Esquema Nacional de Seguridad (ENS)

POLÍTICA DE GESTIÓN y SEGURIDAD DE LA INFORMACIÓN

Febrero 2024 ***Clasificación:****Interno*

Código	Versión	Fecha	Modificación
POL_001µ	1.0	29-02-2024	Versión inicial
Elaborado por:	**Revisado por:**	**Aprobado por:**	**Responsable Documento:**
Responsable del Sistema	Responsable de Seguridad	Pleno Municipal	Responsable de Seguridad

POL_001µ POLÍTICA DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

POL_001µ POLÍTICA DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

Las Entidades Locales adheridas al Marco de Gobernanza de la seguridad de la información de Navarra (en adelante, las Entidades) dependen de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar los objetivos que tienen encomendados. 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 311/2022 de 3 de mayo, en su artículo 12, apartado 2 establece que "Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente".

Trasladando esta exigencia al marco de las Entidades, esto implica que las diferentes áreas de las Entidades 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.

Las entidades 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. Deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo a los Artículos 8 y 10 del ENS.

1.1. JUSTIFICACIÓN DE LA POLÍTICA DE SEGURIDAD

Las Entidades Locales adheridas al Marco de Gobernanza de la seguridad de la información de Navarra (en adelante, las Entidades) dependen de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar los objetivos que tienen encomendados. 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 311/2022 de 3 de mayo, 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 las Entidades, esto implica que las diferentes áreas de las Entidades 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.

Las entidades 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. Igualmente, 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 tal y como vienen reflejados en el Artículo 5:

a) **Seguridad como proceso integral**.

constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información.

b) **Gestión de la seguridad basada en los riesgos.**

permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad.

c) **Prevención, detección, respuesta y conservación**.

contemplando las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen.

d) **Existencia de líneas de defensa.**

Con el objeto de disponer de una estrategia de protección constituida por múltiples capas de seguridad para desarrollar una reacción adecuada frente a los incidentes, se deberán establecer líneas de defensa constituidas por medidas de naturaleza organizativa, física y lógica.

e) **Vigilancia continua.**

Permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

f) **Reevaluación periódica.**

para adecuar la eficacia según se desprenda de la evolución de los riesgos y los sistemas de protección, y en todo caso pudiendo llegar a un replanteamiento de la seguridad.

g) **Diferenciación de responsabilidades.**

Indicando los diferentes roles que participan como son: el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

1.3. OBJETIVOS DE LA SEGURIDAD

Las Entidades establecen 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 las Entidades 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 criticidad, mediante mecanismos que garanticen su seguridad.
- **Control de acceso**: Se limitará el acceso a los activos de información por parte de las personas usuarias, 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 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/as.
- **Protección de datos de carácter personal**: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento, con el fin de 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

Esta Política de Seguridad es de aplicación a todos los sistemas de información que soportan los servicios municipales finalistas ofrecidos a la ciudanía, incluida la Sede Electrónica y que están relacionados con el ejercicio de los derechos por cualquier medio, incluidos los medios electrónicos o con el acceso a la información o al Procedimiento Administrativo Común (Ley 39/2015, de 1 de octubre) y que se encuentran dentro del alcance del Esquema Nacional de Seguridad (ENS).

En cualquier caso, lo indicado en el presente documento aplicará a las Entidades que se adhieran efectivamente al presente marco de gobernanza de la seguridad, aceptando los términos y condiciones que se establezcan.

Se contemplan tanto los servicios comunes que ANIMSA pueda poner a disposición de las Entidades, como los servicios propios que puedan existir en cada una de dichas entidades.

Las Entidades deberá articular los roles de seguridad descritos en esta política y participar en los comités a través de sus representantes.

Esta Política de Seguridad es de obligado cumplimiento para todo el personal que acceda a los sistemas de información TIC de las Entidades, así como a la propia información gestionada por los diferentes organismos en cualquiera de sus formas y formatos.

Aplica con independencia de cuál sea la relación o adscripción con el mismo.

La relación de entidades adscrita a la presente Política de Seguridad de la Información se detalla en el ANEXO I como documento independiente de esta Política.

3. MISIÓN Y SERVICIOS PRESTADOS

Las Entidades, para la gestión de sus intereses y de las funciones y competencias que tienen encomendadas, promueven actividades y prestan servicios públicos que contribuyen a satisfacer las necesidades y expectativas de la población y de todos los grupos de interés.

Las Entidades desean potenciar el uso de las nuevas tecnologías tanto internamente como en sus relaciones con la ciudadanía.

Los principales objetivos que se persiguen con el fin de favorecer la participación y extender gobernanza en las entidades locales son, entre otros, los siguientes:

- Mejorar la calidad de los servicios públicos.
- Fomentar la relación electrónica de la ciudadanía con las Entidades, creando la confianza necesaria
- Reducir los tiempos de tramitación.
- Reducir las cargas administrativas.
- Hacer más transparente y ética las actividades de las Entidades.

4. MARCO NORMATIVO

El marco legal en materia de seguridad de la información en que se desarrollan las actividades de las Entidades en el ámbito de la prestación de los servicios electrónicos a las personas beneficiarias, viene establecido en el **ANEXO III.**

5. ORGANIZACIÓN DE LA SEGURIDAD

5.1. DEFINICIÓN DE ROLES

Tal como indica el artículo 13, apartado 1 del ENS, la seguridad deberá comprometer a todas las personas de la organización.

La Política de Seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del **ANEXO II** del ENS, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento.

La responsabilidad del éxito de una Organización recae, en última instancia, en su Dirección. La Dirección es responsable de organizar funciones y responsabilidades, definir las directrices d la Política de Seguridad, así como 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 (COMSEG)	Se configura como un órgano colegiado que da respuesta a las necesidades de seguridad de las Entidades Locales definidas en el ANEXO I, desde el punto de vista estratégico, en relación con los sistemas de información utilizados para la prestación de todos los servicios establecidos en el alcance.
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 "cibervigilancia" 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 TÉCNICA	Como elemento de verificación, se podrá constituir 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 que desde el Foro de Seguridad se presentarán, a través de un Directorio de Responsables, 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 las personas administradoras y operadoras implementan las medidas de seguridad según lo establecido en la normativa de seguridad aprobada para las Entidades.

El **Órgano de Auditoría Técnico**, en caso de conformarse, se encargará de verificar el cumplimiento de las medidas de seguridad aprobadas y gestionar las certificaciones y auditorías técnicas necesarias.

El Comité de Seguridad se constituye para dar respuesta a las exigencias de seguridad de la información derivada de la Adecuación al Esquema Nacional de Seguridad (ENS, RD 311/2022, de 3 de mayo), desde los puntos de vista estratégico y operativo, en relación con los sistemas de información que dan soporte a los servicios indicados en el alcance.

En consecuencia, quedan fuera del ámbito de aplicación del presente documento todas aquellas actividades (prestacionales o de seguridad) realizadas al margen de los antedichos servicios finalistas.

Corresponde al Comité de Seguridad (COMSEG):

- Liderar, coordinar y velar por el correcto desarrollo de los Proyectos 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 prestados por los organismos adheridos.
- 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 los organismos adscritos 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.

Las funciones de la Oficina de Seguridad serán, entre otras que les puedan ser encomendadas por el COMSEG, las siguientes:

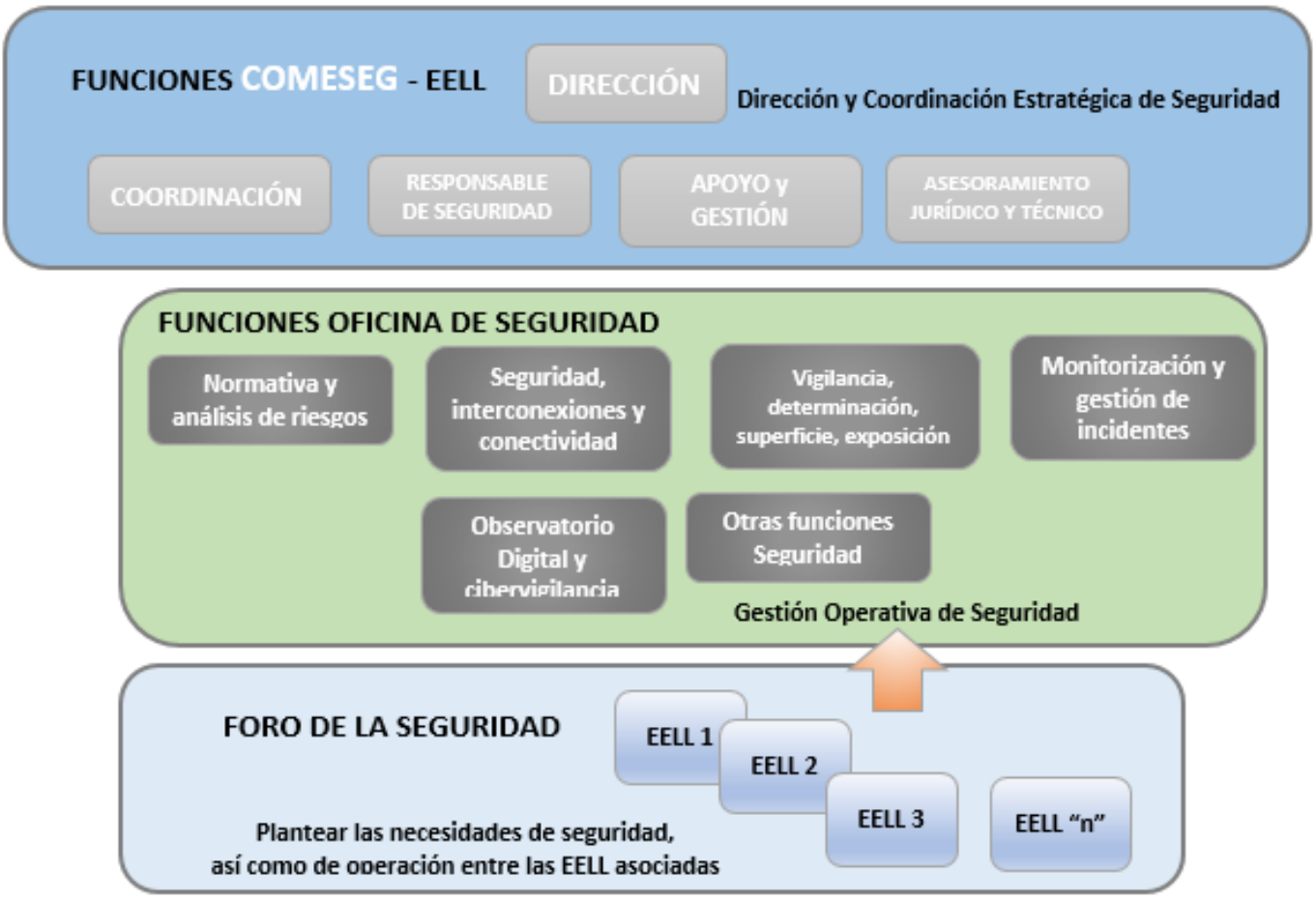
- Gestionar la operativa de los servicios de seguridad de los organismos y otros servicios relacionados, su explotación y mantenimiento.
- Analizar y debatir las cuestiones relacionadas con la seguridad de los sistemas de información de las Entidades adheridas, que hubieren sido presentadas por el Foro de Seguridad a través de su Directorio de Responsables de Seguridad.
- Redactar y presentar propuestas al Comité de Seguridad.

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 las entidades organismos adheridos y tendrá su propio Reglamento Interno para determinar las condiciones de pertenencia, alta y baja de componentes a la Entidad y los quórums 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.

Las Entidades adheridas a este Marco de Gobernanza serán las responsables de la dotación de los medios necesarios para la implantación de las medidas propuestas por el Comité de Seguridad.



5.3. DETALLE DE LOS ÓRGANOS Y DESIGNACIÓN

La designación nominal de la estructura de seguridad se detalla en el **ANEXO II** como documento independiente a esta Política.

5.3.1. COMITÉ DE SEGURIDAD

1.- Presidencia: Corresponderá a la persona designada por el Consejo de Administración de ANIMSA.

2.- Componentes permanentes: Serán componentes permanentes del COMSEG:

- La Dirección de la Oficina de Seguridad, que ejercerá las funciones de Responsable de Seguridad (RSEG) de los servicios del alcance prestados a los organismos adheridos.
- Las personas Responsables de los Sistemas de Información (RSIS) usados para la prestación de los servicios del alcance.
- En caso de conformarse el Órgano de Auditoría Técnica, la persona Responsable y encargado/a (ROAT) será quien deba 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 y, en su caso, la Auditoría de Seguridad de sistemas de información titularidad de los distintos organismos y su posterior Certificación
- Directorio de representantes del foro de seguridad de las entidades adheridas. Las personas que componen el Directorio aunarán a sus competencias en materia de seguridad aquellas otras que les

hubieren sido delegadas por las personas Responsables de la Información y los Servicios de sus respectivas Entidades.

3.- Componentes no permanentes:

- Una persona representante del Centro Criptológico Nacional (CCN), que actuará como asesor/a del COMSEG, con voz, pero sin voto.
- El COMSEG podrá invocar la presencia en sus reuniones de personas especialistas externas, 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.

4.- 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 se reunirá, al menos, cada tres meses.
- Una vez alcanzada la Certificación de Conformidad con el ENS de los servicios prestados, el COMSEG 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 las personas componentes permanentes.
- Las decisiones se adoptarán por mayoría simple de las personas componentes permanentes con un voto de calidad para la Presidencia.

5.3.2. OFICINA DE SEGURIDAD

La Oficina de Seguridad estará formada por:

- La Dirección de la Oficina de Seguridad, que será designada por el presidente del COMSEG, y que actuará como enlace con el COMSEG.
- Las personas Responsables de los Sistemas de Información (RSIS) usados para la prestación de los servicios del alcance.
- Las personas que administran los sistemas incluidos en el alcance del servicio como el personal técnico encargado de la gestión y documentación de los sistemas TIC.

5.3.3. FORO DE SEGURIDAD

Las personas componentes del Foro de Seguridad serán designadas por las Entidades adheridas.

Cada Entidad podrá tener una persona representante con voz y voto, que podrá asistir acompañado/a de otras personas (con voz, pero sin voto).

El Foro de la Seguridad designará a las dos personas que formarán el Directorio de Representantes del Foro, elegidas por las personas componentes con voto.

5.3.4. DESIGNACIÓN DE COMPONENTES PERMANENTES DEL COMITÉ DE SEGURIDAD

PRESIDENCIA	Quien designe el Consejo de Administración de ANIMSA
SECRETARÍA	Quien designe la Presidencia
DIRECCIÓN OFICINA DE SEGURIDAD (RSEG)	Quien designe la Gerencia de ANIMSA

RESPONSABLE DE LOS SISTEMAS DE INFORMACIÓN (RSIS)	Quien designe la Dirección de la Oficina de Seguridad
RESPONSABLE DEL ÓRGANO DE AUDITORÍA TÉCNICO (ROAT)	Quien designe la Presidencia del Comité de Seguridad
ASESOR EN SEGURIDAD	Una persona representante del Centro Criptológico Nacional (CCN)/Otros Asesores
DIRECTORIO DE RESPONSABLES DE SEGURIDAD	Persona 1 designada por el Foro de Seguridad
	Persona 2 designada por el Foro de Seguridad

5.4. DETALLE DE LOS ROLES

5.4.1. RESPONSABLE DE LA INFORMACIÓN

La persona Responsable de la Información es designada por cada Entidad.

- **Compatibilidades**. Este rol podrá coincidir con la del Responsable de Servicio 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 de la persona Responsable de la Información son las siguientes:

Función	Detalle
Establecer los requisitos de seguridad sobre la información	Establecer los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
Determinar niveles de seguridad en cada dimensión	Determinar los niveles de seguridad en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) dentro del marco establecido en el ANEXO I del ENS (Categorías de seguridad de los sistemas de información). Aunque la aprobación formal de los niveles corresponda a la persona Responsable de la Información, podrá recabar una propuesta del Responsable de la Seguridad y podrá tener en cuenta la opinión del Responsable del Sistema.

Adoptar medidas sobre los datos personales	Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados así como los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
Responder del uso	Con la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
Responder ante errores	La persona Responsable de la Información es la persona responsable última de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

5.4.2. RESPONSABLE DEL SERVICIO

La Persona Responsable del Servicio es designada por cada Entidad.

- **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. Tampoco puede 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 establecer los requisitos del servicio 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 a la persona Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión de la persona Responsable del Sistema.
Riesgos	Aprobar el riesgo residual (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 de la persona Responsable del Fichero se encomienda a la persona 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 el Delegado de Protección de Datos (DPD).

Consideraciones. La persona 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, apartado 2 del ENS.

  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. RESPONSABLE DE LA SEGURIDAD

La persona Responsable de la Seguridad es una figura clave, ya que le corresponde dinamizar y gestionar el día a día de todo el proceso de seguridad de la información. Se designará una persona 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 el Comité de Seguridad.

Las funciones de la Persona Responsable de Seguridad son las siguientes:

Función	Detalle
Política, Normativa y Procedimientos	Participará en la elaboración, en el marco del Comité de Seguridad, de la Política y Normativa de Seguridad de la Información, para su aprobación por Dirección. Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.
Formación y concienciación	Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad
Gestión de la Seguridad	Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de las Entidades. Recopilará los requisitos de seguridad de las personas Responsables de Información y Servicio y determinará la categoría del Sistema. Realizará el Análisis de Riesgos. Facilitará a la persona Responsable de Información y a las personas Responsables de Servicio información sobre el nivel de riesgo residual

	esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS. Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al ANEXO II del ENS y del resultado del Análisis de Riesgos. Elaborará, junto a las personas Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad. Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad y probados periódicamente por la persona Responsable de Sistemas. Aprobará las directrices propuestas por las personas 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	Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).

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 cuantas personas Responsables de Seguridad Delegados se considere necesario.

- La designación corresponde a la persona Responsable de la Seguridad. Por medio de la designación de delegados/as, se delegan funciones. La responsabilidad final sigue recayendo sobre la persona Responsable de la Seguridad designado por la Entidad.
- Las personas delegadas se harán cargo, en su ámbito, de todas aquellas acciones que delegue la persona Responsable de la Seguridad. Es habitual que se encarguen de la seguridad de sistemas de información concretos o de sistemas de información horizontales.
- Cada persona delegada tendrá una dependencia funcional directa de la persona Responsable de la Seguridad, que es a quien reportan.

5.4.4. RESPONSABLE DEL SISTEMA

La persona Responsable del Sistema es quien toma las decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día. Se designará una persona Responsable del Sistema en cada organismo adherido o se podrá delegar esta función en el Responsable del Sistema de la Oficina de Seguridad.

Compatibilidades. Este rol podrá coincidir con la persona Administradora de Seguridad del Sistema en organismos de una dimensión reducida o intermedia que tengan una estructura autónoma de funcionamiento.

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

Las funciones del Responsable del Sistema son las siguientes:

Función	Detalle
Gestionar el Sistema	Desarrollar, operar y mantener el Sistema 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. Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con las personas Responsables de la Información afectada, del Servicio afectado y Responsable de la Seguridad antes de ser ejecutada.
Establecer directrices y medidas	Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema. Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo. Determinar la configuración autorizada 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	Elaborar procedimientos operativos de seguridad. Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
Aprobar	Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema. Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
Monitorizar	Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes a la persona Responsable de Seguridad.

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/as Responsables de Sistema Delegados considere necesarios/as.

- La designación corresponde a la persona Responsable del Sistema. Por medio de la designación de delegados/as, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable del Sistema.
- Las personas delegadas se harán cargo, en su ámbito, de todas aquellas acciones que delegue la persona 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.

5.4.5. ADMINISTRADOR/A DE LA SEGURIDAD DEL SISTEMA

La persona Administradora de seguridad se encarga de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.

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

Las funciones de la persona Administradora de la Seguridad del Sistema son las siguientes:

Función	Detalle
Implementar, gestionar y mantener la seguridad	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 las personas 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	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	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	La aplicación de los Procedimientos Operativos de Seguridad. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
Monitorizar la seguridad	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

Las Entidades solo recogerán datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, cada Entidad adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

La normativa vigente en el ámbito de la protección de datos de carácter personal se compone del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril del 2016 (RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD).

En dicha legislación queda regulado que deberán mantenerse actualizados los registros de actividad, así como la inclusión de nuevos tratamientos derivados de la misma en cuanto al tratamiento que realizan personas, empresas u organizaciones de los datos personales relacionados con personas en la Unión Europea (UE).

Las Entidades deben disponer de su propio/a Delegado/a de Protección de Datos (DPD).

La persona Delegada de Protección de Datos desempeña sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Las medidas de seguridad que se tengan que aplicar al tratamiento de los datos de carácter personal serán las establecidas en el artículo 3 del ENS.

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, siendo ésta parte esencial del proceso de seguridad, y debiendo constituir una actividad continua y permanentemente actualizada según lo previsto en el Artículo 7 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 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 se elaborará, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios establecidos en el alcance.

7.3. PROCESO DE ACEPTACIÓN DEL RIESGO RESIDUAL

Los riesgos residuales serán determinados por la persona Responsable de Seguridad y serán presentados al Comité de Seguridad, para que proceda, en su caso a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

8. GESTIÓN DE INCIDENTES DE SEGURIDAD

8.1. INCIDENTES DE SEGURIDAD

Tal y como se establece en al Artículo 25 del ENS, la entidad titular de los sistemas de información dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el Artículo 33, y la Instrucción Técnica de Seguridad correspondiente.

Esta Instrucción Técnica establece los requisitos STIC mínimos que deben implementarse en los sistemas de información de las Administraciones Públicas, cuando manejen información clasificada en los modos seguros de operación “dedicado”, “unificado al nivel superior” o “compartimentado”.

Se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones.

Este registro se empleará para la mejora continua de la seguridad del sistema.

8.2. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos, tal y como se regula en el Artículo 21, apartado 2.

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

La organización deberá implantar las medidas de seguridad oportunas prestando especial atención a los siguientes elementos:

- Protección de información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados

8.3. RESPUESTA ANTE INCIDENTES

Las Entidades deberán:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados.
- Establecer protocolos para el intercambio de información relacionada con el incidente.

8.4. OBLIGACIONES DEL PERSONAL

Los/as componentes de las Entidades tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad de cada Entidad disponer los medios necesarios

para que la información llegue a los implicados.

Las personas componentes a las Entidades 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/as componentes de las Entidades, en particular a los/as 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 y actividades de las Entidades, constituyendo su incumplimiento infracción grave a efectos laborales.

8.5. 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 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 ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias.

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

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

9. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información será revisada por el Comité de Seguridad 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 12 del ENS donde se indica en su apartado c) que deberá seguirse un procedimiento para su designación y renovación.

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

10. ESTRUCTURA Y DESARROLLO DE LA POLÍTICA DE SEGURIDAD

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

A continuación, se detalla cada elemento con precisión:

Documento	Detalle
Política	Define las metas y expectativas de seguridad. Describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos. Debe ser elaborada por el Comité de Seguridad y ser aprobada por la Dirección.
Normativa	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 la persona Responsable de Seguridad y aprobada por el Comité de Seguridad.
Procedimiento	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 la persona Responsable del Sistema y aprobado por la persona Responsable de Seguridad.

Instrucciones Técnicas	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 la persona Responsable del Sistema o Administración del Sistema y deben ser aprobados por la persona Responsable de Seguridad.
Guías	Tienen un carácter formativo y buscan ayudar a las personas usuarias 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. Deben ser aprobadas por la persona Responsable de Seguridad.
Otros Documentos, Registros	Además de los documentos citados, la documentación de seguridad podrá contar con otros adicionales, como son: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, presentaciones, etc.

(*) 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.

11. GLOSARIO DE TÉRMINOS

En la siguiente tabla se definen una serie de términos y abreviaturas que han sido empleados a lo largo de todo el documento y que facilitan el entendimiento del mismo:

Activo	Componente, funcionalidad o recurso que tenga valor para la organización (información, datos, servicios, aplicaciones, equipos, comunicaciones, recursos administrativos, físicos y humanos…).
Amenaza	Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización [UNE-ISO/IEC 27000:2014]. Las amenazas siempre están presentes, pero se pueden intentar evitar o paliar los efectos de su materialización.
Análisis de riesgos	Proceso para el análisis de las amenazas, vulnerabilidades, riesgos e impactos a los que está expuesto un sistema de información, teniendo en cuenta las medidas de seguridad ya presentes. Sirve como punto de partida para identificar las mejoras en las medidas de seguridad, tanto en lo que se refiere a la efectividad como a los costes.
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos [ENS]

Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados [ENS].
Cuerpo normativo	Conjunto de normas que desarrollan de forma más concreta la manera de alcanzar los objetivos de una política.
Dato de carácter personal	Cualquier información concerniente a personas físicas identificadas o identificables [RGPD].
Disponibilidad	Propiedad o característica de los activos consistente en que las Entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren [ENS].
ENS	Esquema Nacional de Seguridad (311/2022, de 3 de mayo).
Gestión de la continuidad	Actividades que lleva a cabo una organización para asegurar que todos los procesos de negocio críticos estarán disponibles para sus usuarios/as, clientes/as, proveedores/as y otras entidades que deban utilizarlos.
Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización con respeto a los riesgos [ENS].
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.
Incidente de seguridad	Suceso inesperado o no deseado con consecuencias negativas para la seguridad del sistema de información [ENS].
Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada [ENS].
LOPDP/GDD	Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.
Medidas de seguridad	Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, disuasión, protección, detección y reacción, o bien de recuperación [ENS].
Política de seguridad	Documento de alto nivel que especifica los objetivos en materia de seguridad de una organización, refleja el compromiso de la dirección para alcanzarlos y rige la forma en que se gestiona y protege la información y los servicios.
Principios Básicos de Seguridad	Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.
Proceso	Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y un fin delimitados, implica recursos y da

	lugar a un resultado [ENS].
RGPD	Reglamento General de Protección de Datos (Reglamento UE 2016/679).
Responsable de la Información	Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.
Responsable de la seguridad	Persona 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.
Riesgo	Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, con daños o perjuicios a la organización [ENS].
Riesgo residual	Riesgo remanente en el sistema tras la implantación de unas determinadas salvaguardas en el plan de tratamiento de riesgos.
Seguridad de la información	Protección de la información y de los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas.
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 [ENS].
Soporte	Medio físico de cualquier tipo (DVD, discos portátiles, etc.) utilizado para almacenar información.
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad [ENS].
Vulnerabilidad	Una debilidad en un activo que puede ser aprovechada por una amenaza [ENS].