política, de conformidad con lo dispuesto en el artículo 12.3 del ENS, es coherente con la Política de Seguridad en el ámbito de la Administración Digital del Ministerio de Hacienda, así como su marco organizativo y tecnológico.

El Sistema de Gestión de Seguridad y Privacidad de la Información (SGSP) del CZFC tiene la siguiente estructura documental:

- Política de Seguridad y Privacidad de la Información (PSP-00)
- Guías CCN-STIC-XXX (externas, publicadas por en Centro Criptológico Nacional)
- Políticas específicas de seguridad y privacidad de la información (PSP-XX)
- Normas de seguridad y privacidad (PSP-XX-N)
- Instrucciones de seguridad y privacidad de la información (ISP-XX)

- Registros de de seguridad y privacidad de la información (RSP-XX)
- Otros documentos de seguridad y privacidad de la Información

A efectos de una mejor organización y estructuración, la entidad mantendrá actualizado un registro con un listado de la documentación del sistema y las reglas de nomenclatura que recaen sobre dicha documentación.

5. OBJETIVOS

Para llevar a cabo la misión a que se refiere esta política, el máximo órgano directivo de la entidad establece los siguientes objetivos de seguridad y privacidad de la información:

- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, así como la privacidad de los datos personales y la continuidad en la prestación de los servicios;
- Implementar medidas de seguridad en función del riesgo;
- Formar y concienciar a los integrantes de la entidad respecto a la seguridad y privacidad de la información. Implementar medidas de seguridad y privacidad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones;
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados;
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmitida a través de redes de comunicaciones sea adecuadamente protegida;
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto;

- Controlar el cumplimiento de las medidas de seguridad y privacidad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema;
- Gestionar los incidentes de seguridad y privacidad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse;
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos;
- Supervisar de forma continuada el sistema de gestión de la seguridad y privacidad, mejorando y corrigiendo las ineficiencias detectadas.

6. PRINCIPIOS RECTORES DE LA POLÍTICA

- Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente.
- Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.
- Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, dando una respuesta ágil

para restaurar la información o servicios prestados, garantizando una conservación segura de la información.

- Existencia de líneas de defensa, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.
- Vigilancia continua y reevaluación periódica: la entidad implementa medios para la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- Diferenciación de responsabilidades: en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas y no existirá relación jerárquica entre ellos.

7. MARCO NORMATIVO

Una de las bases sobre las que se sustenta el sistema es el cumplimiento de los requisitos legales y contractuales aplicables, así como con sus actualizaciones. El marco normativo básico de seguridad de la información en el que son desarrolladas las actividades de la organización, a la fecha de la aprobación de la presente política, es el siguiente:

- 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 (RGPD);
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD);
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas;
- Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público;

- Real Decreto 311/2022, de 3 de mayo, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre (ENS).

Además de esta normativa básica, completan el marco una serie de normas que vendrán relacionadas a modo de anexo a esta política. Este marco será revisado anualmente junto con la propia política, siendo que la entidad dispone de un procedimiento de identificación de la legislación aplicable y actualización permanente, así como de un registro donde se conservan referencias a dichas normas actualizadas junto con enlaces a los boletines oficiales a través de los cuales son publicadas.

8. ORGANIZACIÓN DE SEGURIDAD

La responsabilidad esencial en materia de seguridad de la información recae sobre la Dirección de la entidad, ya que ésta es responsable de organizar las funciones y responsabilidades, así como de facilitar los recursos adecuados para conseguir los objetivos de cumplimiento del ENS e implantación de estándares internacionales, como las normas UNE–ISO/IEC 27001 de Gestión de Seguridad de la información o ISO/IEC 27701 de Gestión de la Privacidad.

Las funciones y responsabilidades en el ámbito de la seguridad de la información estarán distribuidas en los siguientes roles:

- Responsable de la información (RINFO);
- Responsable del servicio (RSER);
- Responsable de seguridad (RSEG);
- Responsable de los sistemas de información (RSIS);
- Administrador de Seguridad del Sistema (AS)
- Representante de la Dirección (RDIR);
- Delegado de Protección de Datos de la organización (DPD), éste último con voz pero sin voto.

La gestión de la seguridad de la información se encomienda al RSEG, quien informará al Comité de seguridad de las necesidades de la emisión de políticas específicas o

procedimientos complementarios a la presente Política de seguridad y privacidad, al objeto de asegurar el cumplimiento de la normativa aplicable. Los roles o funciones de seguridad definidos son los siguientes:

8.1 RESPONSABLE DE LA INFORMACIÓN (RINFO)

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).

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. Aprobar formalmente la valoración de los activos de información y decidir sobre la aceptación de los riesgos residuales resultantes de los análisis de riesgos, a propuesta del Responsable de Seguridad de la Información.
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. Tener la responsabilidad sobre el uso que se haga de una cierta información y, por tanto, de su protección.
e. Establecer los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.

El RINFO es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o integridad de la información.

8.2 RESPONSABLE DEL SERVICIO (RSER)

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

Son funciones propias de este cargo:

a. Establecer los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
b. Aprobar formalmente la valoración de los activos de información de tipo Servicio, y decidir sobre la aceptación de los riesgos residuales resultantes de los análisis de riesgos, a propuesta del Responsable de Seguridad de la Información.
c. Tener la responsabilidad sobre el uso que se haga de determinados servicios y, por tanto, de su protección.
d. Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.

8.3 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (RSEG)

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.

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 potestad para

verificar 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 Política de Seguridad y Privacidad de la Información (PSP), de sus políticas específicas de seguridad y privacidad (PSP), normas de seguridad, procedimientos técnicos y de la configuración de seguridad de los sistemas.
c. Establecer, en coordinación con el Responsable del Sistema y el Administrador de Seguridad, 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 o los estándares internacionales ISO 27001 e ISO 27701, en colaboración con el Responsable de Sistemas y el Administrador de Seguridad.
f. Realizar los preceptivos análisis de riesgos, seleccionar las salvaguardas y 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 y el Administrador de Seguridad.
i. Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

j. Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el Responsable de Sistemas y el Administrador de Seguridad.
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 y el Anexo A de la norma ISO 27001.
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. Coordinar y supervisar la ejecución directa o delegada de las decisiones del Comité de Seguridad.
o. Colaborar con el Delegado de Protección de Datos en relación a las obligaciones y disposiciones del RGPD y la LOPDGDD en torno a la privacidad de la información que contenga datos de carácter personal.
p. Elaborar, en el marco del Comité de Seguridad de la Información, la Política de Seguridad y Privacidad de la Información para su aprobación por el máximo órgano de dirección de la entidad.
q. Informar periódicamente al Comité de Seguridad de las actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema.
r. Elaborar, en coordinación con Responsable de Sistema y el Administrador de Seguridad, Planes de Mejora de la Seguridad para su aprobación por el Comité de Seguridad de la Información.
s. Validar los Planes de Continuidad del Sistema que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.
t. Aprobar las directrices propuestas por el Responsable del Sistema para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios

8.4 RESPONSABLE DEL SISTEMA (RSIS)

De conformidad con lo dispuesto en el artículo 13.1.d), el responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Serán funciones propias 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. Realizar un seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.
d. Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
e. 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.
f. Colaborar con el Responsable de Seguridad en los análisis de riesgos, selección de salvaguardas y revisión del proceso de gestión del riesgo.
g. Elaborar en colaboración con el Responsable de Seguridad de la Información, la documentación de seguridad de tercer nivel (procedimientos técnicos, instrucciones de seguridad, circulares informativas, etc).
h. 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.
i. Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.

j. 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.

8.5 ADMINISTRADOR DE SEGURIDAD DEL SISTEMA (AS)

Serán funciones propias del Administrador de Seguridad:

a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
b. 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.
c. La aplicación de los Procedimientos Operativos de Seguridad (POS).
d. Informar al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
e. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Esta definición de deberes y responsabilidades se completa en los perfiles de puesto y en el registro de responsables, roles y responsabilidades.

9. COMITÉ DE SEGURIDAD (CSEG)

El Comité de Seguridad de la Información (CSEG) es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité.

El CSEG es un órgano colegiado ejecutivo y con autonomía para la toma de decisiones, no sujeto en su actividad a subordinación de ningún otro elemento de la organización.

9.1 DESIGNACIÓN, NOMBRAMIENTO, RENOVACIÓN Y CESE

Corresponde al Delegado Especial del Estado en la Zona Franca de Cádiz, en calidad de titular de la entidad, la designación de los miembros del Comité de Seguridad de la Información.

Los roles de Responsable de la Información y Responsable del Servicio serán asumidos de forma colegiada por el propio CSEG.

Los miembros del Comité serán renovados tácitamente por períodos de dos años en tanto no se promueva una modificación o cuando un cambio organizativo o circunstancial que afecten al sistema de información así lo aconsejen.

Los miembros del CSEG serán cesados cuando se den causas de incompatibilidad, incumplimiento de obligaciones, inhabilitación o cuando razones de interés público o de la propia entidad así lo aconsejen.

La Presidencia del Comité la ostentará el Delegado Especial del Estado en calidad de Titular de la entidad o persona delegada, que hará además las funciones de representación de la Dirección (RDIR). La función de secretario del CSEG recaerá sobre la figura del Responsable de Seguridad de la Información (RSEG).

9.2 COMPOSICIÓN

El Comité de Seguridad de la Información del Consorcio de la Zona Franca de Cádiz estará integrado por los siguientes miembros:

- Representante de la Dirección (RDIR): Delegado Especial del Estado en la Zona Franca de Cádiz, que ostentará la presidencia del Comité;
- Responsable de la Información (RINFO): rol asumido de forma colegiada por el propio comité;
- Responsable del Servicio (RSER): rol asumido de forma colegiada por el propio comité;

- Responsable del Sistema de Información (RSIS): Responsable del Dpto. Informática del CZFC;
- Administrador de Seguridad del Sistema de Información (AS): Técnico/a del Dpto. Informática del CZFC;
- Responsable de Seguridad de la Información (RSEG): Responsable del Dpto. de Protección de datos, seguridad de la información y cumplimiento normativo del CZFC, que realizará la función de secretario del Comité;
- Delegado/a de Protección de Datos (DPD): prestador de servicio DPD externo, con voz pero sin voto;

Asimismo, el Comité estará integrado por las personas que ostentan la representación de las distintas áreas del CZFC:

- Jefatura de Gabinete
- Dirección de Organización y RRHH
- Dirección de Promoción empresarial y Comercio exterior
- Dirección Financiera
- Dirección Técnica
- Secretaría General
- Coordinación de Empresas Participadas

9.3 FUNCIONES

Entre sus funciones destacan las de velar por el cumplimiento del Esquema Nacional de Seguridad y la resolución de conflictos en torno a las diferencias de criterio que puedan surgir en el seno de la organización sobre esta materia.

Sin vocación de exhaustividad, son asimismo funciones propias del CSEG:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos;
- Informar regularmente del estado de la seguridad de la información a la 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 seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades;
- Controlar periódicamente el grado de cumplimiento de las medidas propuestas para reducir el riesgo residual (pudiendo proponer acciones de mejora) y el correcto funcionamiento del procedimiento de gestión e incidentes, velando por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes
- Elaborar y revisar regularmente la Política de Seguridad y Privacidad de la Información para su aprobación por la Dirección, y aprobar la Normativa de Seguridad de la Información;
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo/entidad en materia de seguridad;
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados;
- Velar porque se respete el principio de seguridad desde el diseño, pudiendo requerir el asesoramiento el Responsable de la Seguridad, en todas aquellas iniciativas de la entidad que afecten a la seguridad de la información o de los sistemas. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas en el ámbito de aplicación del ENS;
- 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;
- Recibir del RSEG resumen consolidado de actuaciones en materia de seguridad y privacidad de la información, de los incidentes sobre la materia, del estado de la seguridad del sistema y del riesgo residual al que el sistema está expuesto.

El Comité podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de decisiones o asesoramiento, realizando formación especializada en la materia. También podrá contar con Grupos de Trabajo especializados, internos, externos o mixtos.

Las funciones del Secretario del Comité serán:

- Convocar las reuniones del Comité de Seguridad de la Información, atendiendo a las instrucciones de la Presidencia del Comité.
- Preparar los temas a tratar en las reuniones del Comité, recabando la información de los diferentes responsables.
- Elaborar el acta de las reuniones.
- Remitir el acta de las reuniones a los asistentes, recabando su firma, en su caso.
- Conservar las actas, de acuerdo con los criterios de conservación documental de la entidad.

9.4 CONVOCATORIA, VOTACIÓN Y APROBACIÓN DE ASUNTOS

El CSEG quedará válidamente constituido, a convocatoria del Secretario, mediante quórum del Presidente, Secretario y la mitad de sus miembros en la que deberá reflejarse el orden del día.

La toma de decisiones del comité se realizará mediante votación por mayoría simple. Las decisiones aprobadas y el resultado de las votaciones deberán constar en acta levantada por el Secretario.

En caso de empate en las votaciones, la persona que ostente la Presidencia tendrá voto de calidad.

10. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán estar sometidos a un análisis de riesgos a través del cual se evalúan las amenazas y los riesgos a los que están expuestos. Este análisis se revisa regularmente:

- al menos una vez al año;
- cuando cambie la información manejada;
- cuando cambien los servicios prestados;
- cuando ocurra un incidente grave de seguridad;

- cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el CSEG establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El CSEG dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Para la realización del análisis de riesgos se tendrá en cuenta la metodología de análisis de riesgos desarrollada en el procedimiento denominado *Evaluación de Riesgos de Seguridad de la Información*. Inicialmente, será utilizada la metodología *Magerit. v3* del Centro Criptológico Nacional (CCN).

Los análisis de riesgos deberán ser aprobados por el Responsable de Seguridad de la Información (RSEG).

Cuando el sistema trate datos personales y se haya realizado un análisis de riesgos en protección de datos personales, conforme con los artículos 24 y 32 del RGPD o por una Evaluación de Impacto del artículo 35 del RGPD, el Responsable de la Seguridad, contando con el asesoramiento del DPD, recogerá las medidas propuestas en el plan de tratamiento trasladando al Responsable del Sistema aquellas que deban implementarse. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el ENS.

Asimismo, con las mismas reglas de revisión, deberán ser realizados análisis de riesgos en materia de despliegue y uso de Inteligencia Artificial (IA) en el seno de la organización, de conformidad con lo dispuesto en el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y

las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

11. GESTIÓN DE PERSONAL

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

Todos los miembros de la organización atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

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

12. PROFESIONALIDAD Y SEGURIDAD DE LOS RECURSOS HUMANOS

Esta Política se aplica a todo el personal de la organización y al personal externo que realiza tareas dentro de la entidad, en su caso.

El *Área de Organización y RRHH* incluirá funciones de seguridad de la información en las descripciones de los trabajos de los empleados vinculados al sistema de información, informará a todo el personal que contrate de sus obligaciones con respecto al cumplimiento de la presente Política de Seguridad y Privacidad de la Información, gestionará los compromisos de confidencialidad con el personal y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

El Responsable de Seguridad de la información (RSEG) elaborará un modelo de *Compromiso de Confidencialidad* que firmarán los empleados y terceros que desempeñen funciones en la organización, y participará en el asesoramiento sobre las sanciones que se aplicarán por incumplimiento de esta Política. Asimismo, gestionará el tratamiento de incidentes de seguridad de la información y será responsable de monitorear, documentar y analizar los incidentes de seguridad reportados, así como de comunicarlos al CSEG y a los propietarios de información.

El CSEG será responsable de implementar los medios y canales necesarios para que el RSEG maneje informes de incidentes y anomalías del sistema. El Comité supervisará la investigación, evolución y resolución de incidentes de seguridad de la información.

Todo el personal de la organización es responsable de informar sobre las debilidades e incidentes de seguridad de la información que se detectan oportunamente.

Para fomentar la profesionalidad de los recursos humanos, la organización deberá:

- Determinar la competencia necesaria del personal para llevar a cabo el trabajo que afecta a la Seguridad y Privacidad de la Información;
- Asegurar que las personas sean competentes sobre la base de la educación, capacitación o experiencia adecuadas;
- Demostrar mediante la información documentada la competencia del personal en materia de Seguridad de la Información y Protección de datos personales;

Los objetivos fijados al objeto de controlar la seguridad en torno al personal son:

- Reducir los riesgos de error humano, puesta en marcha de irregularidades, uso indebido de instalaciones y recursos, y manejo no autorizado de la información;
- Explicar las responsabilidades de seguridad en la etapa de reclutamiento del personal e incluirlas en los acuerdos a firmar y verificar su cumplimiento durante el desempeño de las tareas del empleado;
- Asegúrese de que los usuarios estén al tanto de las amenazas y preocupaciones de seguridad de la información y estén capacitados para apoyar la Política de Seguridad y Privacidad de la Información de la organización en el curso de sus tareas normales;

- Establecer compromisos de confidencialidad con todo el personal y usuarios fuera de las instalaciones de procesamiento de información;
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de las debilidades de seguridad existentes, así como los incidentes, con el fin de minimizar sus efectos y prevenir su reincidencia.

13. AUTORIZACIÓN Y CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

El control del acceso a los sistemas de información tiene por objetivo:

- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de la organización y otras redes públicas o privadas.
- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.
- Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y ordenadores personales para el trabajo remoto.

Para habilitar la consecución de estos objetivos, la organización aprueba una política específica de *Gestión de accesos e Identidades*.

14. PROTECCIÓN DE LAS INSTALACIONES

Los objetivos de esta política en materia de protección de las instalaciones son:

- Prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de nuestra organización.

- Proteger los equipos de procesamiento de información crítico de la organización, colocándolos en áreas protegidas y dentro de un perímetro de seguridad definido y con las medidas de seguridad y controles de acceso adecuados. Asimismo, protegerlos en su traslado y mantenimiento.
- Controlar los factores ambientales que podrían perjudicar el buen funcionamiento de los equipos que albergan la información de la organización.
- Implementar medidas para proteger la información manejada por el personal en las oficinas y áreas de tratamiento de la información, dentro del marco normal de sus tareas habituales.
- Proporcionar protección en proporción a los riesgos identificados.
- Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información de la organización: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.
- El RSEG, junto con los propietarios de la Información, según proceda, definirá las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos, y supervisará su aplicación. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.
- Los responsables de los diferentes departamentos definirán los niveles de acceso físico del personal de la organización a las áreas restringidas bajo su responsabilidad. Los propietarios de información autorizarán formalmente el trabajo fuera de las instalaciones a los empleados de la entidad, atendiendo a la política y protocolos implantados en la organización.
- Todo el personal de la organización es responsable del cumplimiento de la política de pantalla limpia y escritorio, para la protección de la información relacionada con el trabajo diario en las oficinas.

Estos objetivos serán desarrollados a través de la política específica de *Seguridad física de instalaciones*.

15. ADQUISICIÓN DE PRODUCTOS

Los diferentes departamentos deben cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su

retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por otro lado, se tendrá en cuenta la seguridad de la información en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.

La política de desarrollo y adquisición de sistemas de información se desarrolla en el procedimiento de desarrollo seguro, prueba y aceptación de nuevos componentes.

16 TERCERAS PARTES /PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES

Cuando la entidad preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad y Privacidad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios; y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando la entidad utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad en la medida en que ataña a dichos servicios o información, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS. En la adquisición de derechos de uso de activos en la nube se tendrán en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II ENS y las Guía de desarrollo.

Dichas entidades, que actúan como terceras partes, quedarán sujetas a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos

operativos para satisfacerla, de modo que la entidad pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe 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 del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la entidad adquiera, desarrolle o implemente un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

17. SEGURIDAD POR DEFECTO

La entidad considera un factor esencial el hecho de que los procesos operativos, de apoyo y estratégicos, así como los proyectos promovidos o participados, integren la seguridad de la información como parte de su ciclo de vida. Los sistemas de información y los servicios deben incluir la seguridad por defecto desde su creación hasta su retirada, incluyéndose la seguridad en las decisiones de desarrollo o adquisición y en todas las actividades en explotación estableciéndose la seguridad como un proceso integral y transversal.

18. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

La entidad se compromete a garantizar la integridad del sistema mediante un proceso de gestión de cambios que permita el control de la actualización de los elementos físicos y lógicos a través de un mecanismo de autorización previa a su instalación en el sistema. Este control será llevado a cabo por el RSIS o el AS, oído el RSEG, el cual evaluará el impacto en la seguridad del sistema antes de que sean autorizados los cambios, y controlará de forma documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas. La autorización de estos cambios relevantes recaerá sobre el Comité de Seguridad (CSEG).

Mediante revisiones periódicas de seguridad, se evaluará el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

19. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

La entidad dispone de una *Política específica de Protección de Datos Personales* en garantía de cumplimiento de la normativa nacional y comunitaria sobre la materia. Dicha política tendrá a su vez rango normativo en el seno de la entidad.

Asimismo, la privacidad se encuentra inserta en la gestión de riesgos como un atributo más de la información, en virtud de lo cual la protección de datos es un elemento transversal en el sistema de información del CZFC.

20. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

La entidad establece medidas de protección para la seguridad de la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, teléfonos móviles, tablets, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

Las medidas técnicas y organizativas idóneas para la protección de la información en tránsito serán las establecidas en los procedimientos de *Seguridad de equipos y soportes* y *Arquitectura de seguridad y Monitorización*, entre otros instrumentos.

21. PROTECCIÓN DE SISTEMAS DE INFORMACIÓN INTERCONECTADOS

La entidad establece medidas de protección para la Seguridad de la Información para proteger el perímetro, en particular, si se conecta a redes públicas o se utilizan principalmente para la prestación de servicios de comunicaciones electrónicas disponibles para el público

En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

22. GESTIÓN DE INCIDENTES Y BRECHAS DE SEGURIDAD

CZFC dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

Los objetivos principales de la Gestión de incidentes son:

- Establecer un sistema de detección y reacción frente a código dañino
- Disponer de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
- Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones.

- Este registro se emplea para la mejora continua de la seguridad del sistema.
- Garantizar que los servicios de IT vuelvan a tener un desempeño óptimo.
- Reducir los posibles riesgos e impactos que pueda causar el incidente.
- Velar por la integridad de los sistemas en el caso de un incidente de seguridad
- Comunicar el impacto de un incidente tan pronto como se detecte para activar la alarma; y poner en práctica un plan de comunicación empresarial adecuado.
- Promover la eficiencia empresarial.

23. CONTINUIDAD DE LA ACTIVIDAD

La entidad, con el objetivo de garantizar la continuidad de las actividades, establece medidas para que los sistemas dispongan de copias de seguridad y establezcan mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

A tal objeto, ha elaborado una política específica de *Continuidad del negocio*, en la cual se establece un Plan de recuperación ante desastres.

24. MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

La entidad establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecidos tanto en el Esquema Nacional de Seguridad como en el estándar internacional ISO 27001.

25. TRANSVERSALIDAD Y DEBER DE COLABORACIÓN EN LA IMPLANTACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Todas las áreas, órganos y unidades departamentales prestarán su colaboración en las actuaciones de implementación de la PSP aprobada a través del presente documento.

El carácter transversal de la misma implica que el contenido de dicha política tendrá carácter informador de los distintos servicios, procesos, proyectos y actuaciones que formen parte de la actividad operativa o institucional de la organización.

26. CONCIENCIACIÓN Y FORMACIÓN

La entidad tiene por objetivo lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros del CZFC y a todas sus actividades, de conformidad con el principio de seguridad integral recogido en el artículo 5 ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se recaen sobre los activos de información.

27. DIRECTRICES/POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Con arreglo a lo dispuesto en el artículo 12 RD 311/2022 por el que se aprueba en ENS, la PSP está integrada por un conjunto de directrices o políticas específicas que rigen la forma en que el CZFC gestiona y protege la información que trata y los servicios que presta.

Este conjunto de directrices está integrado por las siguientes políticas específicas de seguridad y privacidad de la información (PSP):

Directrices/Políticas específicas de Seguridad y Privacidad de la información	
PSP-01	Gestión de riesgos
PSP-02	Autorizaciones y Gestión de cambios
PSP-03-N*	Política de Protección de Datos Personales
PSP-04	Entorno organizativo
PSP-05	Gestión de activos de información
PSP-06-N*	Uso aceptable de los activos de información

PSP-07	Control de acceso e identidades
PSP-08	Seguridad en la contratación de bienes y servicios
PSP-09	Gestión de incidentes de seguridad
PSP-10	Continuidad del negocio
PSP-11	Cumplimiento normativo, protección de registros y auditoría
PSP-12	Seguridad en torno a las personas
PSP-13	Seguridad física de instalaciones
PSP-14	Seguridad de equipos y soportes
PSP-15	Arquitectura de seguridad y monitorización del sistema
PSP-16	Copias de seguridad y sistema de redundancia
PSP-17	Seguridad de redes y comunicaciones
PSP-18	Criptografía y gestión de claves
PSP-19	Desarrollo seguro, prueba y aceptación de aplicaciones

**Políticas específicas con rango de Normativa de Seguridad, con arreglo a lo dispuesto en el control [org.2] del ENS.*

Tanto la presente Política como las distintas políticas específicas enumeradas podrán ser objeto de desarrollo a través de procedimientos operativos de seguridad, denominados Instrucciones de seguridad y privacidad (ISP).

En Cádiz, a la fecha de su firma electrónica.