



POL-001

**Política de Seguridad de la
Información**



Edición	Fecha	Elaborado por:
01	01/10/2020	CCN
Revisado por:	Aprobado por:	Responsable del Proceso
Comité de Seguridad	Comité de Seguridad	Responsable de Seguridad

Control de cambios

Versión	Fecha	Resumen de los cambios producidos
01	01/10/2020	Versión inicial

Índice

1	Introducción	5
1.1	Justificación de la Política de Seguridad	5
1.2	Principios básicos	5
1.3	Objetivos de la Seguridad	6
2	Alcance	8
3	Misión y servicios prestados	8
4	Marco normativo	9
5	Organización de la seguridad	11
5.1	Definición de roles	11
5.2	Jerarquía en el proceso de decisiones y mecanismos de coordinación	12
5.3	Detalle de los organismos y designación	14
5.3.1	Comité de Seguridad.....	14
5.3.2	Oficina de Seguridad.....	¡Error! Marcador no definido.
5.3.3	Foro de Seguridad de ICTS	15
5.3.4	Designación miembros de la estructura de seguridad	15
5.4	Detalle de los roles y designación.....	16
5.4.1	Responsable de la Información.....	16
5.4.2	Responsable del Servicio	18
5.4.3	Responsables de información y Servicio designados	19
5.4.4	Responsable de Seguridad.....	20
5.4.5	Responsable del Sistema	22
5.4.6	Administrador de la Seguridad del Sistema.....	23
6	Datos de carácter personal	25
7	Gestión de riesgos	25
7.1	Justificación.....	25
7.2	Criterios de evaluación de riesgos	25
7.3	Proceso de aceptación del riesgo residual.....	26



8	Gestión de incidentes de seguridad	26
8.1	Prevenición de incidentes.....	26
8.2	Monitorización y detección de incidentes.....	27
8.3	Respuesta ante incidentes.....	27
9	Obligaciones del personal	27
10	Terceras partes	28
11	Revisión y aprobación de la política de seguridad	29
12	Estructura y desarrollo de la Política de Seguridad	29
ANEXO	32
	Glosario de términos	32

1 INTRODUCCIÓN

1.1 JUSTIFICACIÓN DE LA POLÍTICA DE SEGURIDAD

El término Infraestructura Científica y Técnica Singular (ICTS) hace referencia a instalaciones, recursos o servicios necesarios para desarrollar investigación de vanguardia y de máxima calidad, así como para la transmisión, intercambio y preservación del conocimiento, la transferencia de tecnología y el fomento de la innovación. Se incluirá también entre estas entidades aquellas que, aun no perteneciendo al mapa de ICTS, sí responden a las mismas características como Entidades Consorciadas.

Las ICTS y Entidades Consorciadas (en adelante, la Organización) dependen de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos como Organización. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

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. Es por ello que el Esquema Nacional de Seguridad (ENS, en adelante), operado por Real Decreto 3/2010 de 8 de enero, en su artículo 11 establece que “Todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su Política de Seguridad, que será aprobada por el titular del órgano superior correspondiente”.

Trasladando esta exigencia al marco de la Organización, esto implica que las diferentes áreas de la Organización deben aplicar las medidas mínimas de seguridad exigidas por el ENS, así como realizar 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.

Todas las áreas deben cerciorarse de que la seguridad TIC 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. Las áreas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

1.2 PRINCIPIOS BÁSICOS

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

- **Alcance estratégico:** La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas de la Organización para conformar un todo coherente y eficaz.
- **Responsabilidad diferenciada:** En los sistemas TIC se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- **Seguridad integral:** La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, 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 Riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos 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 los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
- **Seguridad por defecto:** Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

1.3 OBJETIVOS DE LA SEGURIDAD

La Organización establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- **Gestión de activos de información:** Los activos de información de la Organización se encontrarán inventariados y categorizados y estarán asociados a un responsable.

- Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.
- Protección de datos de carácter personal: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.
- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

2 ALCANCE

La presente Política de Seguridad de la Información será de aplicación a todas las Infraestructuras Científicas y Tecnológicas singulares o Entidades Consorciadas que se hayan adherido expresamente a la misma y al Marco de Certificación Conjunto de ICTS.

En su consecuencia, esta Política de Seguridad de la Información será de obligado cumplimiento para todo el personal que acceda los sistemas TIC o a la información gestionada por los Organismos, con independencia de cuál sea su destino, adscripción o relación con los mismos.

3 MISIÓN Y SERVICIOS PRESTADOS

la Organización basa su objeto en instalaciones, recursos o servicios necesarios para desarrollar investigación de vanguardia y de máxima calidad, así como para la transmisión, intercambio y preservación del conocimiento, la transferencia de tecnología y el fomento de la innovación. Son únicas o excepcionales en su género, con un coste de inversión, mantenimiento y operación muy elevado, y cuya importancia y carácter estratégico justifica su disponibilidad para todo el colectivo de I+D+i. Los organismos poseen tres características fundamentales:

- Son infraestructuras de titularidad pública
- Son singulares
- Están abiertas al acceso competitivo.

la Organización está distribuidas por todo el territorio nacional y quedan recogidas en lo que se denomina el “Mapa de Infraestructuras Científicas y Técnicas Singulares”. Algunas de las áreas temáticas que la componen y que son objeto de la presente Política de Seguridad son la Astronomía y astrofísica, Ciencias de la Salud y Biotecnología, Energía, Materiales, Ciencias del Mar, de la Vida y de la Tierra, Tecnologías de la Información y las Comunicaciones, Ingeniería y Ciencias

La presente Política de Seguridad de la Información aplica a las diferentes actividades en las que participan la Organización a través de medios electrónicos, en concreto:

- a. Obtención y almacenamiento de información técnica y científica relacionada con proyectos de desarrollo e investigación.
- b. Consulta y compartición de información técnica y científica a través de repositorios de información, publicaciones científicas y otros servicios similares.
- c. Impartición de formaciones y asistencia a conferencias y reuniones relacionadas con las áreas de investigación de los organismos.

- d. Administración interna de los organismos en materias económicas, recursos humanos y otros procedimientos logísticos.
- e. Comunicación y gestión de la operativa diaria para la ejecución de tareas por parte de los usuarios.

4 MARCO NORMATIVO

El marco legal en materia de seguridad de la información en que se desarrollan las actividades de la Organización en el ámbito de la prestación de los servicios electrónicos a los beneficiarios viene establecido por la siguiente legislación:

- Ley 14/2011, de 1 de junio, de la [Ciencia, la Tecnología y la Innovación](#).
- El Real Decreto 3/2010, de 8 de enero, por el que se regula el [Esquema Nacional de Seguridad](#) en el ámbito de la Administración Electrónica, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
- Real Decreto 951/2015, de 23 de octubre, [de modificación del Real Decreto 3/2010](#), de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- 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](#).
- 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, de [Régimen Jurídico del Sector Público](#).
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la [Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad](#).
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la [Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad](#).
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la [Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información](#).

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la [Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad](#).
- Documentos y Guías CCN-STIC, en especial la Guía “[CCN-STIC-821 Normas de seguridad en el ENS](#)” y el Anexo I de la Guía “[CCN-STIC-822 – Procedimientos de seguridad en el ENS](#)”.

5 ORGANIZACIÓN DE LA SEGURIDAD

5.1 DEFINICIÓN DE ROLES

Tal como indica el artículo 12 del ENS, la seguridad deberá comprometer a todos los miembros de la Organización.

La Política de Seguridad, según detalla el Anexo II del ENS, en su sección 3.1, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización.

La responsabilidad del éxito de una Organización recae, en última instancia, en su Dirección. La Dirección es responsable de organizar las funciones y responsabilidades, la política de seguridad del Organismo, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

La estructura organizativa de seguridad, y jerarquía en el proceso de decisiones la componen:

Rol	Funciones
Comité de Seguridad	Se configura como un órgano colegiado que da respuesta a las necesidades de seguridad de los organismos, desde el punto de vista estratégico, en relación con los sistemas de información que la entidad RedIRIS utiliza para la prestación de servicios transversales y de seguridad a la comunidad de la Organización.
Oficina de Seguridad	Como elemento operativo, se constituirá una Oficina de Seguridad , cuyas competencias estarán relacionadas con la Normativa y análisis de riesgos, Seguridad en las interconexiones y conectividad, Vigilancia y determinación de superficie de exposición, Monitorización y gestión de incidentes, Observatorio digital y ciber vigilancia y otras funciones relacionadas con la seguridad.
Foro de Seguridad	El Foro podrá desarrollar sus funciones en pleno o en Grupos de Trabajo para el análisis y realización de propuestas específicas a trasladar a la Oficina de Seguridad y servirán para su análisis, debate y toma de decisiones que serán aprobadas, si procede, por parte del Comité de Seguridad.
Órgano de Auditoría Técnico	Como elemento de verificación, se constituirá un Órgano de Auditoría Técnica , cuyas competencias estarán relacionadas con la verificación de las medidas técnicas de seguridad adoptadas en los organismos, la gestión de la

	certificación, la inspección documental del marco normativo y otras tareas relacionadas con la conformidad de los organismos adheridos.
--	---

5.2 JERARQUÍA EN EL PROCESO DE DECISIONES Y MECANISMOS DE COORDINACIÓN

Los diferentes roles de seguridad de la información (autoridad principal y posibles delegadas) se estructuran en una jerarquía donde, desde el/los **Foro de Seguridad** se presentarán, a través de un Directorio de Responsables de la Organización, propuestas y solicitudes a la **Oficina de Seguridad** para su valoración. La Oficina de Seguridad valorará técnicamente las propuestas recibidas, que serán posteriormente presentadas al **Comité de Seguridad** para su aprobación. El Comité de Seguridad, una vez aprobadas las propuestas, dará instrucciones a la Oficina de Seguridad, que se encargará de cumplimentar y supervisar que administradores y operadores implementan las medidas de seguridad según lo establecido en la normativa de seguridad aprobada para los organismos. El **Órgano de Auditoría Técnico** se encargará de verificar el cumplimiento de las medidas de seguridad aprobadas y gestionar las certificaciones y auditorías técnicas necesarias.

El **Comité de Seguridad** de los servicios transversales prestados por RedIRIS para el mapa de la Organización (**COMSEG-ICTS**) se constituye para dar respuesta a las exigencias de seguridad de la información derivadas de la **Adecuación al Esquema Nacional de Seguridad** (ENS, RD 3/2010, de 8 de enero), desde los puntos de vista estratégico y operativo, en relación con los sistemas de información que la entidad RedIRIS utiliza para la prestación de servicios transversales a la comunidad de ICTS adherida al citado proyecto.

En consecuencia, quedan fuera del ámbito de aplicación del presente documento todas aquellas actividades (prestacionales o de seguridad) que realice la Organización al margen de los antedichos servicios transversales prestados por RedIRIS.

Corresponde al **Comité de Seguridad** (COMSEG-ICTS):

- Liderar, coordinar y velar por el correcto desarrollo de los Proyecto de Adecuación al ENS, adoptando las medidas que correspondan, de acuerdo a los fines del Marco de Certificación Conjunto.
- Alentar los procesos de Certificación de la Conformidad con el ENS para los servicios transversales prestados por RedIRIS a la comunidad de ICTS adheridas.
- Proponer para su análisis y, en su caso, aprobar y publicar Normas, Procedimientos, Criterios o Buenas Prácticas en materia de Seguridad y Adecuación al ENS y Certificación de la Conformidad con el ENS.
- Asesorar a la Organización al Proyecto de Adecuación respecto de los métodos, procedimientos, herramientas y criterios en materia de Certificación de la Conformidad con el ENS y, en general, con su implantación, orientando su gestión al mejor servicio del sector público y la mayor y mejor colaboración con el sector privado, fabricantes y suministradores de productos o servicios.

- Asesorar a las partes implicadas en la identificación de otros esquemas, arreglos o acuerdos, donde la defensa de la validez y reconocimiento mutuo de los certificados emitidos sea de interés para los sectores público y privado.

Las funciones de la **Oficina de Seguridad** serán, entre otras que les puedan ser encomendadas por el COMSEG-ICTS:

- Gestión operativa de los servicios de seguridad de los organismos y otros servicios relacionados, su explotación y mantenimiento.
- Análisis y debate de las cuestiones relacionadas con la seguridad de los sistemas de información de la Organización, que hubieren sido presentadas por el Foro de Seguridad de la Organización a través de su Directorio de Responsables de Seguridad.
- Redacción y presentación de propuestas al COMSEG-ICTS.

El Foro de la Seguridad, que podrá desarrollar sus funciones **en pleno o en Grupos de Trabajo**, podrá analizar y proponer acciones o iniciativas específicas, que se trasladarán a la Oficina de Seguridad.

En el Foro de la Seguridad se plantearán y debatirán, entre otras, las necesidades de seguridad de la Organización y tendrá su propio Reglamento Interno para determinar las condiciones de pertenencia, alta y baja de miembros y los quórum necesarios para la adopción de acuerdos.

El Órgano de Auditoría Técnica se conformará como órgano de verificación, debiendo guardar la debida independencia hacia el resto de la estructura de seguridad, y desarrollará las funciones de auditoría y evaluación de la implantación de las normativas, procedimientos y medidas de seguridad aprobadas por el Comité de Seguridad, además de gestionar la conformidad de los sistemas respecto a las diferentes normativas de seguridad aplicables, en especial el ENS. Reportará los hallazgos y conclusiones obtenidos a través de los procesos de verificación, al Comité de Seguridad para su evaluación.

5.3 DETALLE DE LOS ORGANISMOS Y DESIGNACIÓN

5.3.1 COMITÉ DE SEGURIDAD

1. Presidencia:

Corresponderá a la persona designada por el **Ministerio de Ciencia e Innovación**¹ la presidencia del COMSEG-ICTS.

En caso de no poder ser asumida la presidencia por parte del citado Ministerio, se establecerá una presidencia rotatoria entre todos los miembros de la comunidad de ICTS adheridas al citado proyecto, incluida RedIRIS.

2. Miembros permanentes:

Serán miembros permanentes del COMSEG-ICTS, los siguientes:

- a) El **Director de la Oficina de Seguridad** que ejercerá las funciones de **Responsable de Seguridad de la Información (RSEG)** de los servicios transversales prestados por RedIRIS a las ICTS adheridas, y que actuará como Secretario del Comité y en caso de ser necesario asumirá las funciones de Responsable de Seguridad de la Información de los organismos adheridos.
- b) El **Responsable del (de los) Sistema(s) de Información (RSIS)** titularidad de RedIRIS, usado(s) para la prestación de los servicios transversales, que será designado por RedIRIS.
- c) El **Responsable del Órgano de Auditoría Técnica (ROAT)** de RedIRIS encargado de realizar las Auditorías de Seguridad y las actividades de Conformidad con el ENS de los sistemas de información afectados en la prestación de los servicios transversales prestados por RedIRIS y, en su caso, la Auditoría de Seguridad de los sistemas de información titularidad de la Organización y su posterior Certificación.
- d) El **Directorio de Responsables de Seguridad de la Organización** al antedicho Proyecto de Adecuación al ENS. Los miembros del Directorio de Responsables de Seguridad de la Organización aunarán a sus competencias en materia de seguridad aquellas otras que les hubieren sido delegadas por los Responsables de la Información y los Servicios de sus respectivas entidades.
- e) **Un representante del Centro Criptológico Nacional (CCN)**, que actuará como asesor del COMSEG-ICTS, con voz, pero sin voto.

3. Miembros no permanentes:

¹ Se propone este departamento ministerial puesto que lidera el Consejo de Política Científica, Tecnológica y de Innovación, que es el órgano que articula el Mapa de Infraestructuras Científicas y Técnicas Singulares (ICTS).

El COMSEG-ICTS podrá invocar la presencia en sus reuniones de especialistas externos, de los sectores público, privado y/o académico, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

3. Periodicidad de reuniones y adopción de acuerdos:

Durante el desarrollo del Proyecto de Adecuación al ENS, para evaluar el desarrollo del mismo y posibilitar su adecuado seguimiento, el COMSEG-ICTS se reunirá, al menos, una vez al mes.

Una vez alcanzada la Certificación de Conformidad con el ENS de los servicios transversales prestados por RedIRIS, el COMSEG-ICTS se reunirá, al menos, dos veces al año, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.

En cualquier caso, las reuniones se convocarán por su Presidencia, a su iniciativa o por mayoría de sus miembros permanentes.

Las decisiones se adoptarán por consenso de los miembros permanentes.

5.3.2 OFICINA DE SEGURIDAD

La Oficina de Seguridad estará formada por:

- El **Director de la Oficina** como Responsable de Seguridad de la Información (RSEG) de los servicios transversales prestados por RedIRIS a la Organización en Proyecto de Adecuación al ENS, que será designado por RedIRIS, y que actuará como enlace con el COMSEG-ICTS.
- El **Directorio de Responsables de Seguridad de la Organización**.

5.3.3 FORO DE SEGURIDAD DE ICTS

Los miembros del **Directorio de Responsables de Seguridad de la Organización** habrán sido designados por el **Foro de Seguridad de las ICTS**, conforme a su propio Reglamento Interno, del que formará parte un vocal (con voto) representante de cada ICTS adherida (a ser posible su Responsable de Seguridad), que podrá asistir acompañado de otros miembros de la Organización (con voz, pero sin voto).

5.3.4 DESIGNACIÓN MIEMBROS DE LA ESTRUCTURA DE SEGURIDAD

Quedarán designados los siguientes miembros de la estructura de seguridad:

Presidente:	Persona designada por el MCIN
Secretario:	Persona designada por el Comité de Seguridad
Director de la Oficina de Seguridad (RSEG):	Responsable de seguridad de RedIRIS

Responsable de los Sistemas de Información (RSIS):	Director de RedIRIS
Responsable del Órgano de Auditoría Técnico (ROAT):	Persona designada por RedIRIS
Directorio de Responsables de Seguridad de ICTS:	D. José Muñoz de Luna / Centro Nacional del Hidrógeno
	D. Miguel Angel Carmona / Centro de Láser Pulsado
	D. Javier Valladolid Aguinaga / Consorcio del Centro Nacional de Investigación de la Evolución Humana

5.4 DETALLE DE LOS ROLES Y DESIGNACIÓN

5.4.1 RESPONSABLE DE LA INFORMACIÓN

El Responsable de la Información puede ser una persona concreta perteneciente a cada ICTS, o podrá tener sus funciones delegadas al Comité de Seguridad como órgano responsable.

Compatibilidades. 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.

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

Las funciones del Responsable de la Información son las siguientes:

Función	Detalle
Establecer requisitos de seguridad sobre la información	Establece los <u>requisitos de la información</u> en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.

<p>Determinar niveles de seguridad en cada dimensión</p>	<p>Determinar los <u>niveles de seguridad</u> en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.</p> <p>Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta del Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.</p>
<p>Adoptar medidas sobre los datos personales</p>	<p><u>Adoptar las medidas</u> 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.</p>
<p>Responder del uso</p>	<p>Tiene la <u>responsabilidad</u> última del uso que se haga de una cierta información y, por tanto, de su protección.</p>
<p>Responder ante errores</p>	<p>El Responsable de la Información es el <u>responsable último</u> de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.</p>

5.4.2 RESPONSABLE DEL SERVICIO

El Responsable del Servicio será una persona concreta perteneciente a cada ICTS, o podrá tener sus funciones delegadas al Comité de Seguridad como órgano responsable.

Compatibilidades.

- Es posible que coincidan en la misma persona u órgano las responsabilidades de la información y del servicio. La diferenciación tiene sentido:
 - Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
 - Cuando la prestación del servicio no depende de la unidad que es Responsable de la Información.

Incompatibilidades.

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

Las funciones del Responsable del Servicio son las siguientes:

Función	Detalle
Responsabilidad	Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
Establecer los requisitos de seguridad del servicio	Tiene la potestad de <u>establecer los requisitos del servicio</u> en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
Riesgos	<u>Aprobar el riesgo residual</u> (el resultante una vez aplicados los controles de seguridad).
Gestionar los tratamientos de datos personales	En cuanto a lo dispuesto en el RGPD, por delegación del Responsable del Fichero se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión de los ficheros y tratamientos de datos personales que se realizan en su área en concreto, lo cual deberá realizar en coordinación con la Oficina LOPD del

	ISFAS.
--	--------

Consideraciones. El Responsable del Servicio deberá tener en cuenta las siguientes consideraciones:

- La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.
- 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.

5.4.3 RESPONSABLES DE INFORMACIÓN Y SERVICIO DESIGNADOS

Se han designado como Responsable de Servicio y Responsable de la Información a las siguientes personas

Responsable Información	Responsable de Servicio	Organismo al que pertenece
Delegado COMSEG-ICTS	Delegado COMSEG-ICTS	CENTRO NACIONAL DE HIDRÓGENO (CNH2)
Delegado COMSEG-ICTS	Delegado COMSEG-ICTS	CENRO DE LASERES PULSADOS (CLPU)
Delegado COMSEG-ICTS	Delegado COMSEG-ICTS	CENTRO NACIONAL DE INVESTIGACIÓN SOBRE LA EVOLUCIÓN HUMANA (CENIEH)

5.4.4 RESPONSABLE DE LA SEGURIDAD

El Responsable de la Seguridad de la Información es una figura clave, ya que a él le corresponde dinamizar y gestionar el día a día de todo el proceso de seguridad de la información. Se designará un Responsable de la Seguridad en cada organismo adherido, o en caso de no disponer de recursos suficientes para una designación independiente, se podrá delegar esta función en la figura del Responsable de la Seguridad conjunto, representado en el Comité de Seguridad. La figura de Responsable de Seguridad conjunto asume la dirección de la Oficina de Seguridad.

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

Función	Detalle
Política, Normativa y Procedimientos	<ul style="list-style-type: none"> Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la <u>Política y Normativa de Seguridad</u> de la Información, para su aprobación por Dirección. Elaborará y aprobará los <u>Procedimientos Operativos</u> de Seguridad de la Información.
Formación y concienciación	<ul style="list-style-type: none"> <u>Promoverá</u> la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. <u>Elaborará los Planes</u> de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información
Gestión de la Seguridad	<ul style="list-style-type: none"> <u>Mantendrá la seguridad</u> de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización. <u>Recopilará los requisitos de seguridad</u> de los Responsables de Información y Servicio y determinará la categoría del Sistema. <u>Realizará el Análisis de Riesgos.</u> Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de <u>riesgo residual</u> esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS. <u>Elaborará una Declaración de Aplicabilidad</u> a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos. Elaborará, junto a los Responsables de Sistemas, <u>Planes de Mejora de la Seguridad</u>, para su aprobación por el Comité de Seguridad de la Información. Validará los <u>Planes de Continuidad</u> de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la

	<p>Información y probados periódicamente por el Responsable de Sistemas.</p> <ul style="list-style-type: none"> • <u>Aprobará las directrices</u> propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
Comité de Seguridad.	<ul style="list-style-type: none"> • Facilitará periódicamente al Comité de Seguridad un <u>resumen de actuaciones</u> 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).

Delegación de funciones

En caso de 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 podrá designar cuantos Responsables de Seguridad Delegados considere necesarios.

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

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad. Es habitual que se encarguen de la seguridad de sistemas de información concretos o de sistemas de información horizontales.

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

Se han designado como Responsables de Seguridad independientes a las siguientes personas:

Responsable	Organismo al que pertenece
Delegado en RSEG	CENTRO NACIONAL DE HIDRÓGENO (CNH2)
Delegado en RSEG	CENRO DE LASERES PULSADOS (CLPU)
Delegado en RSEG	CENTRO NACIONAL DE INVESTIGACIÓN SOBRE LA EVOLUCIÓN HUMANA (CENIEH)

5.4.5 RESPONSABLE DEL SISTEMA

El Responsable del Sistema es la persona que toma las decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día, y deberá designarse un responsable de sistema en la Organización.

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

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

Las funciones del Responsable del Sistema son las siguientes:

Función	Detalle
Gestionar el Sistema	<ul style="list-style-type: none"> • <u>Desarrollar, operar y mantener el Sistema</u> de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. • Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. • <u>acordar la suspensión</u> del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
Establecer directrices y medidas	<ul style="list-style-type: none"> • Definir la <u>topología y sistema de gestión</u> del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. • Definir la <u>política de conexión</u> o desconexión de equipos y usuarios nuevos en el Sistema. • <u>Decidir las medidas de seguridad</u> que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo. • <u>Determinar la configuración autorizada</u> de hardware y software a utilizar en el Sistema. • Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
Elaborar	<ul style="list-style-type: none"> • Elaborar <u>procedimientos operativos</u> de seguridad. • Establecer <u>planes de contingencia y emergencia</u>, llevando a cabo frecuentes

	ejercicios para que el personal se familiarice con ellos.
Aprobar	<ul style="list-style-type: none"> • Aprobar <u>los cambios</u> que afecten a la seguridad del modo de operación del Sistema. • Aprobar toda <u>modificación</u> sustancial de <u>la configuración</u> de cualquier elemento del Sistema.
Monitorizar	<ul style="list-style-type: none"> • <u>Monitorizar</u> 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.

Delegación de funciones.

En caso de que, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, se podrá designar cuantos Responsables de Sistema Delegados considere necesarios.

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

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de información. Es habitual que se encarguen de subsistemas de información de cierta envergadura o de sistemas de información que presten servicios horizontales.

Se han designado como Responsables del Sistema independientes a las siguientes personas:

Responsable	Organismo al que pertenece
Responsable del sistema CNH2	CENTRO NACIONAL DE HIDRÓGENO (CNH2)
Responsable del sistema CLPU	CENRO DE LASERES PULSADOS (CLPU)
Responsable del sistema CENIEH	CENTRO NACIONAL DE INVESTIGACIÓN SOBRE LA EVOLUCIÓN HUMANA (CENIEH)

5.4.6 ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA

El Administrador de seguridad es la persona encargada de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.

Se designará como Administrador de Seguridad del sistema a la Oficina de Seguridad como órgano responsable, siendo dirigida por el Director de la Oficina de Seguridad.

Las funciones del Administrador de la Seguridad del Sistema son las siguientes:

Función	Detalle
Implementar, gestionar y mantener la seguridad	<ul style="list-style-type: none"> • La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información. • Asegurar que los controles de seguridad establecidos son cumplidos estrictamente. • Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad. • Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
Gestión, configuración y actualización	<ul style="list-style-type: none"> • 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. • Aprobar los cambios en la configuración vigente del Sistema de Información. • Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
Gestión de las autorizaciones	<ul style="list-style-type: none"> • La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
Aplicar los procedimientos	<ul style="list-style-type: none"> • La aplicación de los Procedimientos Operativos de Seguridad. • Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
Monitorizar la seguridad	<ul style="list-style-type: none"> • Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

6 DATOS DE CARÁCTER PERSONAL

La Organización se encuentra en el proceso de completar sus actividades de conformidad con lo dispuesto en el RGPD y en la LOPDGDD.

7 GESTIÓN DE RIESGOS

7.1 JUSTIFICACIÓN

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

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 9 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

7.2 CRITERIOS DE EVALUACIÓN DE RIESGOS

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Los criterios de evaluación de riesgos detallados **se especificarán en la metodología** de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos.

7.3 PROCESO DE ACEPTACIÓN DEL RIESGO RESIDUAL

Los riesgos residuales serán **determinados por** el Responsable de Seguridad de la Información.

Los niveles de Riesgo residuales esperados sobre cada Información tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán **ser aceptados previamente por** su Responsable de esa Información.

Los niveles de Riesgo residuales esperados sobre cada Servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán **ser aceptados previamente por** su Responsable de ese Servicio.

Los **niveles de riesgo residuales** serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

8 GESTIÓN DE INCIDENTES DE SEGURIDAD

8.1 PREVENCIÓN DE INCIDENTES

Los Departamentos o unidades de la Organización deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. El ENS a través de su artículo 19 establece la que los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. De igual forma, el artículo 17 del citado ENS define que los sistemas de instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Para ello las áreas deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los Departamentos o unidades deben:

- Establecer áreas seguras para los sistemas de información crítica o confidencial.
- 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.

8.2 MONITORIZACIÓN Y DETECCIÓN DE INCIDENTES

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 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de la Organización, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.

Se deberán establecer, en función de las necesidades, las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel sistema.

8.3 RESPUESTA ANTE INCIDENTES

Las áreas 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) que resulten de aplicación, en su caso.

9 OBLIGACIONES DEL PERSONAL

Los miembros de la Organización 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 de la Información disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de la organización atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un programa de concienciación continua para atender a 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.

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

10 TERCERAS PARTES

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

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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 Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

11 REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 11 del ENS.

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

12 ESTRUCTURA Y DESARROLLO DE LA POLÍTICA DE SEGURIDAD

La estructura jerárquica de la documentación de seguridad es la siguiente:



Documento	Detalle
Política	<ul style="list-style-type: none"> Define las metas y expectativas de seguridad. Describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos

	<p>perseguidos.</p> <ul style="list-style-type: none"> • Debe ser elaborada por el Comité de Seguridad y ser aprobada por la Dirección.
Normativa	<ul style="list-style-type: none"> • Establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema. • Es de carácter obligatorio. • Debe ser escrita por personas expertas en la materia o por el Responsable de Seguridad y aprobada por el Comité de Seguridad.
Procedimiento	<ul style="list-style-type: none"> • Determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución. • Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar. • Un procedimiento puede apoyarse en otros documentos para especificar, con el nivel de detalle que se desee, las diferentes tareas. Para ello, puede relacionarse con otros procedimientos o con instrucciones técnicas de seguridad. • Debe ser elaborado por el Responsable del Sistema y aprobado por el Responsable de Seguridad.
Instrucciones técnicas	<ul style="list-style-type: none"> • Determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.). • Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar. • Una instrucción técnica debe ser clara y sencilla de interpretar. • Debe documentar los aspectos técnicos necesarios para que la persona que ejecute la instrucción técnica no tenga que tomar decisiones respecto a la ejecución de la misma. A mayor nivel de detalle, mayor precisión y garantía de su correcta ejecución. • Pueden ser elaborados por el Responsable del Sistema o Administrador del Sistema y deben ser aprobados por el Responsable de Seguridad.
Guías	<ul style="list-style-type: none"> • Tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. • Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.



	<ul style="list-style-type: none">• Deben ser aprobadas por el Responsable de Seguridad.
--	--

En la guía CCN-STIC-801 Responsabilidades y Funciones, se detalla el esquema de las principales responsabilidades (quien debe elaborarlo y quién aprobarlo) para cada uno de estos documentos.

ANEXO

GLOSARIO DE TÉRMINOS

Análisis de riesgos

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal

Cualquier información concerniente a personas físicas identificadas o identificables (RGPD).

Gestión de incidentes

Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Política de seguridad

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos.

Principios básicos de seguridad

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema

Persona que se encarga de la explotación del sistema de información.

Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.