Guía de Seguridad de las TIC
CCN-STIC 801

Esquema Nacional de Seguridad
Responsabilidades y Funciones

Junio 2025

Edita:

centro criptológico nacional

Fecha de Edición: junio de 2025

ÍNDICE

1. OBJETO DE LA GUÍA

Esta guía establece unas pautas de carácter general aplicables a todas las entidades del sector público y, en general, a todas las organizaciones comprendidas en el ámbito de aplicación del ENS, tal y como se encuentra definido en el art. 2 del Real Decreto 311/2022, de 3 de mayo. En consecuencia, se espera que cada organización las particularice para adaptarlas a su naturaleza, competencias y entorno singular.

1. El objeto de esta guía es proponer un marco de referencia que establezca las responsabilidades generales en la gestión de la seguridad de los sistemas de información[1] de las entidades del Sector Público, así como aquellas entidades privadas incluidas en el ámbito subjetivo de aplicación del artículo 2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), desarrollando las figuras o roles más significativos que asuman dichas responsabilidades.
2. Tomando como base las directrices señaladas en esta guía, cada entidad debe establecer y aprobar su propia Organización de Seguridad, de acuerdo con su naturaleza, estructura, dimensión y recursos disponibles, que deberá estar recogida en la Política de Seguridad de la Información de la entidad y, cuando se traten datos personales, en la Política de Protección de Datos.
3. La presente Guía incluye el término "entidad" para referirse, con carácter general, a la entidades del sector público incluidas en el ámbito de aplicación del ENS y, en relación con este, en el artículo 2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante LRJSP). Además, en la presente Guía se empleará el citado término para incluir los prestadores privados comprendidos en lo dispuesto en el artículo 2.3 del ENS.
4. Para la definición de las responsabilidades generales en la gobernanza y gestión de la seguridad de los sistemas de información de las organizaciones que manejan información clasificada se atenderá a lo dispuesto en la Guía CCN-STIC 201. Esta Guía CCN-STIC 801 está alineada con el contenido de la Guía CCN-STIC 201.
5. La gestión de la seguridad de los sistemas de información en las entidades -definición, implantación y mantenimiento- exige establecer una Organización de la Seguridad. Tal organización debe determinar con precisión los diferentes actores que la

[1] El ENS define "sistema de información" como: cualquiera de los elementos siguientes:
1.º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.
2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.
3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos. (Anexo IV. Glosario).

conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte.

6. El artículo 11 del ENS señala:

Artículo 11. Diferenciación de responsabilidades.

> *1. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.*
>
> *2. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.*
>
> *3. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.*

7. En dicho artículo se identifican cuatro figuras: Responsable de la Información, del Servicio, de la Seguridad y del Sistema[2]. Además, en los apartados correspondientes a cada una de ellas se tendrán en cuenta las funciones que asumen las terceras entidades que prestan servicios en relación con las que tiene atribuidas el Responsable de la Seguridad y del Sistema[3].
8. Por otro lado, cuando la entidad está tratando datos personales, se hace necesario contemplar al **Delegado de Protección de Datos** con las funciones definidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD, en adelante); y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD, en adelante). Además, la entidad será considera como Responsable del Tratamiento, de conformidad con la definición del artículo 4 del RGPD y, cuando se externalice la prestación de un servicio donde se deban tratar datos personales, la empresa o entidad contratada será considerada como encargada del tratamiento debiendo cumplir con las obligaciones de la Ley de Contratos del Sector Público, el

[2] Parece claro que, mientras que las responsabilidades del Responsable de la Información y Responsable del Servicio son siempre indelegables, no ocurre lo mismo con las correspondientes al Responsable de la Seguridad, que podrían ser asumidas, como competencias propias, por las Diputaciones Provinciales, Cabildos Insulares u otras organizaciones normativa o contractualmente habilitadas, en el caso de las entidades locales. En cualquier caso, habrá que sostener, con carácter general, que todas las responsabilidades mencionadas son indelegables en tanto no exista una habilitación legal que permita la delegación.

[3] Cuando se utilizan servicios externalizados (mediante contrato, convenio, encomienda, etc.), es frecuente que la entidad prestadora (pública o privada) cuente asimismo con un POC al que será exigible el mantenimiento de la seguridad de los sistemas de información concernidos, sin que ello suponga merma de la responsabilidad exigible al Responsable de la Seguridad de la entidad pública destinataria de los servicios.

RGPD y la LOPDGDD, entre otras, en relación con el contrato de encargado del tratamiento, la ubicación de los servidores y los servicios que prestan.

9. El cuadro siguiente muestra las peculiaridades de las figuras más significativas en materia de seguridad de la información, atendiendo a la norma legal de la que traen causa.

Entidad	Referencia normativa	Funciones y/o Características
Dirección de la Entidad	La derivada de la aplicación de la Ley 40/2015 / otra normativa sectorial considerada (Ley 7/1985, de 2 de abril, reguladora de las bases de régimen local, ...	Entidades del Sector Público del ámbito de aplicación del ENS, cuyo titular ostenta la máxima responsabilidad en el desarrollo de las competencias de la entidad, incluyendo las de seguridad de la información, de conformidad con lo dispuesto en las funciones de la normativa sectorial que le aplique en función de la tipología de la entidad.
Responsable de la Información	ENS, art. 13	El Responsable de la Información es habitualmente una persona (o personas) situada en un nivel Directivo de la organización Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Determina los requisitos (de seguridad) de la información tratada
	ENS, art. 41	Efectúa las valoraciones a las que se refiere el artículo 40 del ENS (categorías de seguridad), así como, en su caso, su posterior modificación.
	Op.exp.7	Recibe información sobre los incidentes y de las actuaciones realizadas para su resolución.
	Mp.info.2	Determinación de los criterios para asignar y modificar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
	ENS, art. 13	El Responsable del Servicio es habitualmente una persona (o personas)

Responsable del Servicio		situada en un nivel Directivo de la organización. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Determinará los requisitos de los servicios prestados.
	ENS, art. 41	Efectuará las valoraciones a las que se refiere el artículo 40 (categorías de seguridad), así como, en su caso, su posterior modificación.
	Op.exp.7. r2.3	Será informado de los incidentes y de las actuaciones llevadas a cabo para su resolución
Responsable de la Seguridad	ENS, art. 13	Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones Será distinto del Responsable del Sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos requiera que ambas funciones recaigan en la misma persona o en distintas personas con relación jerárquica, se aplicarán medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11 del ENS. Una Instrucción Técnica de Seguridad regulará el Esquema de Certificación de Responsables de la Seguridad, que recogerá las condiciones y requisitos exigibles a esta figura.
	ENS, art. 13.5	SERVICIOS EXTERNALIZADOS –POC-:

		El Responsable de la Seguridad del servicio externalizado realizará funciones de Punto de Contacto (POC), o bien las delegará en una persona que *formará parte de su área o tendrá comunicación directa con la misma.* EL POC debe contar con el apoyo de la dirección de la entidad. Tiene como funciones la canalización y supervisión tanto del cumplimiento de los requisitos de seguridad del servicio que presta o solución suministrada como las comunicaciones relativas a la seguridad de la información y la gestión de incidentes. En todo caso, la responsabilidad última será de la entidad del sector público destinataria de los citados servicios.
	ENS, art. 28	Formalización y aprobación de las medidas seleccionadas del Anexo II en la Declaración de Aplicabilidad, incluyendo las medidas compensatorias o complementarias de vigilancia y su correspondencia con las medidas del Anexo II antes citado.
	ENS, art. 31	Análisis de los informes de Auditoria de primera, segunda o tercera parte que se refieran a los sistemas de su ámbito competencial, y presentación de sus conclusiones al Responsable del Sistema y, en su caso, al Comité de Seguridad de la Información.
	ENS, art. 41	La determinación de la categoría de seguridad del sistema, con base en las valoraciones de los Responsables de la Información y del Servicio
	Op.exp.5	Aprobación explicita de los cambios que impliquen un riesgo de nivel ALTO con carácter previo a su implantación
	Mp.info.1	Cuando el sistema trate datos personales, el Responsable de la Seguridad recogerá los requisitos de

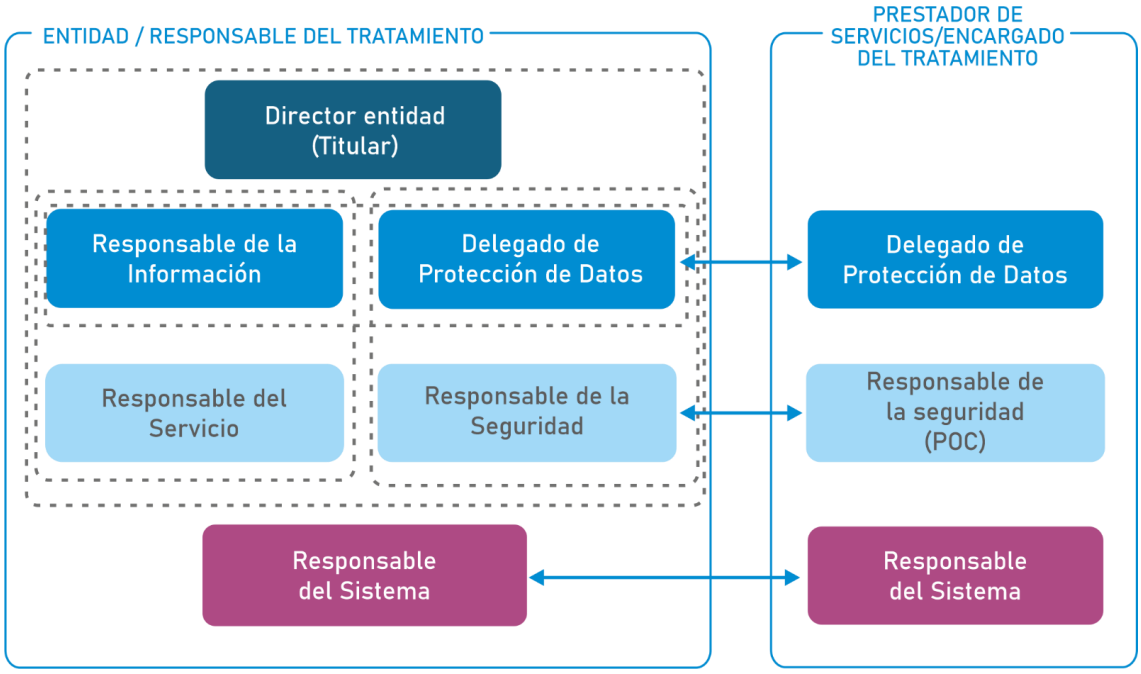
		protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y con la evaluación de impacto en la protección de datos, si se ha llevado a cabo
	Anexo III	Análisis de los informes de auditoría de primera, segunda o tercera parte, notificando o las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.
Responsable del Sistema	ENS, art. 13	Será distinto del Responsable de la Seguridad no debiendo existir dependencia jerárquica entre ambos. Cuando, con carácter excepcional y justificado, ambas figuras recaigan en la misma persona se implementarán medidas compensatorias como señala el art. 11 del ENS Se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad Estas funciones las podrá realizar mediante recursos propios de la entidad o contratados
	ENS, art. 31	Adopta las medidas correctoras adecuadas derivadas de los informes de Auditoría de primera, segunda o tercera parte. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, podrá

		suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación
	ANEXO III	Adopción de medidas correctoras de las auditorías de primera, segunda o tercera parte, según las conclusiones trasladadas por el Responsable de la Seguridad
Administradores del sistema/ de la seguridad	ENS, Art.13 Op.acc.1.r1.1	Actúan como delegados del Responsable del Sistema o del Responsable de la Seguridad
	Op.acc.1. r1.3	Mantiene la lista actualizada de usuarios autorizados
	Op.exp.3. r2.1	Configuración del sistema operativo, aplicaciones tanto de estaciones y servidores como electrónica de red del sistema.
Delegado de Protección de Datos	ENS, art. 3	Además de las funciones que le atribuye la normativa especial (RGPD, LOPDGDD) y los criterios de las autoridades de control (Comité Europeo de Protección de Datos, Agencia Española de Protección de Datos...), el ENS indica que asesora al Responsable o Encargado del Tratamiento en la realización de análisis de riesgos y evaluaciones de impacto.
	Mp.info.1.	El Responsable de la Seguridad contará con la opinión del Delegado de Protección de Datos en relación con los requisitos de la normativa de protección de datos en el sistema de información cuando se traten datos personales

Más adelante se incluyen algunas precisiones adicionales en torno a estas figuras.

2. ESTRUCTURA DE LA SEGURIDAD

10. Atendiendo a lo señalado en los epígrafes precedentes, podemos representar la Estructura de Seguridad (de la Información y de Protección de Datos) según se muestra en la figura siguiente.



Esquema conceptual de la Seguridad de la Información y la Protección de Datos

11. La figura anterior representa un Esquema conceptual de la estructura de Seguridad de la Información y la Protección de Datos, señalando la ubicación o posibles ubicaciones de las figuras que se mencionan, independientemente de su posición concreta en la entidad pública de que se trate o la existencia de posibles Comités u órganos colegiados en los que pudiera integrarse algunas de tales figuras.

12. En base a la figura anterior, podemos señalar lo siguiente:

    a. La operativa de una entidad en el ámbito de aplicación del ENS y del RGPD puede requerir el concurso de terceros externos a la propia organización (públicos o privados). Por este motivo, en la figura aparecen los roles correspondientes a la organización interna y también aquellos otros que pudieran ubicarse en organizaciones externas.

    b. Por imperativo legal, la responsabilidad máxima -también en materia de seguridad de la información ENS y protección de datos- se encuentra en el Titular (Dirección) de la entidad de que se trate en función de las competencias que le son atribuidas por las normas aplicables a cada una de ellas;

    c. Las figuras de Responsable de la Información y Responsable del Servicio pueden recaer en la misma persona, Comité u órgano colegiado. Dependiendo de la

naturaleza o tamaño de la organización, ambas figuras podrán ser coincidentes asimismo con la del Titular de la entidad de que se trate.

d. El Responsable de la Seguridad de la entidad poseerá una responsabilidad inmediata. No obstante, si se utilizan o contratan servicios de terceros (públicos o privados, como sería el caso de la contratación de derecho de uso de activos en la Nube) es imperativo que tales terceros cuenten asimismo con un Punto de Contacto (POC), puesto que puede ser desempeñado por el Responsable de la Seguridad del tercero. En este caso, el Responsable de la Seguridad de la entidad poseerá una responsabilidad mediata,

e. Cuando se contratan con terceros la prestación de los servicios o de determinadas actividades que comporten el tratamiento de datos personales, (siendo en este último caso Encargado del Tratamiento), el Responsable del Sistema del prestador del servicio será quien ejerza dichas funciones con carácter temporal en relación con los sistemas donde se presta el servicio, con una responsabilidad inmediata.

f. El Delegado de Protección de Datos (DPD) puede ser interno o externo a la organización, pudiendo revestir asimismo la forma de un órgano colegiado (Comité Delegado de Protección de Datos), velando siempre por evitar conflicto de intereses en cualquiera de sus miembros. Además de ello, podrá designarse un único DPD para varias autoridades u organismos públicos, teniendo en consideración su estructura y tamaño.

g. La AEPD ha señalado la posibilidad de que el Delegado de Protección de Datos coincida con el Responsable de la Seguridad del ENS "*en aquellas organizaciones que, por su tamaño y recursos, no pudieran observar dicha separación, sería admisible la designación como delegado de protección de datos de la persona que ejerciera las funciones de responsable de seguridad del ENS, siempre que en la misma concurran los requisitos de formación y capacitación previstos en el RGPD. Además, resultaría imprescindible adoptar todas las medidas organizativas, debidamente reflejadas en su Política de seguridad de la información, que garantice la necesaria independencia y la ausencia de conflicto de intereses, por lo que no podría recibir instrucciones respecto al desempeño de sus funciones como delegado de protección de datos, deberá responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. En todo caso, esta circunstancia, que como decíamos, tiene carácter excepcional, deberá evaluarse caso por caso, y deberá dejarse documentada dicha designación haciendo constar los motivos por lo que el organismo correspondiente no ha podido observar dicha separación de funciones, así como las medidas que garantizan la necesaria independencia del delegado de protección de datos*."

h. De conformidad con el principio de "segregación de responsabilidades" recogido en el art. 11 del ENS, el Responsable de la Seguridad será una figura diferenciada del Responsable del Sistema, no habiendo dependencia jerárquica entre ambos.

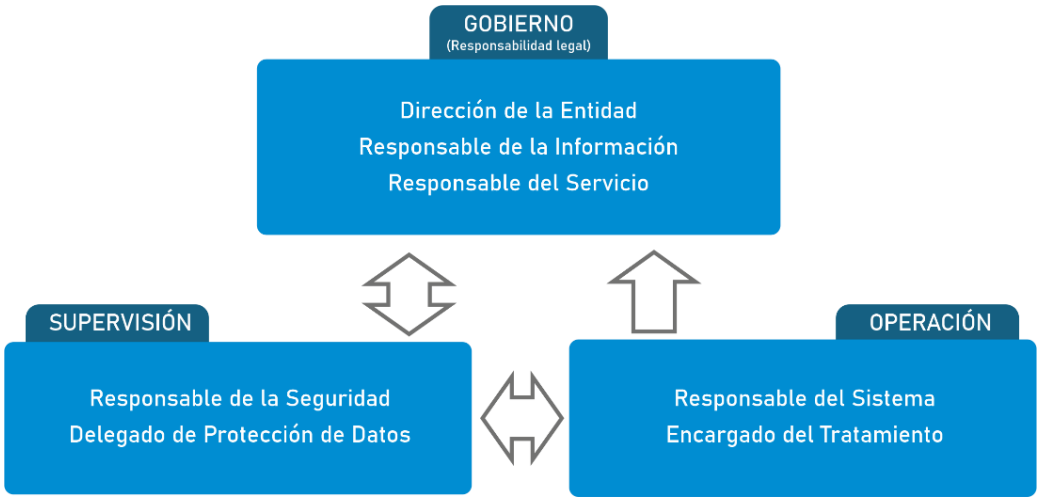
13. El Esquema propuesto diferencia tres grandes bloques de responsabilidad:

    a. Gobierno: La **responsabilidad legal** y la **especificación de las necesidades o requisitos**, que corresponde a la Dirección de la entidad y a los responsables de la información y del servicio y, de acuerdo con las funciones de aprobación de la Declaración de aplicabilidad y de la determinación de la categoría del sistema, al responsable de la seguridad. En entidades de mayor tamaño pueden existir responsables funcionales sobre el tratamiento de datos personales en las diferentes áreas o departamentos.

    b. Supervisión: La **supervisión y asesoramiento**, que corresponde al Responsable de la Seguridad y al Delegado de Protección de Datos, en sus respectivos ámbitos.

    c. Operativo: La **operación del sistema** de información, que corresponde al Responsable del Sistema.

14. La figura siguiente muestra estos bloques de responsabilidad:



Bloques de responsabilidad

15. Como hemos señalado, es posible -y habitual, en organizaciones de tamaño significativo- la existencia de ciertos órganos o comités que pueden colaborar en la seguridad de la entidad, ya sea física, de la información, de protección de datos, o todas ellas.

16. Los más habituales de tales comités son:

    - Comité de Seguridad Corporativa.
    - Comité de Seguridad de información y
    - Comité de Protección de Datos[4].

[4] Cuando, excepcionalmente, pudiera constituirse un Comité conjunto Seguridad de la Información – Protección de Datos, se deberá tener especial cuidado en analizar los posibles conflictos de intereses, muy especialmente en lo que se refiere al Delegado de Protección de Datos, que, en el ejercicio de sus

17. La figura siguiente muestra el encaje habitual de estos comités en una estructura establecida en tres **niveles**: gobierno, ejecutivo/supervisión y operativo.

Niveles de la estructura de seguridad

18. Cuando haya órganos colegiados, estos se constituirán de conformidad con lo dispuesto en la Sección 3ª del Capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público u otra normativa sectorial que le sea de aplicación.

3. RESOLUCIÓN DE CONFLICTOS

19. El mecanismo concreto de resolución de controversias debe figurar en la Política de Seguridad de la Información de la organización.
20. Seguidamente, se examinan los roles correspondientes a los tres niveles señalados.

4. NIVEL DE GOBIERNO: LOS RESPONSABLES DE LA INFORMACIÓN Y DEL SERVICIO

21. La responsabilidad de la actividad de una entidad, con carácter general se sitúa, en última instancia, en su Titular, sin perjuicio de las concretas atribuciones de funciones de las normas administrativas o sectoriales a otros órganos o personas físicas

funciones, no podrá recibir instrucciones, debiendo responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. La Política de Seguridad de la organización y los Términos de Referencia de este Comité deberán reflejar claramente las cautelas adoptadas en tal sentido, conforme a lo dispuesto en el precitado Informe Jurídico de la AEPD 2018-0170. Por otro lado, cuando se constituyan Comités separados, nada obsta para que, teniendo en cuenta las precisiones señaladas, algunos miembros de ambos comités sean coincidentes, como sucede habitualmente con las Oficinas o Unidades de apoyo a la Seguridad de la Información.

22. Con carácter general corresponde al Titular de la entidad, sin perjuicio de las funciones atribuidas a otros órganos, la definición de las estrategias de acción, la dirección de la actividad y las relaciones internas y externas. Además, en función de las competencias que tenga atribuidas, podrá aprobar la Política de Seguridad de la Información y la de Protección de Datos, así como facilitar los recursos adecuados para alcanzar los objetivos propuestos en materia de seguridad, siendo el responsable último del cumplimiento de las obligaciones en materia de seguridad.
23. Así pues, la figura de la Dirección de la entidad (personificada en su Titular) cobra una importancia capital: de la Dirección depende el compromiso de la entidad con la seguridad y su adecuada implantación, gestión y mantenimiento.
24. Por otro lado, suele ser habitual que en una entidad coexistan diferentes informaciones y servicios. La Política de Seguridad de la Información (y Protección de Datos, en su caso) deberá identificar claramente a quién corresponden las funciones que se han señalado con anterioridad para el Responsable de la Información, del Servicio, de la Seguridad, del Sistema y Delegado de Protección de Datos, pudiendo determinar, además, aquellos puestos que serían incompatibles para el desempeño de estas funciones.
25. Con las salvedades señaladas con anterioridad, es posible que una misma persona pueda aunar varias responsabilidades o formar éstas parte de un órgano colegiado a excepción de las figuras del responsable de la seguridad y del sistema.

4.1 EL RESPONSABLE DE LA INFORMACIÓN

26. La información es la materia prima de la que se nutre la actividad de las entidades y puede tener su origen en la propia entidad, las personas que se relacionan con ellas y en terceras entidades (públicas o privadas).

Origen de la información

27. El Responsable de la Información[5] es habitualmente una persona (física o un órgano colegiado) situada en el nivel Directivo de la organización. Esta figura tiene la

[5] Information Owner: Official with statutory or operational authority for specified information and responsibility for es-tablishing the controls for its generation, classification, collection, processing, dissemination, and disposal. See also information steward.

responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección

28. Como hemos visto en el primer epígrafe de esta Guía, el ENS asigna al Responsable de la Información, como principal función, la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información, pudiendo ser una persona física concreta o un órgano colegiado.
29. Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema[6] y la del Delegado de Protección de Datos de acuerdo con las funciones de asesoramiento que le asigna el RGPD.
30. La determinación de los niveles 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.

4.2 EL RESPONSABLE DEL SERVICIO

31. El ENS asigna al Responsable del Servicio -que puede ser una persona física o un órgano colegiado de la entidad-, la función principal 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.
32. 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 y del Delegado de Protección de Datos.
33. La determinación de los niveles 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.
34. En la valoración de un servicio siempre se debe atender a los requisitos de seguridad de la información que maneja (a veces se dice "se heredan los requisitos"), a los que se suele añadir requisitos de disponibilidad, accesibilidad, interoperabilidad, etc.

NIST 800-53: Official with statutory or operational authority for specified information and respon-sibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [CNSSI_4009:2010].

[6] Naturalmente, la responsabilidad última de la adecuada determinación del nivel de seguridad de la información tratada (y los riesgos asumibles) se encuentra en el Titular de la entidad del Sector Público de que se trate, figura que, como hemos visto, puede ser coincidente con la del Responsable de la Información. En el mismo supuesto se encuentra el nivel de seguridad del servicio cuya última responsabilidad recae en el Titular de la entidad.

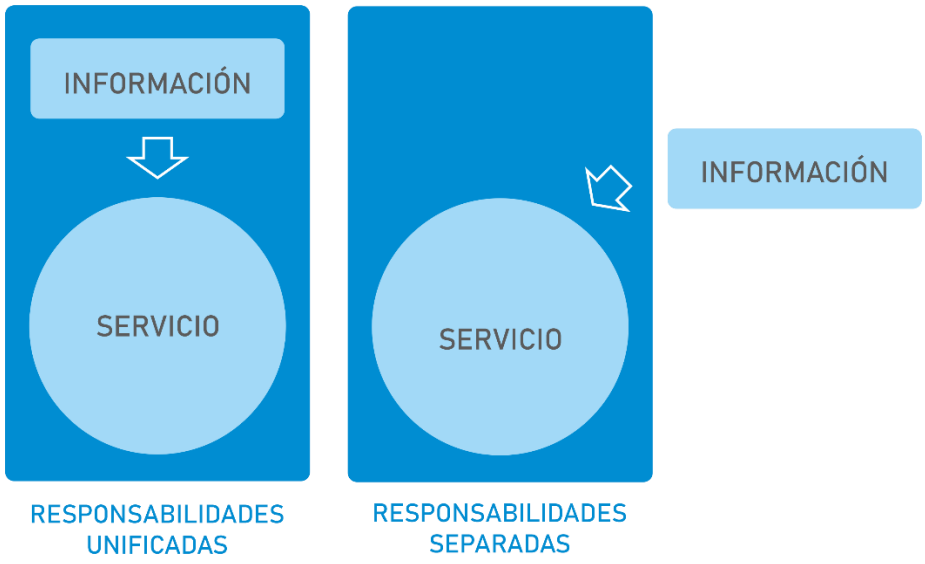
4.3 RESPONSABILIDADES UNIFICADAS

35. Como hemos señalado, es posible que coincidan en la misma persona u órgano colegiado las responsabilidades de la información y del servicio.

36. No obstante, la diferenciación tiene sentido:

    a. Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental o área que presta dicho servicio.

    b. Cuando la prestación del servicio no depende de la unidad o área que gestiona la información.



Responsabilidades unificadas y separadas

5. NIVEL DE SUPERVISIÓN: EL RESPONSABLE DE LA SEGURIDAD

37. El ENS señala que, entre sus principales funciones, el Responsable de la Seguridad[7] determina las decisiones para satisfacer los requisitos de seguridad de la información

[7] Chief Information Security Officer (CISO): The person in charge of information security within the enterprise ISACA, Cybersecurity Glossary, 2014
Chief Information Security Officer (CISO): The CISO (chief information security officer) is a senior-level executive responsible for aligning security initiatives with enterprise programs and business objectives, ensuring that information assets and technologies are adequately protected (http://whatis.techtarget.com/)
Senior Agency Information Security Officer (SAISO): Official responsible for carrying out the Chief Information
Officer responsibilities under the Fed-eral Information Security Management Act (FISMA) and serving as the Chief Information Of-ficer's primary liaison to the agency's authorizing officials, information system owners,

y de los servicios y supervisará la implantación de dichas medidas para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones

38. Además de ello, como hemos visto con anterioridad, en caso de servicios externalizados, la responsabilidad última la tiene siempre la entidad del Sector Público destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, convenio, encomienda, etc.) a la organización prestataria del servicio (lo que sucede, por ejemplo, en la utilización de servicios en la nube).

39. Las funciones esenciales del Responsable de la Seguridad, sin perjuicio de otras enumeradas en el apartado 2 de la presente Guía, son:
    a. Determinar las medias de seguridad aplicables, en función de las valoraciones hechas por los Responsables de la Información y los Servicios.
    b. Elaborar y aprobar la Declaración de Aplicabilidad, atendiendo a los requerimientos del Responsable de la Información y del Servicio
    c. Determinación de la categoría del sistema, atendiendo a las valoraciones del Responsable de la Información y del Servicio.
    d. Comprobar que las medidas de seguridad de la información han sido adecuadamente implementadas por el Responsable del Sistema.
    e. Participar en la elaboración y en la propuesta de la Política de Seguridad de la Información y los procedimientos, normativas e instrucciones en aplicación del ENS.
    f. Analizar los riesgos antes del despliegue de los sistemas de inteligencia artificial en la entidad, atendiendo a las valoraciones del Responsable de la Información y del Servicio y, en su caso, del Delegado de Protección de Datos y supervisar su despliegue.
    g. Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

---

and information systems security officers. (Note: Organizations subordinate to federal agencies may use the term Senior Information Security Officer or Chief Information Security Officer to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.) [CNSSI_4009:2010]

Senior (Agency) Information Security Officer: Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. (Note: Organizations subordinate to federal agencies may use the term Senior Information Security Officer or Chief Information Security

Officer to denote individuals filling positions with similar responsibilities to Senior Agency Information Security

Officers.) U.S. Code 44, Sec. 3544. Federal agency responsibilities, 2007

Chief Information Security Officer (CISO): The position of CISO is relatively new in most organizations. The CISO should be providing tac-tical information security advice and examining the ramifications of new technologies. In most corporations the CISO reports to the CIO or CTO. The CISO role does not usually include respon-sibility for physical security, risk management and business continuity, which are more often del-egated to the CSO. (http://www.csoonline.com/glossary/)

h. En la gestión de los ciberincidentes, contando con los responsables de la entidad, de la información y de los servicios, calificará la peligrosidad de estos de acuerdo a la Guía CCN-STIC 817, actuando como punto de contacto con las autoridades competentes en materia de seguridad y, en función de los roles asignados en la Política podrá notificar los mismos, en su caso, al CCN-CERT. Cuando fuese precisa la notificación al CSIRT de referencia está deberá realizarse sin dilaciones indebidas y con carácter inmediato, sin perjuicio de la remisión de información ampliada de forma paulatina.

40. Además de ello, cuando la figura del Responsable de la Seguridad del ENS coincide con la **Entidad Responsable de Seguridad de la Información** derivada de la Directiva NIS, podrá desplegar las funciones señaladas en el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, vigentes a la fecha de redacción de la presente Guía, o en las normas de trasposición o ejecución de las Directiva NIS2 siempre que cuente con la habilitación suficiente.

    - Estas funciones deberán tener en cuenta las regulaciones de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se derivadas modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2), la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo, así como la normativa nacional que resulte de su transposición.

41. Por otro lado, el Responsable de la Seguridad colaborará con el Delegado de Protección de Datos de la Entidad en la gestión de los incidentes que afecten a datos personales y, en su caso, a la notificación a las autoridades de control y a las personas afectadas.
42. Considerando que las leyes 39/2015 y 40/2015 consagran el uso de los medios electrónicos en el desenvolvimiento cotidiano de las entidades del Sector Público, el Responsable de la Seguridad debe estar situado en una posición que le permita tener un acceso directo a los niveles directivos de la organización teniendo en cuenta las peculiaridades organizativas de cada entidad pública o privada.
43. En aquellos sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesite de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad, cada organización podrá designar Responsables de Seguridad Delegados. La propuesta de designación corresponderá al Responsable de la Seguridad, que delegará funciones, no responsabilidad
44. Los Responsables de Seguridad Delegados se harán cargo, en su ámbito competencial, de todas aquellas funciones delegadas por el Responsable de la Seguridad. Es habitual que se encarguen de la seguridad de sistemas de información

concretos (departamentales, por ejemplo) o de sistemas de información horizontales.

45. Cada Responsable de la Seguridad Delegado mantendrá una dependencia funcional directa del Responsable de la Seguridad, a quien reportará.
46. En entidades más grandes, no hay obstáculo para que la responsabilidad de la seguridad sea dirigida a través de un órgano colegiado, cuyo presidente, formalmente, será el Responsable de la Seguridad en los términos expresados en el ENS, reflejados en la presente guía.
47. El comité u órgano colegiado, podrá estar formado por todas aquellas personas con responsabilidad en materia de seguridad de la información (Responsable de la Seguridad, Responsables de Seguridad Delegados, Responsables de seguridad por Aplicaciones o funciones verticales, sistemas, etc.), incluyendo, cuando sea el caso, a los POC o responsables de seguridad de los sistemas de información externos que suministran servicios a la entidad pública de que se trate.
48. En el supuesto de externalizaciones de servicios, la entidad tercera debe disponer de un Punto de Contacto (POC), sin perjuicio de otras figuras que puedan requerirse por normativa sectorial especifica como la de protección de datos personales. El POC, que puede ser el Responsable de la Seguridad o una persona de su área o departamento o con quien esté en comunicación, tiene entre sus principales funciones se encuentran:
    a. Canalización de las comunicaciones en materia de seguridad e incidentes a la entidad que contrata el servicio.
    b. Supervisión del cumplimiento de los requisitos de seguridad del servicio que presta o solución suministrada.
    c. Gestión de incidentes de seguridad.

6. NIVEL OPERATIVO: EL RESPONSABLE DEL SISTEMA

6.1 EL RESPONSABLE DEL SISTEMA

49. El Responsable del Sistema tiene entre otras funciones:
    a. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
    b. Adopción de las medidas correctoras derivadas de las auditorías de seguridad.
50. El Responsable del Sistema, en los sistemas de categoría Alta, puede suspender el tratamiento de una cierta información o la prestación de un determinado servicio si, en una auditoría, se aprecian deficiencias graves de seguridad. Tras la suspensión, será informada la dirección de la entidad, y los responsables de la información y los servicios afectados y el Responsable de la Seguridad, pudiendo solicitar la opinión del Delegado de Protección de Datos.

51. En la gestión de incidentes de seguridad (ciberincidentes) podrá, de acuerdo con el Responsable de la Seguridad, suspender de forma cautelar y urgente el tratamiento de la información y la prestación de los servicios como medida de contención. Dicha suspensión deberá ser comunicada al Titular de la entidad y a los responsables de la información y del servicio y, en caso de afección a datos personales al Delegado de Protección de Datos y si afecta a la tramitación administrativa, a los servicios jurídicos de la entidad para, en su caso, proceder a la suspensión de los plazos.
52. En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, cada organización podrá designar cuantos **Responsables del Sistema Delegados** considere necesarios. La propuesta de designación corresponde al Responsable del Sistema, que delega funciones, no responsabilidad.
53. Los Responsables del Sistema Delegados se harán cargo, en su ámbito competencial, de todas aquellas acciones delegadas por el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información. Es habitual que estas figuras se encarguen de subsistemas de información de cierta envergadura o de sistemas de información que presten servicios horizontales.
54. Cada Responsable del Sistema Delegado mantendrá una dependencia funcional directa del Responsable del Sistema, a quien reportarán.

6.2 SEGURIDAD FÍSICA

55. Las medidas de protección de las instalaciones físicas pueden clasificarse en: **obstáculos físicos** (accesos físicos, torniquetes, puertas, candados, etc.); **técnicas de vigilancia** (sistemas de alarma, técnicas de vigilancia y monitorización); **sistemas de inteligencia** (herramientas de análisis y simulación de información basados en los datos extraídos de la monitorización); **vigilantes y personal de seguridad**.
56. Como quiera que el ENS contempla preceptos y medidas de seguridad específicos para la seguridad física, las entidades afectadas deberán desarrollar un marco conjunto capaz de dar respuesta a ambas exigencias: físicas y lógicas.
57. Así, el Responsable de la Seguridad Física adoptará las medidas de seguridad que le competan, dentro de las determinadas por el Responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.
58. El Responsable de la Seguridad Física, cuando disponga de la titulación o formación adecuada, podrá realizar las funciones de Responsable de Seguridad y Enlace en aquellas organizaciones que además de estar en el ámbito de aplicación del ENS, se consideren como Infraestructuras Críticas

7. EL ADMINISTRADOR DE SISTEMAS/ SEGURIDAD

59. Atendiendo a la estructura organizativa de la entidad, la entidad podrá contar con un Administrador que, según las funciones que realice, puede depender del Responsable del Sistema o del Responsable de la Seguridad.
60. Las funciones más significativas del Administrador del Sistema serían las siguientes:
    a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
    b. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
    c. La aplicación de los Procedimientos Operativos de Seguridad (POS).
    d. Informar al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
    e. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
61. Son funciones del Administrador dependiente del Responsable de la Seguridad:
    a. Comprobar que los controles de seguridad establecidos son adecuadamente observados.
    b. Comprobar que son aplicados los procedimientos aprobados para manejar el sistema de información.
    c. La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
    d. Comprobar 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.
    e. 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.
    f. Informar al Responsable de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
    g. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
62. Como hemos señalado, puede depender del Responsable del Sistema o del Responsable de la Seguridad (pero no de ambos).
63. En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesite de personal

adicional para llevar a cabo las funciones del Administrador, se podrán designar administradores delegados.

64. Los administradores delegados serán responsables, en su ámbito competencial, de aquellas acciones que delegue el Administrador relacionadas con la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

65. El administrador delegado será designado a solicitud del Administrador, del que dependerá funcionalmente.

8. COMITÉS

66. Como hemos señalado con anterioridad, algunas responsabilidades pueden instrumentalizarse por medio de Comités, que se constituirán como órganos colegiados, de conformidad con lo señalado en la Ley 40/2015 u otra legislación especial que regule a la entidad. Estos Comités, que estarán formados por miembros de todas las partes implicadas, facilitan el desenvolvimiento de la organización y suelen ser habituales en entidades de tamaño mediano o grande.
67. Son habituales los siguientes:

    a. **Comité de Seguridad Corporativa**, que se responsabiliza de alinear todas las actividades de la organización en materia de seguridad, destacándose los aspectos de seguridad física y patrimonial (seguridad de las instalaciones), seguridad de la información, Compliance (seguridad y conformidad legal) y planes de contingencia.

    b. **Comité de Seguridad de la Información**, dependiente del anterior, que se responsabiliza de alinear las actividades de la organización en materia de seguridad de la información.

8.1 COMITÉ DE SEGURIDAD CORPORATIVA

68. La seguridad de la información es una más de las áreas de seguridad de una organización. En organizaciones de tamaño significativo suele existir un **Comité de Seguridad Corporativa** (con su propio Secretario, al que suele denominarse **Responsable de la Seguridad Corporativa -CSO-).** El Responsable de la Seguridad de la Información (CISO) será un miembro de este Comité, junto con otros **responsables de seguridad de otras áreas o departamentos**; Las funciones de este Comité, fundamentalmente, se centran en la coordinación de los diferentes sistemas relacionados con la seguridad en sus distintas vertientes y el cumplimiento normativo especializado relacionada con esta, para evitar disfunciones entre las diferentes Políticas, normas y procedimientos. Cada entidad podrá atribuir las funciones que considere relevantes teniendo en cuenta las que puedan atribuirse al Comité de Seguridad de la Información.

8.2 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

69. La coordinación de la seguridad de la información en las entidades dentro del ámbito de aplicación del ENS es especialmente importante por exigencia de racionalización del gasto y para evitar disfunciones que propicien la aparición de brechas de seguridad provocadas por puntos débiles en los sistemas de información que posibiliten incidentes accidentales o, incluso, ciberataques.
70. El **Comité de Seguridad de la Información,** que coordina la seguridad de la información en la entidad, deberá estar formado por todas aquellas personas de la entidad que participen en la responsabilidad, definición o implantación de la ciberseguridad de la información tratada o los servicios prestados, entre ellos, el Titular de la entidad (o persona delegada, que ostentará la presidencia del Comité), los responsables de la Información, los Servicios, la Seguridad y el Sistema, el Delegado de Protección de Datos y por representantes de otras áreas de la organización afectadas. La composición se determinará en la Política de Seguridad de la Información de la organización.
71. Entre otras funciones el Comité de Seguridad de la Información deberá:
    a. Atender las inquietudes que, en materia de seguridad, se planteen desde la Dirección de la entidad y de los diferentes departamentos.
    b. Informar y ser informado regularmente del estado de la seguridad de la información a la Dirección.
    c. Promover la mejora continua del sistema de gestión de la seguridad de la información, con la aprobación de planes específicos.
    d. Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
    e. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
    f. Controlar periódicamente el grado de cumplimiento de las medidas propuestas para reducir el riesgo residual (pudiendo proponer acciones de mejora) y el correcto funcionamiento del procedimiento de gestión e incidentes, velando por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes
    g. Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección (o por el órgano competente) y aprobar la Normativa de Seguridad de la información
    h. Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo/entidad en materia de seguridad.
    i. Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

j. Velar porque se respete el principio de seguridad desde el diseño, pudiendo requerir el asesoramiento el Responsable de la Seguridad, en todas aquellas iniciativas de la entidad que afecten a la seguridad de la información o de los sistemas. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas en el ámbito de aplicación del ENS.

k. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

72. Puesto que el Comité de Seguridad de la Información no es un comité técnico, podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de decisiones o asesoramiento, realizando formación especializada en la materia. También podrá contar con Grupos de Trabajo especializados, internos, externos o mixtos.

73. Habitualmente, el Responsable de la Seguridad actuará como Secretario del Comité de Seguridad, con las siguientes funciones derivadas:

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

9. GESTIÓN DEL PERSONAL

74. Como quiera que el ENS también contempla preceptos y medidas de seguridad relativas al personal, los responsables de RR.HH. ajustarán sus acciones a lo establecido por el ENS, a la Política de Seguridad de la Información de la entidad, normativas y procedimientos de desarrollo en relación con el personal de dicha entidad.

75. El departamento de RR.HH. de la entidad implementará las medidas de seguridad que le competan, dentro de las determinadas por el Responsable de la Seguridad de la Información, e informarán a éste de su grado de implantación, eficacia e incidentes.

10. CONTRATACIÓN DE SERVICIOS /ADQUISICIONES DE PRODUCTOS

76. En la contratación de prestadores de servicios que incluyen sistemas de información (servicios de seguridad) o en la adquisición de productos de seguridad o servicios de

seguridad de las tecnologías de la información o la comunicación, con carácter previo a la contratación (en la redacción de los pliegos de condiciones técnicas o la solicitud de ofertas), el responsable de compras o contratación de la entidad deberá solicitar asesoramiento al Responsable de la Seguridad sobre los requisitos a solicitar a los licitadores, de conformidad con el artículo 19 del ENS. En caso de que el prestador de servicios contratado realice tratamientos de datos personales por cuenta de la entidad, además, deberá consultarse al Delegado de Protección de Datos.

77. En la contratación del suministro de un derecho de uso de activos[8] en la nube deberá atenderse al contenido de la medida de seguridad "[op.nub] Servicios en la nube" y en las Guía que se desarrollen, siendo relevante, además, que el prestador cuente con un POC debidamente formado cuyo contacto deberá comunicar antes del inicio del contrato.

11. NOMBRAMIENTOS

78. Es función de la Dirección o de otro órgano de la entidad, según la norma sectorial que regula el régimen jurídico de la misma, designar:
    - A los Responsables de la Información, del Servicio, de la Seguridad y del Sistema
    - A los responsables delegados de la Seguridad y del Sistemas, a propuesta de los Responsables titulares correspondientes
    - A los Administradores de la seguridad y del sistema, así como los delgados de estos, a propuesta del Responsable de la Seguridad y del Sistema respectivamente.
79. Los responsables de la Información y/o del Servicio podrán configurarse como un órgano colegiado que será constituido de acuerdo con la normativa reguladora de la entidad., Dicho órgano colegiado podrá ser el propio Comité de Seguridad de la Información en entidades de pequeño tamaño.
80. El procedimiento de nombramiento de los responsables mencionados en el párrafo anterior debe constar en la Política de Seguridad de la Información de la entidad, y debe revestir el carácter de formal, siendo acorde con las normas que regulen la asignación de funciones al personal en la entidad.

12. REPORTES Y FLUJO DE INFORMACIÓN

81. Los números representan las flechas señaladas en el gráfico al final del apartado.

    (1) El Administrador de la seguridad/del sistema, reportará al Responsable del Sistema o al Responsable de la Seguridad, según su dependencia funcional, de los

[8] Según informe 13/2021 de 10 de junio de la Junta Consultiva de Contratación Administrativa sobre la Calificación jurídica de los contratos de prestación de servicios en la nube.

incidentes relativos a la seguridad del sistema y de las acciones de configuración, actualización o corrección.

(2) El Responsable del Sistema reportará al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.

(3) El Responsable del Sistema reportará al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.

(4) El Responsable del Sistema reportará al Responsable de la Seguridad de las actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema y le entregará un resumen consolidado de los incidentes de seguridad.

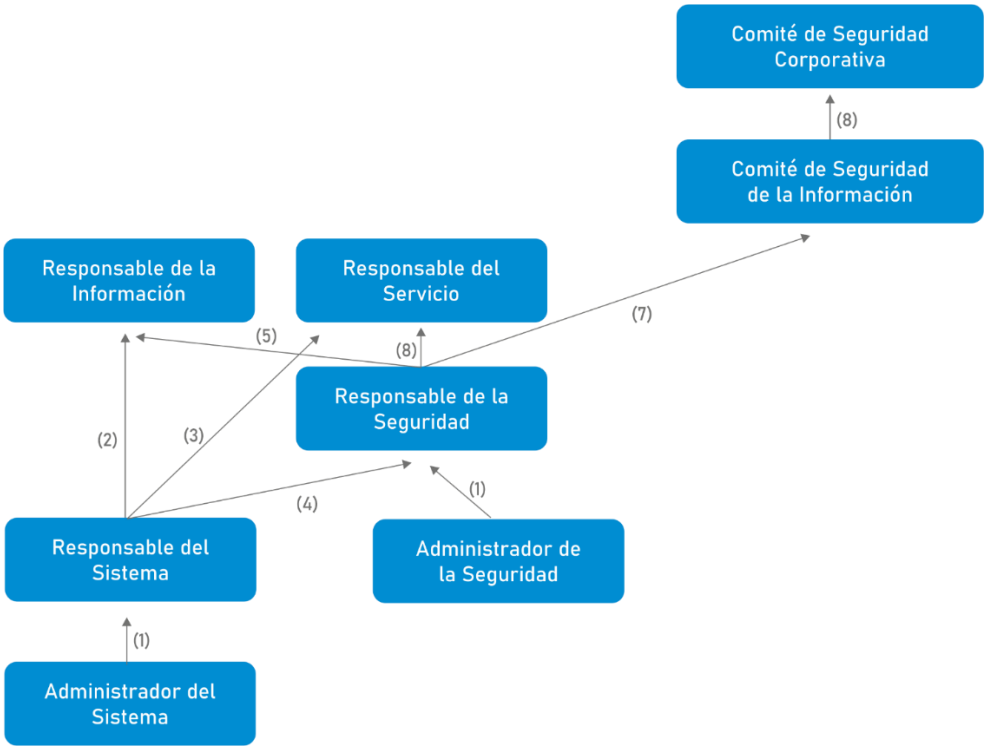
(5) El Responsable de la Seguridad reportará al Responsable de la Información las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

(6) El Responsable de la Seguridad reportará al Responsable del Servicio las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

(7) Cuando exista un Comité de Seguridad de la Información, el Responsable de la Seguridad reportará a dicho Comité, entregando un resumen consolidado de actuaciones en materia de seguridad y de los incidentes relativos a la seguridad de la información, e informándole del estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

(8) Cuando exista un Comité de Seguridad Corporativa, el Responsable de la Seguridad informará a dicho Comité cuando le sea requerido

82. El Responsable de la Seguridad informará a la Dirección de la entidad, a través del Comité, entregándole un resumen consolidado de actuaciones en materia de seguridad y de los incidentes relativos a la seguridad de la información, e informándole del estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.



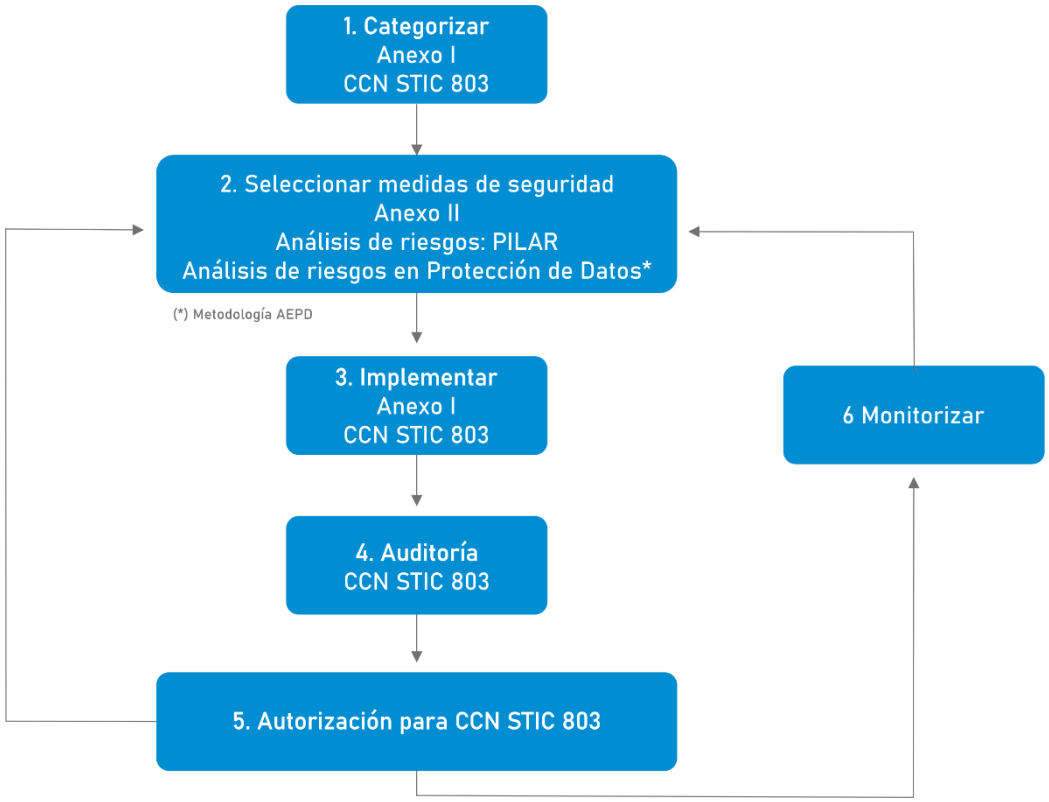
13. GESTIÓN DE LOS RIESGOS

83. La gestión de los riesgos es una tarea que debe realizarse de manera continua sobre los sistemas de información y orientar todas las restantes actividades de acuerdo con los principios de gestión de la seguridad basada en el riesgo y de vigilancia continua y reevaluación periódica.
84. La forma de realizar el análisis de riesgos se detalla en el Anexo II del ENS, medida [op.pl.1] "Análisis de riesgos", estableciendo una proporcionalidad entre el nivel de detalle del análisis y la categoría del sistema de información, con medidas de refuerzo en función de la categorización del sistema.
85. El Responsable de la Información es el propietario de los riesgos sobre la información.
86. El Responsable del Servicio es el propietario de los riesgos sobre los servicios.
87. El propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario[9].
88. Cuando el sistema trate datos personales y se haya realizado un análisis de riesgos en protección de datos personales, conforme con los artículos 24 y 32 del RGPD o por una Evaluación de Impacto del artículo 35 del RGPD, el Responsable de la Seguridad, contando con el asesoramiento del DPD, recogerá las medidas propuestas en el plan

[9] Naturalmente, en última instancia, es el Titular de la entidad pública de que se trate el responsable de aceptar los riesgos residuales o solicitar medidas adicionales de mitigación de tal riesgo residual.

de tratamiento trasladando al Responsable del Sistema aquellas que deban implementarse. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.

89. La responsabilidad de monitorizar un riesgo recae en el Responsable de la Seguridad.
90. Cuando la organización utilice recursos externos (servicios, productos, instalaciones o personal), mantendrá la plena responsabilidad de los riesgos para la información tratada o los servicios prestados, debiendo adoptar las medidas necesarias para ejercer su responsabilidad y mantener el control en todo momento.



Proceso de Gestión de Riesgos

Proceso de Gestión de Riesgos:

91. Paso 1 – **Categorizar la seguridad del sistema de información:**
    a. El Responsable de la Información o el Responsable del Servicio establece los niveles requeridos[10].
    b. El Responsable de la Seguridad determina la categoría del sistema.
92. Paso 2 – **Seleccionar las medidas de seguridad:**

[10] Ver Anexo I del ENS y guía CCN-STIC 803.

a. El Responsable de la Seguridad elabora y aprueba la Declaración de Aplicabilidad, teniendo en cuenta los mínimos requeridos por el Anexo II del ENS y las medidas adicionales o compensatorias que se estimen oportunas.

b. El Responsable de la Seguridad realiza el pertinente análisis de riesgos. Y, cuando se tratan datos personales, comprueba con el Delegado de Protección de Datos las medidas derivadas del análisis de riesgos específico en protección de datos, incorporándolas junto con las de análisis de ENS.

93. Paso 3 – **Implementar las medidas de seguridad:**

a. El Administrador del Sistema se encarga de aplicar las medidas acordadas[11].

94. Paso 4 – **Evaluar y monitorizar la seguridad del sistema de información:**

a. Corresponde al Responsable de la Seguridad pudiendo recurrir a apoyos o auditorías externas cuando sea pertinente[12].

95. Paso 5 – **Autorización para operar:**

a. El Comité de Seguridad de la Información es informado del análisis de riesgos y aprueba el umbral del riesgo residual y el plan de gestión de riesgo propuesto.

b. El Responsable de la Información acepta el riesgo residual sobre la información que le compete.

c. El Responsable del Servicio acepta el riesgo residual sobre los servicios que le competen.

d. Puede ser necesario un Plan de Mejora de la Seguridad para atender a los riesgos que no son aceptables, regresando al paso 2.

96. Paso 6 – **Monitorizar:**

a. El Administrador de la Seguridad recopila información sobre el desempeño del sistema de información en materia de seguridad.

b. El Responsable de la Seguridad monitoriza que el sistema de información se comporta dentro de los márgenes aceptados de riesgo.

c. Los Responsables de la Información y de los Servicios son informados de desviaciones significativas del riesgo sobre los activos de los que son propietarios y, en su caso, el Delegado de Protección de Datos. Si las desviaciones son elevadas, el Responsable del Sistema puede acordar la suspensión temporal del servicio, en caso de ciberincidente de alto impacto o derivado del resultado de una auditoría para sistemas en categoría ALTA hasta que se puedan garantizar niveles aceptables de riesgo debiendo comunicar dicha suspensión al

[11] Ver guía CCN STIC 804. No obstante, algunas de tales medidas podrían salir de su ámbito y ser implementadas por otros.
[12] Ver guía CCN STIC 802.

Responsable de la Seguridad y al Titular de la entidad que será el último responsable de la toma de decisiones, sin perjuicio de otras comunicaciones señaladas en el apartado 12 de esta Guía.

14. OTROS MODELOS DE GOBERNANZA DE SEGURIDAD

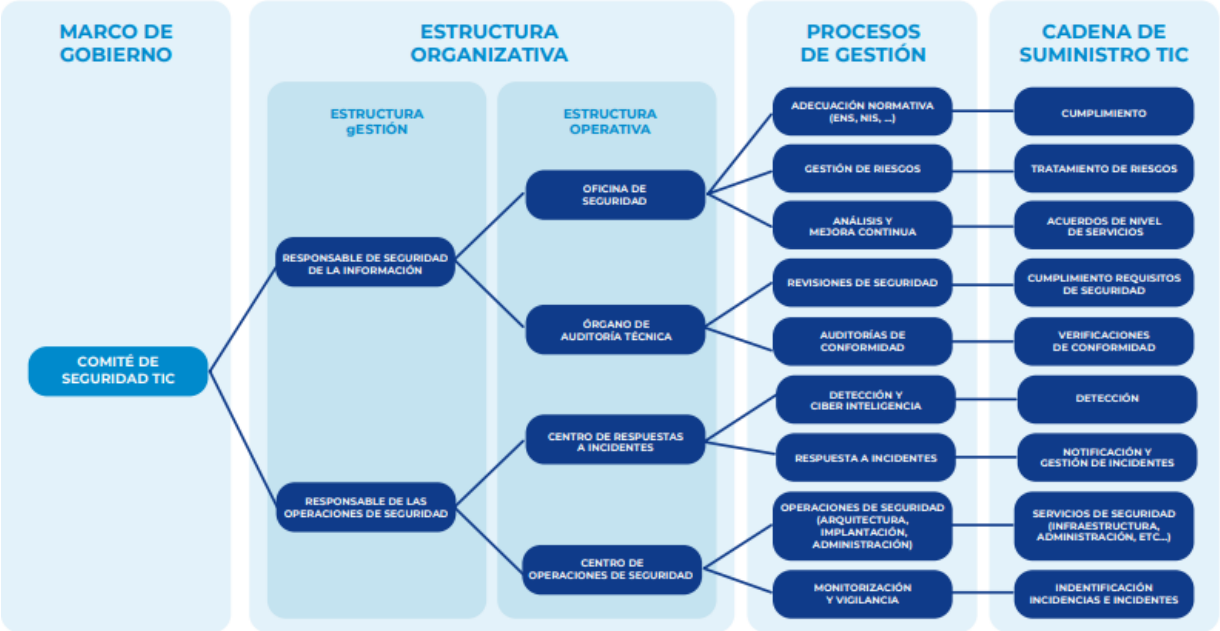
97. Esta Guía recoge un modelo general de responsabilidades en la gobernanza de la seguridad de la información conforme al ENS. Además, de acuerdo con el contenido del artículo 30 del ENS, existen diferentes Perfiles de Cumplimiento Específicos (PCE) para ámbitos determinados donde, partiendo del modelo general, se pueden establecer especialidades en las responsabilidades atendiendo a las características del sector al que aplica el PCE.

14.1 MODELO DE GOBERNANZA EN CIBERSEGURIDAD

98. Por otro lado, aquellas entidades de mayor tamaño o que deseen aplicar un modelo más extendido pueden completar esta estructura básica con otra relacionada con el marco de Gobernanza de la Ciberseguridad que puede disponer también de un modelo básico y uno extendido. El básico está diseñado conforme al siguiente esquema, según se recoge en la guía sobre dichos modelos:

99. El modelo extendido cuenta, además, con otras figuras relevantes para la seguridad de la información en entidades de tamaño medio/alto, donde la responsabilidad

última en materia de seguridad recae en el Comité de Seguridad TIC y que cuenta con dos áreas diferencias el Responsable de la Seguridad de la Información, que a su vez dirige el a Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC y el Órgano de Auditoría Técnica. Por su parte el Responsable de Operaciones de Seguridad que a su vez está al frente del Centro de Operaciones de Seguridad y del Centro de Respuesta a Incidentes. Dicha estructura que se desarrolla en el siguiente esquema de la citada Guía:



14.2 FORO DE SEGURIDAD

100. En aquellas organizaciones que en la gestión de la seguridad de la información se integran otras entidades de menor tamaño (como puede ser el caso de las Diputaciones en relación con los Ayuntamientos de menos de 20.000 habitantes o las Universidades[13]. Este Foro, que deberá constar en la Política de Seguridad de la Información, actuará como un órgano de participación y consulta de las entidades adheridas al modelo de gestión de la seguridad de la información y permitirá recabar sus necesidades en la materia.

101. El Foro, que podrá integrarse en otros de similar naturaleza preexistentes, deberá disponer de un reglamento de funcionamiento y de grupos de trabajo para la participación, consulta, debate y toma de decisiones que serán elevadas al Comité de Seguridad de la Información para su análisis y, en su caso, aprobación.

102. A modo de ejemplo del funcionamiento, se recoge el diseño de la Guía CCN-STIC 881

[13] Véase la Guía 881

15. MODELO GOBERNANZA ENS Y OTRA NORMATIVA

103. Las diferentes entidades sujetas al ENS pueden, en ocasiones, estar dentro del ámbito de aplicación de otras normas, tanto de la UE como estatales, que pueden influir en el modelo de gobierno de la seguridad de la información. Para evitar duplicidades en las figuras, además de las ya descritas en el apartado del Responsable de la Seguridad y el de Seguridad Física, se podrán implementar otras en el modelo de gobierno de la seguridad que, en todo caso, deben respetar la diferenciación de responsabilidades del ENS y sus funciones.

15.1 DIRECTIVA NIS2 Y CER

104. En relación con la normativa con un mayor impacto se encuentra:

- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Si bien la anterior Directiva fue traspuesta a nuestro ordenamiento jurídico por el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

desarrollado en el Real Decreto 43/2021, de 26 de enero, la actual, a fecha de redacción del informe, está pendiente de su trasposición. Además, se deberá tener en cuenta, en función de los sectores involucrados, los Reglamentos de Ejecución de la Directiva NIS2 dictados por la Comisión Europea. En función de la consideración de las entidades dentro el alcance de NIS2 como esenciales o importantes deberán adoptar diferentes medidas, incluyendo aquellas para determinados sectores, por ejemplo, en la comunicación de incidentes de seguridad.

- Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE, actualmente pendiente de transposición. La anterior Directiva se había traspuesto por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, desarrollada por el Real Decreto 704/2011, de 20 de mayo.

15.2 CONCURRENCIA CON EL RGPD

105. Esta sección trata de los puntos de contacto del ENS con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos – RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de derechos digitales, que complementa al RGPD. La relación específica entre la protección de datos personales y el ENS, además de lo recogido en el artículo 3 del ENS, se encuentra en la DA Primera de la LOPDGDD.

106. Las entidades, en función de si tratan datos personales determinando sus fines y medios (artículo 4 del RGPD) o los trata por cuenta de otro, podrán actuar como responsables o encargados del tratamiento, debiendo cumplir con las obligaciones señaladas en la normativa específica.

107. El RGPD y la LOPDGDD identifican las funciones del Delegado de Protección de Datos Personales que además tienen su reflejo en el ENS ya que asesora y supervisa la implementación de las obligaciones de la normativa de protección de datos, colabora con las autoridades de control y, en suma, actúa como garante del derecho a la protección de datos de las personas físicas afectadas por los tratamientos de las entidades.

108. Finalmente, recordar que la figura del DPD puede constituirse a través de un órgano colegiado (adoptando la forma de un Comité Delegado de Protección de Datos), pudiendo contar entre sus miembros con expertos externos -personas físicas o jurídicas-, especializados en seguridad de la información y protección de datos, siempre que quede garantizada la inexistencia de conflicto de intereses entre sus miembros.

109. Aunque la figura del DPD se menciona frecuentemente en la norma, son de especial relevancia los artículos 37 y 39 de la Sección 4 del RGPD Así, el artículo 37 indica que el DPD es un rol externalizable.
110. Por su parte, el artículo 39 delimita sus funciones. Además, se deben tener en cuenta las referencias específicas al Delegado de Protección de Datos y funciones del Capítulo III de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales y las directrices de las autoridades de control en la materia.
111. Por otro lado, el propio ENS en su artículo 3 hace referencia a esta figura.
112. En determinadas circunstancias, no es incompatible que el DPD coincida con el Responsable de la Seguridad del ENS, como se ha mencionado en el epígrafe 3 de la presente Guía.
113. El Delegado de Protección de Datos, como se indica en el ENS y dentro de sus funciones de asesoramiento, debe informar sobre los asuntos relacionados con los datos personales, incluyendo las medidas derivadas del análisis de riesgos en protección de datos o de las evaluaciones de impacto.
114. Por otro lado, el Delegado de Protección de Datos debe ser informado de los incidentes de seguridad que afecten a datos personales para cumplir con las obligaciones de los artículos 33 y 34 del RGPD.
115. El Delegado también formará parte del Comité de Seguridad de la Información cuando se traten asuntos que atañen al tratamiento de los datos personales.

15.3 INTELIGENCIA ARTIFICIAL

116. El Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial, que será aplicable con carácter general el 2 de agosto de 2026, incluye la necesidad de atender a los riesgos en ciberseguridad en el desarrollo y/o despliegue de un sistema de inteligencia artificial (IA) de alto riesgo.
117. Si bien contempla obligaciones específicas para los sistemas de IA de alto riesgo, también recomienda la adopción de medidas para todos los sistemas de IA, así lo indica en el Considerando 165: “El desarrollo de sistemas de IA que no sean sistemas de IA de alto riesgo conforme a los requisitos establecidos en el presente Reglamento puede dar lugar a la adopción más amplia de una IA ética y fiable en la Unión. Se debe alentar a los proveedores de sistemas de IA que no son de alto riesgo a crear códigos de conducta, entre los que se incluyen los correspondientes mecanismos de gobernanza, destinados a impulsar la aplicación voluntaria de la totalidad o parte de los requisitos aplicables a los sistemas de IA de alto riesgo, adaptados teniendo en cuenta la finalidad prevista de los sistemas y el menor riesgo planteado y teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector, como las tarjetas de modelo y de datos Asimismo, se debe animar a los proveedores y, en su caso, a los responsables del despliegue de todos los sistemas de IA, ya sean o no de alto riesgo, y de los modelos de IA, a aplicar, con carácter voluntario, requisitos adicionales relativos, por ejemplo, a los elementos de las Directrices éticas de la Unión para una IA fiable, (...)”.

118. Para aquellas entidades que desarrollen, importen o desplieguen (responsables de despliegue) sistemas de IA en sus organizaciones, en el caso de que deban desarrollar un modelo de gobernanza, podrán integrarlo en el de seguridad de la información, respetando los diferentes roles y funciones en función de las especificidades de cada norma.
119. En todo caso, el Responsable de la Seguridad ENS deberá conocer el sistema de IA, en el caso del responsable del despliegue antes de su implementación en la entidad, para valorar los riesgos de seguridad y realizar las acciones de supervisión que considere necesarias, todo ello, sin perjuicio del debido conocimiento que también deben tener otros roles en desarrollo de sus funciones (Responsable de la Información, del Servicio, del Sistema o Delegado de Protección de Datos).

16. ANEXO A. RESPUESTA A INCIDENTES Y MATRIZ RACI

RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La entidad, de acuerdo con el artículo 25 del ENS, deberá contar con un procedimiento para la gestión de incidentes de acuerdo con la instrucciones técnicas, guías o buenas prácticas publicadas por el CCN-CERT.

La entidad cuando sean operador de servicios esenciales, un proveedor de servicios digitales o se encuentre dentro del ámbito de aplicación de la Directiva NIS2 o de sus reglamentos de ejecución dispondrán también de los requisitos propias estas normas en dicho procedimiento de gestión de incidentes incluyendo las comunicaciones a las diferentes autoridades de control, además de las relacionadas con el cumplimiento de las obligaciones de la normativa de protección de datos personales.

A continuación, se describen pautas generales que, en todo caso deberán ser acordes con las Instrucciones Técnicas o Guías publicadas como la CCN-STIC 817.

- Administrador de Seguridad: Deberá llevar un registro actualizado de las incidencias detectadas, tanto comunicadas internamente dentro de la propia entidad como por terceras contratadas. Los incidentes se tramitarán conforme a lo establecido en la Guía CCN-STIC 817, asignando a cada registro una etiqueta con su clasificación. El incidente será comunicado a:
  - Administrador del Sistema: para que inicie las actividades de resolución y/o contención para evitar su propagación.
  - Responsable de la Seguridad, en todo caso, en los incidentes altos, muy altos o críticos (según la Guía CCN-STIC 817), deberá revisar la clasificación y, en su caso, comunicar al Titular de la entidad la necesidad de comunicar, con carácter inmediato, a las autoridades competentes (CCN-CERT, sin perjuicio de la comunicación a INCIBE en empresas privadas). Además, deberá tenerse en cuenta el impacto en la entidad de las Directiva NIS2 teniendo en cuenta que los incidentes significativos deben ser comunicados al CSIRT de referencia, con los plazos establecidos en otra normativa sectorial, y el intercambio de datos en ciberamenazas, sin perjuicio de las especialidades de las entidades consideradas como críticas.
  - Delegado de Protección de Datos, que tramitará la brecha conforme a la normativa sectorial y los criterios interpretativos de las autoridades de control, dentro del plazo y con los requisitos de la normativa sectorial.
- Administrador del Sistema: Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo, bajo la supervisión del Responsable del Sistema que podrá suspender el sistema, debiendo comunicarlo de forma inmediata al Responsable de la Seguridad, de la Información y del Servicio y al Titular de la entidad

- Administrador del Sistema: Mantener y recuperar la información almacenada por el sistema de información y sus servicios asociados, teniendo en cuenta las indicaciones del Responsable del Sistema.
- Administrador de Seguridad: Investigar el incidente: determinar el modo, los medios, los motivos y el origen del incidente., bajo la supervisión del Responsable de la Seguridad.
- RSEG: Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro, pudiendo solicitar la opinión del Responsable de la Información, del Servicio y del Delegado de Protección de Datos, en su caso. Proponer la comunicación al CCN-CERT al Titular de la entidad y gestionar la misma. En caso de ser una entidad prestadora de servicios, el POC deberá comunicar el incidente de forma inmediata al RSEG de la entidad contratante.
- RSIS: Planificar la implantación de las salvaguardas en el sistema, implementadas por el Administrador del Sistema
- Comité de Seguridad de la Información: Proponer para su aprobación por la Dirección, el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente.
- RSIS: Ejecutar el plan de mejora de la seguridad aprobado.
- RSEG: Supervisar la implementación de dichas medidas, dando cuenta al Comité de Seguridad de la Información sobre el grado de ejecución.

MATRIZ RACI

La matriz RACI que se expone a continuación es orientativa y cada entidad deberá adecuarla a su organización particular.

La matriz de la asignación de responsabilidades (RACI, por las iniciales inglesas de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo). De esta manera, se logra asegurar que cada una de las tareas esté asignada a un individuo o a un equipo.

	Rol	Descripción
A	**Accountable**	**Toma la decisión** (y responde de ello). A veces se dice que **Autoriza** (el trabajo a realizar) y **Aprueba** (el trabajo finalizado y, a partir de ese momento, se hace responsable de él). Sólo puede existir un A por cada tarea. Se trata de la figura que debe asegurar que se ejecutan las tareas.
R	**Responsible**	**Realiza el trabajo** (previamente autorizado por A) y es responsable por su realización. Lo habitual es que exista un solo R. Si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo. Se trata de la figura que debe ejecutar las tareas.
C	**Consulted**	**Se le consulta antes de tomar la decisión**. Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I	**Informed**	**Se le informa de las decisiones tomadas.** Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Tarea	Dirección	RINFO	RSERV	RSEG	RSIS	AS
niveles de seguridad requeridos por la información		A	I	R	C	
niveles de seguridad requeridos por el servicio		I	A	R	C	
determinación de la categoría del sistema		I	I	A	I	
análisis de riesgos	A	I	I	R	C	
declaración de aplicabilidad		I	I	A	C	
medidas de seguridad adicionales		I	I	A	C	
configuración de seguridad		I	I	A	C	R
aceptación del riesgo residual	A	C	C	R	I	
documentación de seguridad				A	C	I
política de seguridad	A	C	C	R	C	
normativa de seguridad		C	C	A	C	I
procedimientos de seguridad		I	I	C	A	I
implantación de las medidas de seguridad		I	I	C	A	R
supervisión de las medidas de seguridad				A	I	R
estado de seguridad del sistema	I	I	I	A	I	R
planes de mejora de la seguridad		I	I	A/R	C	
planes de concienciación y formación		I	I	A	C	
planes de continuidad		I	I	C	A	
suspensión cautelar del servicio	I	I	I	A	R/A	
seguridad en el ciclo de vida				C	A	

Debemos entender la “suspensión cautelar del servicio” como una respuesta ágil ante un problema de seguridad detectado, y de corta duración. Si fuera de larga duración, la aprobación de la suspensión debería recaer en la Dirección de la organización, siendo consultados los RINFO, RSERV y RSEG, y siendo responsable de su ejecución el RSIS.

Algunas tareas carecen de R porque no entra dentro del alcance de esta guía establecer quién se encarga de su realización. No obstante, en cada entidad se deberá determinar quién se encarga de cada tarea o cómo se subdivide hasta poder concretar.