Política de Seguridad de la Información de Isdefe

ISSGFG-202137-5IL
05.07.2024

REGISTRO DE CAMBIOS

NUEVA EDICIÓN	FECHA ELABORACIÓN NUEVA EDICIÓN	SECCIÓN AFECTADA	OBSERVACIONES
1	05.05.2020	TODAS	PRIMERA EDICIÓN DEL DOCUMENTO
2	19.01.2023	TODAS	REVISIÓN DEL DOCUMENTO POR RD 311/2022
3	20.10.2023	Ver Observaciones	Modificación del código del documento por error en la versión 2. Apartado 7.2: se aclara que en el caso de ausencia del Presidente del CSI el sustituto será el miembro de la Dirección con más antigüedad en la empresa. Apartado 7.2: se modifica el número de reuniones del CSI de tres a 2 al año. Apartado 11: se eliminan referencias a terceras partes.
4	05.03.2024	Ver Observaciones	Apartados 5, 7, 7.2 por Inclusión en la Política de la figura del DPD. Nuevos apartados 7.5 DPD y 7.8 Encargado del Tratamiento y remuneración de los apartados siguientes. Mejora en las responsabilidades del responsable y encargado del tratamiento (apartado 7.3). Aclaración en los apartados 7.4, 7.6 y 7.7 de la designación de responsables delegados. Modificación del apartado 9 de análisis y gestión de riesgos.
5	05.07.2024	1, 7.9	Se simplifica el texto del apartado de Objeto. Se incluye el proceso de renovación de los roles de seguridad de la información.

LISTA DE DISTRIBUCIÓN

DESTINATARIO	ORGANISMO/EMPRESA
TODO EL PERSONAL DE ISDEFE	ISDEFE

ÍNDICE

1. OBJETO

El objeto del presente documento es definir la Política de Seguridad de la Información (PSI) de Ingeniería de Sistemas para la Defensa de España, S.A., S.M.E., M.P., Isdefe.

La PSI se ha elaborado teniendo en cuenta las normas relacionadas en el apartado 4 de este documento "Marco Normativo", y en especial el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS). En su revisión y aprobación ha participado toda la Organización de Seguridad de la Información establecida en el apartado 7 de este documento.

La PSI establece los principios básicos, la organización y las responsabilidades de seguridad para alcanzar un grado de protección adecuado, asegurando la consistencia e integridad de todas las medidas implantadas en materia de seguridad de la información, así como la privacidad de los datos de carácter personal.

La PSI está orientada a asegurar el cumplimiento de la misión de Isdefe.

2. MISIÓN DE ISDEFE

Isdefe es una sociedad mercantil estatal que forma parte del sector público institucional estatal, que tiene la consideración de medio propio y servicio técnico de la Administración General del Estado (AGE) y de los Entes, Entidades y Organismos dependientes de ellos. Está adscrita al Ministerio de Defensa de España, siendo su presidente la persona titular de la Secretaría de Estado de Defensa.

La misión de Isdefe es:

> "*Apoyar al Ministerio de Defensa, a las Administraciones Públicas e Instituciones Internacionales en áreas de interés tecnológico y estratégico, mediante servicios de la máxima calidad en consultoría, ingeniería, así como en la gestión, operación técnica y mantenimiento de complejos aeroespaciales".*

3. ÁMBITO DE APLICACIÓN

Esta PSI es aplicable a:

- Toda la información de Isdefe, propia o encomendada a ella, salvo en el caso de existencia de alguna normal legal o contractual de aplicación, cuyo cumplimiento sea obligatorio, independientemente de su formato.
- Todos los sistemas de información y comunicaciones administrados y gestionados por Isdefe, salvo aquellos que por impedimentos legales u operativos no puedan ser administrados o gestionados adecuadamente por Isdefe, en cuyo caso, se regirán por la normativa de seguridad específica que venga determinada por tales circunstancias.
- Todas las personas (empleados, subcontratistas, colaboradores, terceras partes, etc.) que accedan o manejen información de Isdefe o accedan a sus sistemas de información y comunicaciones.
- Todas las instalaciones de Isdefe donde se maneje su información.
- La información clasificada en poder de Isdefe, establecida en la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa de aplicación a la misma, así como a los sistemas de información y comunicaciones que la manejan**, sin perjuicio de las medidas especiales y complementarias de seguridad adoptadas por Isdefe** para estos sistemas teniendo en cuenta las normas de protección de la información clasificada publicadas por la Autoridad Nacional, así como las políticas y normas

derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales.

Cualquier norma, instrucción o procedimiento en relación con el referido ámbito de aplicación de la Seguridad de la Información en Isdefe, debe someterse y no contradecir a lo establecido en esta Política.

4. MARCO NORMATIVO

a) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

b) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

c) Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

d) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

e) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

f) 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).

g) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

h) Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

i) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información que traspone la Directiva Europea NIS (Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

j) La Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. El Real Decreto-Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

k) Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE – Reglamento de Servicios Digitales.

l) Ley 9/1968, de 5 de abril, de Secretos Oficiales, modificada por la Ley 48/1978, de 7 de octubre.

m) Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales.

n) Normas de la Autoridad Nacional para la Protección de la Información Clasificada.

Asimismo, formarán parte del marco regulatorio las normas aplicables a la administración electrónica y seguridad de la información que complementen desarrollen o sustituyan las anteriores y que se encuentren dentro del ámbito de aplicación de la PSI de Isdefe.

5. PRINCIPIOS BÁSICOS

Isdefe define el siguiente conjunto de principios básicos de seguridad, entendiéndolos como las directrices de obligado cumplimiento que se deben tener en cuenta en cualquier actividad de la empresa:

PS-1. **Principio de Seguridad como Proceso Integral**: La seguridad en Isdefe se entiende como un proceso integral, constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con la información y los sistemas de información que la maneja, excluyéndose así cualquier actuación individual o tratamiento coyuntural.

La seguridad de la información cuenta con el compromiso y apoyo de todos los niveles directivos de forma que esté coordinada e integrada con otras iniciativas de la organización encaminadas a garantizar un sistema de seguridad coherente y eficaz.

PS-2. **Principio de Gestión de la Seguridad Basada en Riesgos**: El proceso de análisis y gestión de riesgos será una parte esencial del proceso de seguridad de la información, debiendo constituir una actividad continua y permanentemente actualizada. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables mediante el despliegue de medidas de seguridad que establecerán un equilibrio entre la naturaleza de la información y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de la información, se deberán tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

PS-3. **Principio de Prevención, Detección, Respuesta y Conservación**: Se evitará, o al menos prevendrá, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad, debiendo monitorizar los sistemas de información de manera continuada para detectar incidentes o anomalías en los niveles de prestación de los servicios y estableciendo mecanismos para responder eficazmente a los incidentes de seguridad y definiendo protocolos para el intercambio de información relacionada con el incidente. Así mismo, el sistema deberá garantizar la conservación de la información, así como la disponibilidad de los servicios durante todo el ciclo de vida de la información.

PS-4. **Principio de Existencia de Líneas de Defensa**: La seguridad de la información como de los sistemas de Tecnologías de la Información y Comunicaciones (TIC) que la manejan ha de implementarse con una estrategia de protección constituida por múltiples capas de seguridad organizativas, físicas y lógicas, dispuestas de forma que, cuando una de las capas falle permita ganar tiempo para una reacción adecuada, reducir la probabilidad de la ocurrencia y minimizar el impacto final de un incidente de seguridad.

PS-5. **Principio de Vigilancia Continua**: Se medirá el estado de la seguridad, su evolución, la detección de actividades o comportamientos anómalos, las vulnerabilidades y deficiencias en la configuración de los sistemas, debiendo dar oportuna respuesta a las mismas.

PS-6. **Principio de Reevaluación Periódica**: Las medidas de seguridad se reevaluarán y actualizarán periódicamente, mediante procesos de inspección y auditorías, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

PS-7. **Principio de Diferenciación de Responsabilidades**: En los sistemas de información se diferenciarán los roles de responsable de la información, responsable del servicio, responsable de seguridad y responsable del sistema.

En los supuestos de tratamientos de datos personales, se identificará al responsable del tratamiento y, en su caso, al encargado del tratamiento, de acuerdo con lo dispuesto en el artículo 4, apartados 7 y 8 del RGPD y al Título V, Capítulo I y II de la LOPDGDD.

PS-8. **Principio de Seguridad en el Ciclo de Vida de los Sistemas TIC**: La seguridad de la información será una parte integral en cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de diseño, desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y sus necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en los pliegos de licitación para proyectos TIC.

PS-9. **Principio de Protección de Datos Personales**: Se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos personales. Dichas

medidas deberán ser apropiadas en función del análisis de riesgos, así como de una evaluación de impacto relativa a la protección de datos cuando sea probable que un tratamiento, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas según de derive del análisis de riesgos, así como de las eventuales evaluaciones de impacto.

PS-10. **Principio de Gestión de Activos de las Tecnologías de la Información y Comunicaciones (TIC)**: Todos los activos TIC de Isdefe se encontrarán inventariados y categorizados y estarán asociados a un responsable de las decisiones relativas al mismo, incluyendo su seguridad y su acceso.

PS-11. **Principio de Gestión de la Continuidad**: Se deberá garantizar un nivel determinado de disponibilidad de los activos de Isdefe, debiéndose establecer medidas de seguridad sobre la información y los recursos que la manejan, así como otros activos que permitan su recuperación, la evaluación de los daños y la adopción de las medidas oportunas para evitar de nuevo ese fallo, de acuerdo a una Política de la Continuidad de Negocio.

PS-12. **Principio de Finalidad**: Todo activo de la empresa, incluida la información generada por Isdefe, es propiedad de Isdefe, y debe ser utilizado únicamente para los fines de la propia empresa.

PS-13. **Principio de Necesidad de Conocer**: El acceso y difusión de toda la información manejada por Isdefe (propia o externa) debe estar basado en el principio de '**Necesidad de Conocer***',* entendiéndolo como el acceso a dicha información para el correcto desarrollo y cumplimiento de las funciones encomendadas por la organización. Esta 'Necesidad de Conocer' será determinada por el superior jerárquico con competencia en la materia del empleado, salvo que por normativa específica se establezca otro nivel.

PS-14. **Principio de Legalidad**: Las medidas y procedimientos de seguridad para la protección de los activos de la empresa cumplirá siempre con lo establecido en la legalidad vigente aplicable a la materia y de manera especial en lo que afecta a la información clasificada, información sensible y a los datos de carácter personal; así como a la propiedad intelectual e industrial y a la protección del medio ambiente. Igualmente se debe garantizar, bajo el principio de reciprocidad y equivalencia, la protección de los activos propiedad de terceros cuya custodia tenga encomendada la empresa.

PS-15. **Principio de Jerarquía Normativa**: Se deberá garantizar la subordinación de las normas de grado inferior a las de rango superior.

6. REQUISITOS MÍNIMOS DE SEGURIDAD

Los requisitos mínimos de seguridad por los que se desarrolla la PSI son:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de actividad y detección de código dañino.
m) Incidentes de seguridad.

n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

Todos estos requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema de información, y debiendo cumplirse de acuerdo con lo establecido en el artículo 28 del ENS.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La organización de la seguridad debe tener en cuenta la propia organización de Isdefe, y en consecuencia, las responsabilidades en seguridad de la información deben emerger de todos los ámbitos, garantizándose la actuación coordinada y eficaz, de acuerdo con lo previsto en el artículo del ENS relativo a la diferenciación de responsabilidades y funciones.

La estructura organizativa que se define en Isdefe para la gestión de la seguridad de la información establece tres niveles organizativos:

- **Nivel 1 – Gobierno**: Perfil **estratégico** que entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde de la consecución de los objetivos. Está formado por:
  - Responsable de la Información.
  - Responsable del Servicio.
  - Comité de Seguridad de la Información.
  - Responsable del Tratamiento de Datos de Carácter Personal (DCP).
- **Nivel 2 – Supervisión:** Perfil **ejecutivo** que entiende qué actividades realiza cada área y cómo las áreas se coordinan entre sí para alcanzar los objetivos de seguridad de la información marcados por la Alta Dirección. Está formado por:
  - Responsable de Seguridad.
  - Delegado de Protección de Datos.
- **Nivel 3 – Operación:** Perfil **operativo** que se centra en unas actividades concretas y controla cómo se ejecutan y explotan dichas actividades. Está formado por:
  - Responsable del Sistema.
  - Administrador(a) de la Seguridad del Sistema.
  - Encargados(as) del Tratamiento de DCP.

Las **funciones y tareas** específicas asignadas a cada rol definido en la estructura anterior se deberán definir de forma detallada en una **Norma de Organización de la Seguridad de Isdefe**.

7.1. RESPONSABLE DE LA INFORMACIÓN Y RESPONSABLE DEL SERVICIO

Los roles, responsabilidades y funciones del Responsable de la Información (RINFO) y Responsable del Servicio (RSERV), se unifican siendo estos desempeñados por el Consejero Delegado de Isdefe y es, por tanto, el responsable de establecer los requisitos, en materia de seguridad, de la información que se maneja y de los servicios que se prestan según lo dispuesto en el Anexo I del ENS.

Esta responsabilidad es indelegable, aunque las actividades relacionadas con estas funciones podrán ser realizadas por Responsables de Información y Servicios de Unidades Organizativas (RIS-UO) expresamente designados para ello.

7.2. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información (CSI) es el órgano que se responsabiliza de *coordinar, alinear e impulsar todas las actividades de la organización en materia de seguridad de la información*.

Está compuesto por:

- **Presidencia** del CSI que corresponde al Consejero Delegado de Isdefe (Responsable de la Información y Servicio).
- **Secretaría** del CSI que corresponde al responsable del Departamento de Gobernanza, Transparencia y Calidad siendo el encargado de dar soporte al Consejero Delegado en el ámbito de sus competencias en la Seguridad de la Información, además de las funciones propias de la secretaría del Comité listadas posteriormente.
- **Responsable de Seguridad** que corresponde al responsable del Departamento de Seguridad.
- **Responsable del Sistema** que corresponde al responsable del Departamento de Sistemas de Información y Medios (DSIM).
- **Vocales** del CSI, personas que puedan apoyar la coordinación y el alineamiento de todas las actividades de Isdefe en materia de seguridad de la información. Los vocales podrán ir variando en el tiempo, según las necesidades y restructuración orgánica de Isdefe, lo que se reflejará en una resolución aprobada por el Consejero Delegado a propuesta del propio Comité. Inicialmente serán vocales constituyentes del CSI las personas responsables de:
  - Dirección de Administración y Recursos Humanos.
  - Dirección de Desarrollo de Negocio.
  - Dirección de Planificación y Económico-Financiera.
  - Dirección de Operaciones.
  - Dirección de Modernización Tecnológica y Transformación Digital.
  - Departamento Jurídico.
  - Departamento de Innovación, Procesos y Transformación Digital.
  - Gerencia de Seguridad de la Información.
  - Delegado de Protección de Datos.
  - Oficina Técnica del Responsable de Seguridad.
  - Administrador de Seguridad del Sistema.

Todos los componentes del CSI tendrán voz y podrán recabar información o presencia en el mismo de terceras personas en las áreas de su responsabilidad, que tendrán voz, pero no voto. Podrán, así mismo, delegar la asistencia al CSI en reuniones concretas.

En casos de vacante, ausencia, enfermedad, abstención, recusación u otra causa legal, de algunas de las personas que forman parte del CSI, esta será designada por el Consejero Delegado de Isdefe. En el caso del Presidente del CSI, la presidencia corresponderá al miembro de la dirección de mayor antigüedad en la empresa.

El CSI se reunirá con carácter ordinario, como mínimo, dos veces al año, para coordinar e impulsar la seguridad de la información en Isdefe. Sin perjuicio de lo anterior, la secretaría podrá convocar al CSI de manera extraordinaria:

a) A petición urgente motivada del responsable de la información y del servicio, del responsable de seguridad o del responsable del sistema.

b) A petición de al menos un tercio de sus miembros.

c) Al detectar incidencias de seguridad graves.

d) Ante la necesidad de establecer nuevas directrices de seguridad.

7.3. RESPONSABLE DEL TRATAMIENTO DE DCP

El Responsable del Tratamiento de DCP de acuerdo con el RGPD (art.4.7) y LOPDGDD (Título V) es Isdefe, como persona jurídica, y es el responsable de determinar los fines y medios del tratamiento y aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa vigente en materia de protección de datos personales.

La responsabilidad principal del responsable del tratamiento es aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD, revisando y actualizando dichas medidas cuando sea necesario, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas (artículo 24 del RGPD / artículo 28 de la LOPDGDD).

7.4. RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

Los roles, responsabilidades y funciones del Responsable de Seguridad de la información (RSEG**)**, incluida la clasificada, estarán asignadas al responsable del Departamento de Seguridad, que determina las decisiones pertinentes para satisfacer los requisitos de seguridad establecidos por el Responsable de la información y el Responsable del Servicio.

El RSEG podrá designar Responsables de Seguridad de la Información Delegados (RSEG-D) a propuesta, en su caso, de su responsable jerárquico, para la ejecución de sus tareas encomendadas para ciertos tipos de información o de servicios de los sistemas de información. Estos RSEG-D dependerán funcionalmente del RSEG. Se delegan las funciones, no las responsabilidades.

7.5. DELEGADO DE PROTECCIÓN DE DATOS

El responsable del tratamiento de DCP designará un Delegado de Protección de Datos (DPD) que deberá ser parte de la plantilla de Isdefe.

La posición y responsabilidades del DPD de Isdefe estarán de acuerdo con lo dispuesto en el artículo 38 y 39 respectivamente del RGPD y al Título V, Capítulo III de la LOPDGDD.

7.6. RESPONSABLE DEL SISTEMA

Los roles, responsabilidades y funciones del Responsable del Sistema (RSIS) estarán asignadas al responsable del DSIM, responsabilizándose de la prestación del servicio tecnológico (explotación de los sistemas de información) de los sistemas de información de Isdefe, incluidos los sistemas clasificados, atendiendo a las medidas de seguridad determinadas por el RSEG.

El RSIS tiene el cometido del diseño, desarrollo, implementación, instalación, operación, mantenimiento y verificación del funcionamiento de todos los sistemas de información de Isdefe, incluidos los clasificados, durante todo su ciclo de vida, debiendo cumplir en cada fase del ciclo de vida con los requisitos de seguridad establecidos por el RSEG.

El RSIS podrá designar Responsables del Sistema Delegados (RSIS-D) a propuesta, en su caso, de sus responsables jerárquicos, para la ejecución de sus tareas encomendadas para ciertos tipos de información

o servicios de los sistemas de información de Isdefe. Estos RSIS-D, dependerán funcionalmente del RSIS. Se delegan las funciones, no las responsabilidades.

7.7. ADMINISTRADOR DE SEGURIDAD DEL SISTEMA

Los roles, responsabilidades y funciones del Administrador de Seguridad del Sistema (ASS) estarán asignadas al responsable del Área de Sistemas y Soporte, encargándose de la implantación, instalación, operación y mantenimiento de las medidas de seguridad de los sistemas de información de Isdefe, incluidos los sistemas clasificados.

El RSIS podrá designar a los Administradores de Seguridad del Sistema Delegados (ASS-D) que considere necesarios, a propuesta, en su caso, de sus superiores jerárquicos, para la ejecución de las tareas encomendadas al ASS para ciertos tipos de información o servicios de los sistemas de información de Isdefe. Se delegan funciones, no las responsabilidades.

7.8. ENCARGADOS DEL TRATAMIENTO

El Encargado del Tratamiento de DCP de acuerdo con el RGPD (art.4.8) y LOPDGDD (Título V) es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento, Isdefe.

Las responsabilidades principales del encargado se establecen en el artículo 28 del RGPD y artículos 28 y 33 de la LOPDGDD.

7.9. PROCEDIMIENTO DE DESIGNACIÓN Y RENOVACIÓN

La designación del Responsable de Información, Responsable del Servicio, Responsable de Seguridad, Responsable del Sistema y Administrador de Seguridad del Sistema corresponde al Consejero Delegado.

No se precisa renovación de estos roles ya que estas responsabilidades están asignadas a cargos orgánicos, por lo que mientras se esté desempeñando el cargo orgánico tendrá asignada la responsabilidad correspondiente al rol asignado. Por tanto, un rol se renovará cuando el puesto quede vacante y se designe a un nuevo responsable.

7.10. RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre las personas designadas como responsables, de conformidad con lo previsto en la presente Política, corresponderá la resolución del mismo al superior jerárquico, si pertenecen a la misma dirección. En caso contrario, la resolución corresponderá al Consejero Delegado.

8. DATOS DE CARÁCTER PERSONAL

El Registro de las Actividades de Tratamiento (RAT) de Isdefe recoge todos los tratamientos de Datos de Carácter Personal (DCP). En aplicación del principio de responsabilidad proactiva establecido en el RGPD, las actividades de tratamiento de DCP se integrarán en la categorización de sistemas del ENS, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

Todos los sistemas de información de Isdefe se ajustarán a las medidas de seguridad requeridos por la normativa para la naturaleza y finalidad de los DCP definidos.

De acuerdo con la Disposición adicional primera - Medidas de seguridad en el ámbito del sector público de la LOPDGDD, el ENS incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del RGPD. Se aplicará, asimismo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

Las auditorías de seguridad previstas en el ENS incorporarán la revisión de las medidas técnicas y organizativas de seguridad de los datos personales a las que se refiere este artículo.

9. ANÁLISIS Y GESTIÓN DE RIESGOS

La aplicación e implantación de las medidas de seguridad debe realizarse valorando y asumiendo un nivel de riesgos conocido, consiguiendo de esta forma un nivel de protección aceptable en proporción a los daños que pudieran producirse.

Se deberá realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos los sistemas de información que están sujetos a esta Política.

A su vez, se deberá realizar una gestión continua de los riesgos y como resultado de esta, deberán revisarse los análisis de forma periódica. Independientemente de esta gestión continua, se revisará anualmente y cuando:

- cambie sustancialmente la información manejada;
- cambien sustancialmente los servicios prestados;
- ocurra un incidente grave de seguridad o cuando se reporten vulnerabilidades graves que impliquen un cambio sustancial en las salvaguardas del sistema.

El RSEG, manteniendo informado convenientemente al CSI, será el responsable del seguimiento y control de los riesgos sobre la información y los servicios debiendo armonizar los distintos análisis de riesgos. Para ello establecerá una metodología reconocida de análisis y gestión de riesgos y, en lo posible, una herramienta para la realización de estos análisis de riesgos también velará por la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo en su caso, inversiones de carácter horizontal.

El RSEG será el encargado de la realización de los análisis y de la gestión de los riesgos, pudiendo recabar el apoyo de otras unidades organizativas de Isdefe.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se estructura de conformidad con el Principio de Jerarquía Normativa, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes.

- **Primer nivel:** Constituido por el presente documento de “Política de la Seguridad de la Información de Isdefe”. El ámbito de aplicación de esta política alcanza a toda la empresa, la elabora el RSEG y la aprueba el Consejero Delegado.
- **Segundo nivel:** Constituido por las normas y directrices generales de seguridad que desarrollan y detallan la PSI de Isdefe. Su aplicación podrá ser a toda la empresa, o bien referirse a un ámbito

específico inferior (Centro de Trabajo, Sistema concreto, áreas, etc.). La aprobación de estas normas de segundo nivel será realizada por el Responsable de la Información y del Servicio, previa comunicación y estudio por el CSI.

- **Tercer nivel:** Están incluidas en este nivel los documentos de seguridad, que describen paso a paso cómo realizar una cierta actividad mediante procedimientos, guías, recomendaciones, instrucciones, técnicas, etc., en las que predominan disposiciones explicativas, de carácter técnico o procedimental, que se deben seguir o a las que se deben ajustar las conductas, tareas o actividades de las personas y organización en relación con la Seguridad de la Información, para el mejor cumplimiento de uno o varios servicios, áreas o aspectos de Seguridad.

  Su aprobación corresponderá al RSEG.

Esta estructura normativa podrá incorporar asimismo otros instrumentos tales como estándares de seguridad, buenas prácticas, informes técnicos, a criterio de cada uno de los responsables de la estructura de seguridad y siempre dentro del ámbito de sus competencias y responsabilidades.

El Responsable de la Información y Servicio determinará, en cada momento, las responsabilidades de la elaboración de las diferentes normas, procedimientos, guías, instrucciones, etc. en función de la materia o área de que se trate.

11. OBLIGACIONES DEL PERSONAL

Todos los empleados de Isdefe tienen la obligación de conocer y cumplir esta PSI y su normativa de desarrollo, siendo responsabilidad de Isdefe de disponer de los medios necesarios para que la información llegue a todos los afectados mediante la formación y concienciación necesaria en este campo.

Todos los empleados de Isdefe deben conocer y aplicar todas las normas de seguridad y aceptar la existencia de determinadas actividades que pueden ser objeto de control y supervisión, estando estas definidas con objeto de no violar el derecho a la privacidad de las personas y asegurar el cumplimiento de la legislación vigente aplicable. Se debe verificar su cumplimiento durante el desempeño de sus funciones en la organización.

12. FORMACIÓN Y CONCIENCIACIÓN

Todo el personal relacionado con la información, los servicios y los sistemas de información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad de la información. Para garantizar la seguridad aplicable a los sistemas y servicios, se articularán los mecanismos necesarios para llevar a la práctica la concienciación y la formación específica necesaria e imprescindible en todos los niveles de la organización a través de un Plan de Formación y de Concienciación en materia de seguridad de la información responsabilizándose de su elaboración el RSEG y de su aprobación el Responsable de la Información y del Servicio.

Deberán establecerse sesiones de concienciación en materia de seguridad de la información de forma periódica a todo el personal afectado por esta política, en particular al personal de nueva incorporación. Las personas con responsabilidad en el uso, operación o administración de los sistemas de información 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

Teniendo en cuenta que Isdefe presta servicios a otros organismos, o maneja información de otros organismos, se les informará y notificará esta PSI, estableciendo los canales necesarios para reporte y coordinación de los respectivos Comités de Seguridad, y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Isdefe utilice servicios de terceros, o ceda información a terceros, se les notificará esta PSI y la Normativa de Seguridad que implique a dichos servicios o información.

Cuando Isdefe realice una subcontratación y ésta acceda a los servicios y/o información de Isdefe, dicha tercera parte deberá quedar sujeta a las obligaciones establecidas en la presente PSI y a su normativa de desarrollo.

El acceso a los recursos, por parte de estos contratistas, estará condicionado a la adhesión a la PSI y a las normativas asociadas, siendo éstas de obligado cumplimiento.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del RSEG 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 (RIS-UO) afectados antes de seguir adelante.

14. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El RSEG propondrá la revisión de la PSI, siendo aprobada por el Consejero Delegado de Isdefe, previo análisis por parte del CSI, y difundida para que la conozcan todas las partes afectadas.

La revisión de la presente Política se realizará, al menos, bienalmente y se orientará:

- A la identificación de oportunidades de mejora en la gestión de la seguridad.
- A la adaptación a la normativa de aplicación y, en particular al ENS de forma sustancial.
- A la adaptación a los cambios en la estructura organizativa de Isdefe.

15. INCUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El incumplimiento de esta PSI, y en su caso de las normas y procedimientos que la desarrollen, podrá dar lugar a las responsabilidades que, de orden penal, civil, administrativas o laborales correspondan, mediante las correspondientes denuncias, demandas o sanciones disciplinarias.

Sin perjuicio de lo establecido en el párrafo anterior, la dirección de la empresa podrá limitar a los infractores, con carácter temporal o permanente y de modo total o parcial, el uso o acceso de medios o recursos propiedad de Isdefe y, en su caso, de las entidades a las que presta apoyo técnico.

El incumplimiento por terceras partes de la adhesión a esta Política y su normativa de desarrollo podrá dar lugar a penalizaciones o la cancelación del contrato de acuerdo con las cláusulas administrativas suscritas entre las partes.

16. APROBACIÓN Y ENTRADA EN VIGOR

La presente PSI de Isdefe es aprobada por el Consejero Delegado de Isdefe.

Esta PSI es de aplicación desde la fecha de su firma y hasta que sea reemplazada por una nueva Política.

De acuerdo con el Principio de Jerarquía Normativa, quedan derogados todos aquellos aspectos de las normativas de seguridad de la información que entren en contradicción con lo establecido en la presente Política y, en especial, las versiones anteriores aprobadas de la ‘Política de seguridad de la Información de Isdefe’, y la ‘Política de Seguridad de la Información Clasificada en poder de Isdefe’, con código ISSGFI-153855-1IL, de fecha 29.09.2015.