centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 801

Esquema Nacional de Seguridad
Responsabilidades y Funciones



Noviembre 2026

Edita:

centro criptológico nacional

Firmado digitalmente por CCN
Fecha: 2026.11.12 12:52:20 +01'00'

© Centro Criptológico Nacional, 2026

Fecha de Edición: noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN 5
2 OBJETO DE LA GUÍA 6
3 BLOQUES DE RESPONSABILIDAD 11
3.1 NIVEL DE GOBIERNO 12
3.1.1 ÓRGANO DE DIRECCIÓN 12
3.1.2 RESPONSABLE DE LA INFORMACIÓN 15
3.1.3 RESPONSABLE DEL SERVICIO 16
3.1.4 RESPONSABLE FUNCIONAL 16
3.2 NIVEL DE SUPERVISIÓN 17
3.2.1 RESPONSABLE DE LA SEGURIDAD 17
3.2.2 ADMINISTRADOR DE LA SEGURIDAD 19
3.3 NIVEL DE OPERACIÓN 20
3.3.1 RESPONSABLE DEL SISTEMA 20
3.3.2 RESPONSABLE DE PROTECCIÓN FÍSICA 22
3.3.3 ADMINISTRADORES DE SISTEMAS 22
4 RELACIONES CON TERCEROS 23
4.1 ENTIDADES EXTERNAS 23
4.2 PROVEEDORES 24
5 RESOLUCIÓN DE CONFLICTOS 26
6 GESTIÓN DEL PERSONAL 26
7 NOMBRAMIENTOS 27
8 ANEXO A: MARCOS NORMATIVOS A INTEGRAR 28
8.1 PROTECCIÓN DE DATOS PERSONALES 28
8.1.1 BLOQUES DE RESPONSABILIDAD 28
8.1.1.1 GOBIERNO Y DIRECCIÓN 29
8.1.1.2 SUPERVISIÓN 31
8.1.1.3 OPERACIÓN 32
8.1.2 RELACIONES CON TERCEROS 33
8.1.2.1 ÓRGANOS DE CONTROL 33
8.1.2.2 INTERESADOS 33
8.1.2.3 ENCARGADOS DE TRATAMIENTO 33

8.1.3 GESTIÓN DE RIESGOS 35
8.2 INTELIGENCIA ARTIFICIAL.....35
8.2.1 BLOQUES DE RESPONSABILIDAD.....37
8.2.1.1 GOBIERNO Y DIRECCIÓN.....37
8.2.1.2 SUPERVISIÓN 40
8.2.1.3 OPERACIÓN.....42
8.2.2 RELACIONES CON TERCEROS.....43
8.2.2.1 CADENA DE SUMINISTRO 43
8.2.3 GESTIÓN DE RIESGOS 46
9 ANEXO B: MATRIZ RACI ORIENTATIVA Y COORDINACIÓN EN INCIDENTES 49
9.1 GOBIERNO, PLANIFICACIÓN Y GESTIÓN DE RIESGOS 49
9.2 DOCUMENTACIÓN Y OPERACIÓN 50
9.3 COORDINACIÓN EN INCIDENTES.....50

1 INTRODUCCIÓN

Los Sistemas y Tecnologías de la Información y las Comunicaciones (STIC) constituyen un elemento estratégico esencial para las entidades incluidas en el ámbito de aplicación del Esquema Nacional de Seguridad (ENS), al sustentar la prestación de servicios digitales, la gestión de la información y los procesos de toma de decisiones. En un contexto marcado por la rápida evolución tecnológica el valor de dichos activos se incrementa, debido a la creciente interconexión de los sistemas y la incorporación de capacidades emergentes. En consecuencia, resulta imprescindible garantizar su adecuada gestión, protección y gobernanza, asegurando su integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad, así como su alineamiento con los objetivos institucionales y el interés general.

Este contexto tecnológico se desarrolla, además, en un entorno de riesgo crecientemente complejo. La Estrategia de Seguridad Nacional de 2021 ratificó la vulnerabilidad del ciberespacio como uno de los principales riesgos para la seguridad del país, consideración que ha sido nuevamente reflejada en el Informe Anual de Seguridad Nacional 2025, aprobado por el Consejo de Seguridad Nacional el 21 de abril de 2026, que sitúa los riesgos asociados al ciberespacio entre los de mayor intensidad para la Seguridad Nacional. La ampliación de la superficie de exposición, la interdependencia creciente entre sistemas y servicios y la convergencia de actores estatales, criminales, híbridos y oportunistas configuran un panorama de ciberamenazas cada vez más complejo, persistente y transversal.

A ello se añade que la aceleración tecnológica de los últimos años ha precipitado un cambio de escala y de naturaleza en el ámbito de la ciberseguridad. Tecnologías como la inteligencia artificial, la computación cuántica, las redes 5G, el Internet de las Cosas (IoT) o los entornos cloud actúan simultáneamente como motores de innovación y como catalizadores de nuevos vectores, técnicas y modelos de ataque, incrementando la exposición de las organizaciones y exigiendo una respuesta más madura desde el punto de vista organizativo, normativo y operativo.

Por todo ello, la ciberseguridad debe dejar de proyectarse como una cuestión técnica u operativa y pasa a configurarse como una cuestión estratégica, directamente vinculada al gobierno de la entidad, a la continuidad de los servicios, a la protección de los derechos fundamentales de la ciudadanía y a la resiliencia institucional.

Paralelamente, la protección de los sistemas, de la información y de las infraestructuras se desenvuelve en un marco normativo cada vez más cambiante y exigente, caracterizado por la concurrencia de distintas normas europeas y nacionales, tanto de carácter transversal como sectorial, en materias tales como protección de datos personales, inteligencia artificial, resiliencia operativa digital, resiliencia de entidades críticas o información clasificada.

Esta realidad obliga a las entidades a evolucionar desde enfoques parciales o fragmentados hacia modelos integrados de gobernanza, capaces de articular de forma coherente las responsabilidades, funciones, mecanismos de supervisión y relaciones entre los distintos actores implicados.

La Administración pública española cuenta, no obstante, con un grado relevante de madurez en materia de seguridad de la información gracias a la implantación progresiva del ENS, lo que proporciona una base sólida en términos de principios, organización, controles y cultura de seguridad. El ENS constituye, por ello, el eje vertebrador sobre el que debe articularse la adaptación de los modelos de gobernanza a las nuevas exigencias tecnológicas y regulatorias, permitiendo integrar de forma ordenada y coherente los distintos marcos normativos que resulten de aplicación.

Por todo ello, y tomando como base las directrices señaladas en esta guía y las responsabilidades y funciones identificadas por el ENS, cada entidad deberá establecer y aprobar su propio modelo de gobernanza, de acuerdo con su naturaleza, estructura, dimensión, recursos y marco normativo aplicable. Dicho modelo deberá quedar adecuadamente reflejado en la Política de Seguridad de la Información de la entidad, así como, en su caso, en las restantes políticas y disposiciones internas que desarrollen materias específicas relacionadas con la seguridad, la protección de datos, la resiliencia o el cumplimiento normativo.

A tal fin, la presente guía establece las directrices necesarias para facilitar la evolución de los modelos de gobernanza existentes y su adaptación a los requerimientos derivados de las principales normas europeas y nacionales en materia de seguridad de la información, protección de datos personales, inteligencia artificial, ciberseguridad, resiliencia de entidades críticas, resiliencia operativa digital en el sector financiero e información clasificada. Corresponde a cada entidad realizar, con carácter previo, el oportuno análisis de contexto, a fin de determinar qué disposiciones le resultan aplicables, tanto desde una perspectiva general como sectorial.

2 OBJETO DE LA GUÍA

La presente guía tiene por objeto proporcionar, en el marco del Esquema Nacional de Seguridad, un modelo de referencia para la identificación, ordenación y articulación de las responsabilidades y funciones previstas en su artículo 11, estructurándolas en distintos bloques de responsabilidad que permitan su adaptación a modelos de gobernanza acordes con la naturaleza, características y contexto de cada entidad.

La guía parte de la diferenciación entre responsable de la información, responsable del servicio, responsable de la seguridad y responsable del sistema, así como de la exigencia de separar la responsabilidad sobre la seguridad de la correspondiente a la explotación de los sistemas de información. Asimismo, toma en consideración que la política de seguridad de la organización debe detallar las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

La finalidad de la guía no es imponer una estructura organizativa única, sino ofrecer a las entidades un marco común de referencia, suficientemente flexible para que cada una de ellas pueda definir su propio modelo de gobernanza sobre la base del ENS, integrando de forma coherente los distintos marcos normativos que le resulten de aplicación. Se persigue, así, dotar a las entidades de un criterio común para ordenar las funciones de dirección, supervisión y operación de la seguridad, evitar solapamientos o vacíos de

responsabilidad y reforzar la consideración de la ciberseguridad como una función estratégica integrada en el gobierno de la entidad.

A los efectos de la presente guía, el término «entidad» se emplea para referirse, con carácter general, a las entidades del sector público incluidas en el ámbito de aplicación del ENS y, en relación con este, a las comprendidas en el artículo 2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, así como a los prestadores privados a los que resulte de aplicación el artículo 2.3 del ENS.

Se parte de lo dispuesto en el artículo 11 del ENS, que establece lo siguiente:

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.

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.
Responsable del Servicio	ENS, art. 13	El Responsable del Servicio 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. 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 los artículos 11 y 13.3 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, comunicando 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 artículo 13.3 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.

3 BLOQUES DE RESPONSABILIDAD

Existen tres bloques de responsabilidad que delimitan funciones, roles y ámbitos de decisión, permitiendo una gestión clara y coordinada de la seguridad de la información. Estos bloques facilitan la asignación de competencias, la segregación de funciones y la supervisión efectiva, asegurando la alineación con los objetivos organizativos y el cumplimiento normativo. Esta distribución constituye una propuesta organizativa de la presente guía, inspirada en la diferenciación de responsabilidades del ENS, y permite integrar otros marcos normativos sin alterar las atribuciones jurídicas que correspondan a cada responsable.

Esta sistematización tiene por finalidad facilitar una comprensión ordenada del modelo, delimitar con claridad los ámbitos de decisión, supervisión y ejecución, y permitir a cada entidad adaptar su organización interna de acuerdo con su naturaleza, estructura y contexto, sin perjuicio de la necesaria diferenciación de responsabilidades y de la adecuada coordinación entre los distintos bloques.

a. **Gobierno**: El ámbito de Gobierno comprende la responsabilidad última sobre la seguridad, así como la definición de necesidades, criterios, prioridades y requisitos en materia de seguridad. Corresponde al Titular de la entidad u órgano de dirección, así como a los responsables de la información y del servicio, en el ámbito de sus respectivas competencias.

   Asimismo, corresponde a este ámbito aprobar las medidas que procedan, asignar prioridades y recursos, y asegurar la existencia de mecanismos de rendición de cuentas, seguimiento y control que permitan conocer el grado de cumplimiento y la eficacia de las medidas adoptadas.

   El artículo 11 del ENS exige que la política de seguridad detalle las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

b. **Operación**: Comprende la gestión, explotación y administración de los sistemas de información, así como garantizar la implantación efectiva de las medidas de seguridad que deban materializarse sobre dichos sistemas. Estas funciones corresponden al Responsable del Sistema, a los administradores de sistemas y, en su caso, a las restantes figuras de carácter operativo que se encuadren en este bloque (incluidos proveedores de IT).

   En este bloque podrá integrarse asimismo la función de protección física, cuando le corresponda implantar medidas físicas vinculadas a la protección de sistemas, instalaciones o activos de soporte.

   Su cometido es garantizar la correcta implantación, mantenimiento y funcionamiento de las medidas aplicables sobre los sistemas, sin asumir por ello funciones de supervisión independiente de la seguridad. El artículo 11 del ENS

exige que la responsabilidad sobre la seguridad esté diferenciada de la responsabilidad sobre la explotación de los sistemas de información.

c. **Supervisión:** Comprende las funciones de asesoramiento, propuesta, impulso, control, monitorización y supervisión en materia de seguridad de la información. Este ámbito corresponde, en lo que respecta al ENS, al Responsable de la Seguridad, a los Administradores de Seguridad y a las capacidades técnicas que actúen funcionalmente bajo la dirección de la seguridad de la información, incluidos, en su caso, los Centros de Operaciones de Seguridad (SOC).

   La utilización de capacidades técnicas de monitorización, detección, análisis o respuesta inicial no altera la naturaleza de estas funciones cuando su cometido principal sea la supervisión de la seguridad y no la operación del sistema. Por ello, el SOC no debe entenderse como una extensión funcional del Responsable del Sistema, sino como una capacidad técnica de la función de seguridad orientada a la vigilancia continua, la alerta temprana, el análisis y el apoyo a la respuesta desde la perspectiva de la seguridad.

La siguiente figura muestra los tres bloques de responsabilidad y las figuras más relevantes asociadas al cumplimiento del ENS:



3.1 NIVEL DE GOBIERNO

3.1.1 Órgano de dirección

El órgano de dirección de una entidad debe ser considerado como aquel que tiene la capacidad de fijar la estrategia, los objetivos y la orientación general de la entidad, y que se ocupa de la vigilancia y control del proceso de adopción de decisiones de dirección, todo ello conforme a las competencias que tenga legalmente atribuidas.

A estos efectos, deberá acudirse a la normativa sectorial aplicable para determinar qué órgano ostenta dicha condición en cada caso. Con carácter orientativo, y en relación con los distintos tipos de entidades del sector público definidos en el artículo 2 de la Ley

40/2015, podrán servir de orientación las figuras de la tabla siguiente, sin perjuicio de la normativa sectorial, los estatutos y el reparto efectivo de competencias, que prevalecen en cada entidad:

Entidad	**Órgano de dirección**
La Administración General del Estado	Titular del Ministerio
Las Administraciones de las CCAA	Titular de la Consejería
Las entidades de la Administración Local	Órgano competente conforme a la Ley 7/1985, la legislación de régimen local y la organización de la entidad (alcaldía/presidencia, pleno o junta de gobierno, según la atribución)
Diputaciones y provincias	Presidente/a
Sector público institucional	Órgano previsto estatutos o norma
Universidades	Consejo de Gobierno

Así pues, el Órgano de dirección adquiere una relevancia esencial, en tanto que de él depende el grado de compromiso de la organización con la seguridad de la información y su adecuada implantación, gestión y mantenimiento.

En consecuencia, la seguridad de los sistemas de información no se concibe como una cuestión meramente técnica, sino como un elemento estratégico integrado en el ámbito del gobierno y la dirección. El órgano de dirección deberá asumir la aprobación de la estrategia de seguridad y de las medidas correspondientes, así como la supervisión y el control, de forma independiente a los órganos responsables de la operación y ejecución.

En este punto, cobra especial relevancia en el ámbito de la toma de decisiones del Órgano de dirección, el Responsable de la Seguridad, con quien ésta deberá mantener una comunicación directa y permanente y que será el responsable de elaborar y proponer al Órgano de dirección la estrategia de seguridad de la entidad, su política de seguridad y las medidas correspondientes para la gestión de riesgos de ciberseguridad, técnicas y organizativas.

Dichas medidas deberán disponer de la correspondiente dotación presupuestaria que garantice su efectiva implementación y el desarrollo de las funciones del Responsable de la Seguridad.

Los miembros de los órganos de dirección deberán recibir formación adecuada de forma periódica al objeto de adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad.

El Órgano de dirección además deberá garantizar en relación con los responsables identificados en el art. 11 del ENS que se cumpla con los siguientes requisitos:

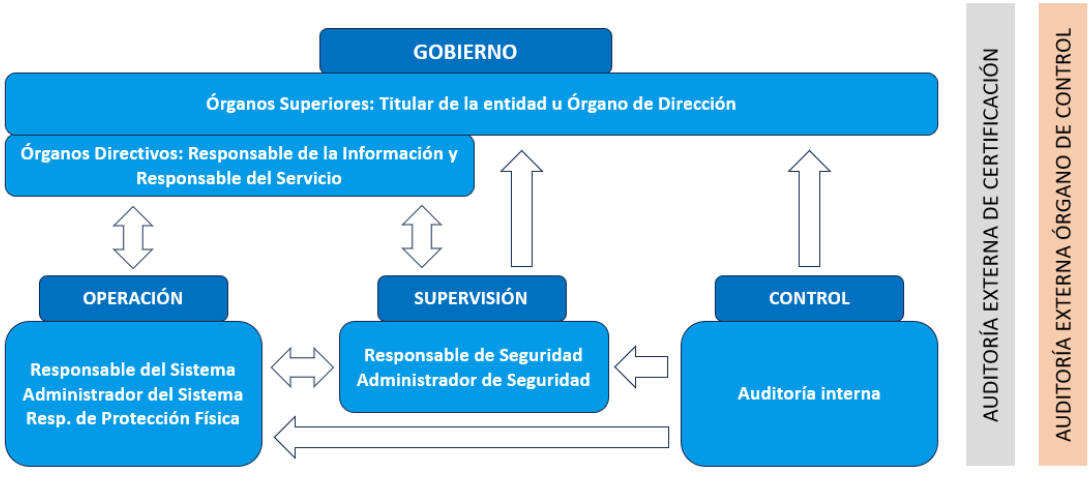
a. Contar con personal con conocimientos especializados y experiencia en materia de ciberseguridad, desde los puntos de vista jurídico, organizativo y técnico, adecuados al desempeño de sus funciones.
b. Contar con los recursos necesarios para el desarrollo de sus funciones.
c. Ostentar una posición en la organización que facilite el desarrollo de sus funciones, participando de forma adecuada y en todas las cuestiones relativas a la seguridad.
d. Mantener la debida independencia entre los distintos responsables.

Con el fin de dar pleno cumplimiento a las funciones de control y responsabilidad inherentes al órgano de dirección, y teniendo en cuenta los artículos 9 (Existencia de líneas de defensa), 10 (Vigilancia continua y reevaluación periódica) y 31 (Auditoría de la seguridad) del ENS, se recomienda la realización de auditorías que reporten directamente al órgano de dirección; y que, cuando desarrollen funciones de control independiente, deberán ser independientes de los bloques de operación y supervisión.

Se propone así el concepto de control independiente dirigido a proporcionar al bloque de gobierno, como máximo responsable de la seguridad de la información de la entidad, una visión objetiva sobre el grado de adecuación, cumplimiento y eficacia del modelo de seguridad y de las medidas aprobadas.

Esta función podría articularse mediante un equipo de auditoría interna o, en su caso, a través de auditorías realizadas por terceros, siempre que se garantice su independencia respecto al bloque de operación y al de supervisión. Su finalidad no es solamente certificar la adecuación de la entidad al ENS, sino evaluar, con carácter independiente, si el modelo diseñado, implantado y supervisado por las restantes líneas resulta adecuado y eficaz, reportando directamente al órgano de dirección.

Como recomendación de gobernanza, distinta de las líneas de defensa técnicas, organizativas y físicas contempladas en el artículo 9 del ENS, la entidad podría configurar un modelo de tres líneas de funciones. En este modelo de gobernanza, la primera línea garantiza la implantación de las medidas de seguridad en los sistemas; la segunda línea supervisa la seguridad y mantiene la vigilancia continua sobre su adecuación; y la tercera línea verifica, de forma independiente, el grado de cumplimiento y la eficacia del conjunto de las medidas.



Este modelo permite ordenar las relaciones entre gobierno, operación y supervisión, reforzar la diferenciación de responsabilidades exigida por el ENS, evitar solapamientos o vacíos funcionales y facilitar la integración coherente de los distintos marcos normativos que resulten de aplicación a cada entidad.

A su vez, es posible —y habitual, en organizaciones de tamaño significativo— la existencia de ciertos órganos o comités para la gestión y coordinación de la seguridad en la entidad (art. 12.1.d) del ENS), ya sea física, de la información, de protección de datos, o todas ellas. Si bien estos órganos o comités deben ser de apoyo a los distintos bloques de responsabilidad, no podrán sustituir las competencias y responsabilidades que legalmente tiene atribuidas los distintos responsables.

Los comités más habituales son:

- Comité de Seguridad Corporativa
- Comité de Seguridad de la Información.

En caso de resultar de aplicación marcos normativos adicionales podrán constituirse comités específicos adicionales o integrar el contenido en comités ya existentes en la organización. Se recomienda, en la medida de lo posible, aprovechar las estructuras organizativas ya existentes, como comités ejecutivos o grupos de trabajo, para canalizar las funciones de gobernanza de seguridad, evitando la creación de nuevos órganos y favoreciendo la eficiencia, la coordinación y la integración en la dinámica operativa de la organización.

Por último, cuando la entidad recurra a terceros para la prestación de servicios, para la provisión de soluciones tecnológicas o para la realización de actividades que afecten a la seguridad de la información, el modelo de gobernanza deberá extenderse a dichas relaciones externas, definiendo los puntos de interlocución, las obligaciones de seguridad y los mecanismos de supervisión y control que resulten necesarios; de acuerdo con lo dispuesto en 4 RELACIONES CON TERCEROS de la presente Guía.

El modelo de gobernanza deberá revisarse periódicamente y cuando se produzcan cambios relevantes en la organización, en los sistemas de información, en el entorno regulatorio o en el perfil de riesgos.

3.1.2 Responsable de la Información

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

El Responsable de la Información será un puesto situado en el nivel Directivo de la organización dentro del bloque de gobierno. Esta figura tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

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; atendiendo a lo dispuesto en el art. 40 y 41 del ENS.

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.

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.

3.1.3 Responsable del Servicio

El Responsable del Servicio será un puesto situado en el nivel Directivo de la organización dentro del bloque de gobierno. Su función principal será 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; atendiendo a lo dispuesto en el art. 40 y 41 del ENS.

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.

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.

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.

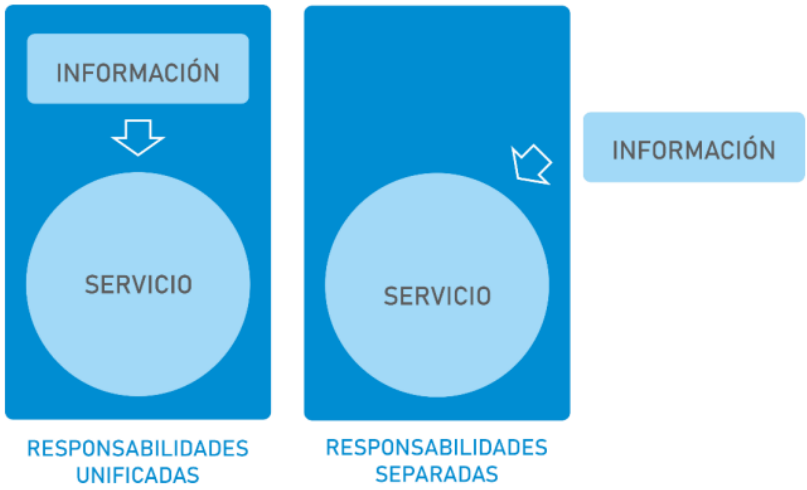
3.1.4 Responsable Funcional

Es posible que en una misma persona concurran las responsabilidades de la información y del servicio, pudiendo denominar esta figura como Responsable Funcional.

La diferenciación orgánica entre Responsable de Información y Responsable de Servicio tiene especial sentido cuando:

- El servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental o área que presta dicho servicio.

- La prestación del servicio no depende de la unidad o área que gestiona la información.



Responsabilidades unificadas y separadas

3.2 NIVEL DE SUPERVISIÓN

El entorno de seguridad de la información es cada vez más complejo y dinámico, lo que, en determinados contextos, hace necesario que el Responsable de Seguridad (RSEG) disponga de una estructura organizativa de apoyo, ya sea con recursos internos o mediante capacidades externas especializadas.

A estos efectos, y desde un punto de vista funcional, pueden tomarse como referencia los servicios gestionados descritos en la guía CCN-STIC 896, adaptándolos a las necesidades y madurez de la organización.

3.2.1 Responsable de la Seguridad

El ENS señala que, entre sus principales funciones, el Responsable de la Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios y supervisará la implantación de dichas medidas para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

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).

Las funciones esenciales del Responsable de la Seguridad, sin perjuicio de otras que la organización pueda encomendarle, son:

a. 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.

b. Proponer la valoración de información y servicios.
c. Determinar la categoría del sistema, de conformidad con el artículo 41 del ENS, y seleccionar las medidas de seguridad aplicables, en función de las valoraciones hechas por los Responsables de la Información y los Servicios.
d. Formalizar y firmar la Declaración de Aplicabilidad con las medidas del anexo II seleccionadas, conforme al artículo 28.2 del ENS. Cuando se utilicen medidas compensatorias, documentar la correspondencia con las medidas sustituidas y aprobar formalmente el conjunto, de acuerdo con el artículo 28.3 del ENS. La Dirección adoptará las decisiones organizativas y presupuestarias que le competan, sin sustituir la firma y aprobación formal atribuidas al Responsable de la Seguridad.
e. Supervisar y comprobar que las medidas de seguridad de la información han sido adecuadamente implementadas por el Responsable del Sistema; reportando a la Dirección sobre estas cuestiones.
f. Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, en lo relativo a aspectos tanto físicos como lógicos.
g. Supervisar los requisitos de seguridad de los servicios recibidos y de las soluciones suministradas por terceros, así como la coordinación y los intercambios de información sobre seguridad e incidentes, sin perjuicio de las funciones del punto de contacto que corresponde designar a la organización prestataria conforme al artículo 13.5 del ENS.
h. Aprobación explícita de los cambios que impliquen un riesgo de nivel ALTO con carácter previo a su implantación.
i. Análisis de los informes de Auditoría a los que hace referencia el art. 31 del ENS, que se refieran a los sistemas de su ámbito competencial, y presentación de sus conclusiones al Responsable de Sistema y, en su caso, al Comité de Seguridad de la Información.
j. Dirigir funcionalmente la gestión de los ciberincidentes en su ámbito, con arreglo a los procedimientos aprobados y a las orientaciones de la Guía CCN-STIC 817. La obligación de notificar los incidentes de impacto significativo que corresponde a las entidades del sector público deriva del artículo 33.2 del ENS y de la Instrucción Técnica de Seguridad aplicable; la Política de Seguridad podrá determinar qué cargo o unidad efectuará materialmente esa notificación al CCN. Los prestadores privados se atendrán al régimen de notificación previsto en el artículo 33.7 del ENS, sin perjuicio de otros deberes sectoriales y contractuales de comunicación.
k. Recibir, interpretar y supervisar la aplicación de las instrucciones y guías emanadas de la autoridad de control, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
l. Velar por el cumplimiento de empresas externas y proveedores de los criterios de seguridad de la información establecidos por la entidad.
m. Elevar al Comité de Seguridad (si existe) y/o a los Responsables de la Información y de los Servicios los riesgos críticos o incumplimientos significativos que no hayan podido ser mitigados o aceptados en el nivel correspondiente.

El Órgano de dirección además deberá garantizar que el Responsable de la Seguridad cumpla con los siguientes requisitos:

a. Contar con personal con conocimientos especializados y experiencia en materia de ciberseguridad, desde los puntos de vista jurídico, organizativo y técnico, adecuados al desempeño de sus funciones.
b. Contar con los recursos necesarios para el desarrollo de sus funciones.
c. Ostentar una posición en la organización que facilite el desarrollo de sus funciones, participando de forma adecuada y en todas las cuestiones relativas a la seguridad, y manteniendo una comunicación real y efectiva con el Órgano de dirección.
d. Mantener la debida independencia respecto de los responsables de las redes y los sistemas de información.

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 responsabilidades.

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.

Cada Responsable de la Seguridad Delegado mantendrá una dependencia funcional directa del Responsable de la Seguridad, a quien reportará.

3.2.2 Administrador de la seguridad

Atendiendo a la estructura organizativa de la entidad, la entidad podrá contar con un Administrador que, según las funciones que realice, podrá depender del Responsable de la Seguridad.

Conviene precisar que las figuras del Administrador de Seguridad, en el marco del Esquema Nacional de Seguridad, pueden desempeñar funciones de supervisión o tareas técnicas de ejecución, según su configuración y adscripción organizativa. Las funciones operativas y las de supervisión independiente deben diferenciarse expresamente.

En este sentido, la adscripción del administrador no elimina la necesidad de documentar quién autoriza, quién ejecuta y quién supervisa cada actuación, en coherencia con los artículos 11 y 13.3 del ENS. Todo ello sin perjuicio de que, en organizaciones de menor tamaño, ambos planos —responsabilidad y ejecución— puedan coincidir en una misma persona.

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. Supervisar, sin asumir necesariamente su ejecución material, 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.

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.

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.

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

3.3 NIVEL DE OPERACIÓN

3.3.1 Responsable del Sistema

El Responsable del Sistema es la figura encargada de garantizar el adecuado funcionamiento y explotación de los sistemas de información, entre otras funciones debe:

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. Garantizar la correcta implantación de las medidas de seguridad propuestas por el Responsable de la Seguridad y aprobadas por la Dirección.
c. Adopción de las medidas correctoras derivadas de las auditorías de seguridad.
d. Velar por la existencia y mantenimiento de un inventario actualizado de sistemas, servicios, aplicaciones, infraestructuras y activos bajo su responsabilidad.

Desde el punto de vista jerárquico, deberá situarse en un nivel organizativo que le permita ejercer sus funciones con autoridad suficiente sobre la explotación de los sistemas y coordinarse eficazmente con el Responsable de Seguridad y el resto de los roles implicados en la gobernanza de la seguridad de la información.

El Responsable del Sistema deberá contar con los recursos técnicos y humanos necesarios para garantizar la operación, mantenimiento y seguridad de los sistemas bajo su responsabilidad, pudiendo apoyarse en equipos especializados internos o servicios externos cuando la complejidad lo requiera.

El Responsable del Sistema 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 o exista algún tipo de dependencia jerárquica, se implementarán medidas compensatorias como señala el art. 13.3 del ENS.

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.

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, así como a los servicios jurídicos de la entidad para, en su caso, proceder a la suspensión de los plazos.

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.

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.

Cada Responsable del Sistema Delegado mantendrá una dependencia funcional directa del Responsable del Sistema, a quien reportarán.

3.3.2 Responsable de Protección Física

Las medidas de seguridad físicas pueden clasificarse en medidas de protección perimetral (control del acceso a las instalaciones), control de accesos físicos (identificación, autenticación y registro de personas), protección de instalaciones y equipos (sistemas antiintrusión, videovigilancia o ubicación segura) y medidas ambientales y de continuidad (energía, climatización o protección frente a incendios). Asimismo, se incluyen las relativas al personal de seguridad, responsable de la vigilancia, control y respuesta ante incidentes, actuando como elemento activo en la aplicación y supervisión de estas medidas. Tal y como recoge el ENS, la seguridad del Sistema deberá tener un planteamiento integral, por lo que las entidades afectadas deberán desarrollar un marco conjunto capaz de dar respuesta a ambas exigencias: físicas y lógicas.

Así, el Responsable de la Protección 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.

3.3.3 Administradores de sistemas

Atendiendo a la estructura organizativa de la entidad, la entidad podrá contar con un Administrador que, según las funciones que realice, dependerá del Responsable del Sistema.

Conviene precisar que las figuras del Administrador del Sistema, en el marco del Esquema Nacional de Seguridad, deben entenderse principalmente como un rol de responsabilidad y gestión, y no necesariamente como funciones de ejecución técnica directa.

En este sentido, no se exige que dichas funciones recaigan en la persona que realiza materialmente las tareas operativas, sino en quien asume la responsabilidad de que dichas actuaciones se planifiquen, ejecuten correctamente y se ajusten a la política de seguridad establecida. Todo ello sin perjuicio de que, en organizaciones de menor tamaño, ambos planos —responsabilidad y ejecución— puedan coincidir en una misma persona.

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.

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.

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.

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

4 RELACIONES CON TERCEROS

En el ámbito de la seguridad de la información, se observa un incremento constante de las obligaciones de interacción con terceros externos a la organización, derivado tanto de la creciente exigencia regulatoria como de la dependencia de servicios y soluciones prestadas por proveedores. Estas relaciones implican la necesidad de establecer mecanismos formales de coordinación, supervisión y control que garanticen el cumplimiento normativo, la adecuada gestión de riesgos y la protección de la información compartida, abarcando desde la comunicación con órganos reguladores hasta la gestión de contratos, acuerdos de nivel de servicio y medidas de seguridad aplicables a terceros.

El modelo de gobernanza de la entidad debe contemplar expresamente la relación con dichos terceros, asegurando que las responsabilidades, canales de comunicación y mecanismos de control queden definidos de forma clara y coherente con el marco organizativo interno. Esto deberá ser trasladado a la Política de Seguridad de Información de la entidad.

La entidad debe realizar un análisis sistemático de su contexto organizativo, normativo y operativo con el fin de identificar las entidades externas a las que está obligada a reportar información en materia de seguridad de la información. Este análisis debe considerar tanto a los órganos reguladores y de supervisión, organismos de coordinación y respuesta, proveedores, usuarios de los servicios públicos, otras administraciones públicas (interoperabilidad, convenios, cesiones de datos), auditores y entidades certificadoras, Fuerzas y Cuerpos de Seguridad del Estado, autoridades judiciales y colaboradores. Esto permite definir de forma clara los canales de comunicación, las obligaciones de reporte y los requisitos aplicables, asegurando así el cumplimiento normativo y la adecuada gestión de la seguridad.

4.1 ENTIDADES EXTERNAS

La entidad debe cumplir las obligaciones de notificación previstas en el artículo 33 del ENS y en las restantes normas aplicables. En particular, las entidades del sector público notificarán al CCN los incidentes con impacto significativo en la seguridad de los sistemas de información, conforme a la Instrucción Técnica de Seguridad correspondiente

(artículo 33.2 del ENS). Las organizaciones privadas que presten servicios a entidades públicas se atendrán al régimen del artículo 33.7, sin perjuicio de las comunicaciones debidas a la entidad destinataria y de otras obligaciones sectoriales. Asimismo, las entidades sujetas al artículo 32 del ENS participarán en los mecanismos de recogida de información sobre el estado de la seguridad en los términos allí establecidos.

En ambos casos recae sobre el Responsable de Seguridad de la entidad la función de proponer el establecimiento de los canales internos oportunos para reportar dicha información en tiempo y forma.

En caso de otras administraciones públicas a las que la entidad pueda prestar servicios o existan intercambios de información, el Responsable de Seguridad deberá establecer un POC para canalizar adecuadamente aquellos aspectos relativos a seguridad de la información. Esta figura podrá ser asumida por el Responsable de la Seguridad, por una persona integrada en su área o departamento de seguridad, o por cualquier otra persona expresamente designada a tal efecto, sin perjuicio de las figuras adicionales que deban existir conforme a la normativa sectorial aplicable.

4.2 PROVEEDORES

Para la contratación de servicios y/o productos TIC y de seguridad, el modelo de gobernanza de la entidad deberá contemplar la exigencia contractual, cuando corresponda que el tercero prestador disponga de un punto de contacto en materia de seguridad que actúe como interlocutor ordinario con la entidad. En los supuestos sujetos al artículo 13.5 del ENS, salvo causa justificada y documentada, el punto o persona de contacto (POC) deberá ser el Responsable de la Seguridad de la organización prestataria, formar parte de su área o mantener comunicación directa con ella y disponer del apoyo de sus órganos de dirección. Todo ello sin perjuicio de las funciones adicionales exigibles por la normativa sectorial y de protección de datos.

El punto de contacto en materia de seguridad tendrá, al menos, las siguientes funciones:

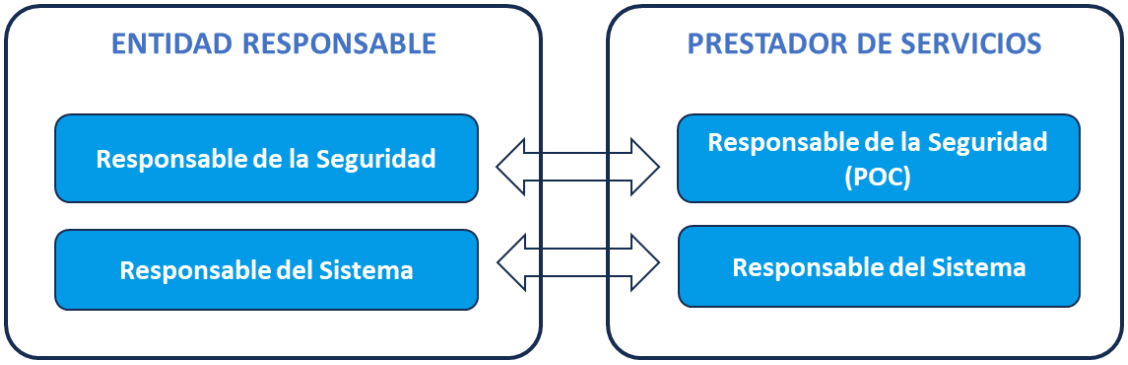
a. Canalizar las comunicaciones entre el tercero y la entidad en todas las cuestiones relacionadas con la seguridad del servicio prestado o de la solución suministrada.
b. Coordinar y efectuar el seguimiento del cumplimiento de los requisitos de seguridad exigibles al servicio externalizado, facilitando a la entidad la información necesaria para el ejercicio de sus funciones de supervisión y control.
c. Coordinar la comunicación, escalado y gestión de los incidentes de seguridad que afecten al servicio o a los sistemas implicados, de acuerdo con los procedimientos, compromisos y niveles de servicio que resulten de aplicación

En la contratación de servicios de seguridad o en la adquisición de productos de seguridad de las tecnologías de la información o la comunicación, con carácter previo a la contratación (durante la preparación de los pliegos o la solicitud de ofertas), se recomienda que el responsable de compras o contratación solicite asesoramiento al Responsable de la Seguridad sobre los requisitos técnicos y organizativos que deban exigirse. Esta intervención constituye una buena práctica de gobernanza y no un mandato literal del artículo 19 del ENS, cuyo contenido material sobre certificación de funciones de seguridad y contratación deberá cumplirse cuando resulte aplicable.

Así mismo, el Responsable de Seguridad conviene también que sea consultado sobre los requisitos a incluir en el proceso de contratación para valorar el cumplimiento del ENS de los sistemas de información de las entidades del sector privado que presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

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

La figura que acompaña este epígrafe representa un esquema conceptual de referencia de la estructura de seguridad de la información en la relación entre la entidad y el tercero prestador de servicios. Su finalidad es ofrecer una visión global de las principales figuras que pueden intervenir, diferenciando entre los roles propios de la entidad y aquellos otros que pueden ubicarse en organizaciones externas.



Dicho esquema no establece por sí mismo una adscripción orgánica concreta, ni define relaciones jerárquicas o funcionales cerradas entre las figuras representadas. La articulación de estas deberá realizarse conforme al modelo de gobierno, gestión y control adoptado por cada entidad, atendiendo, en todo caso, a los principios de segregación de funciones, responsabilidad diferenciada, supervisión y trazabilidad de decisiones. En este sentido, la figura debe interpretarse como un marco de referencia orientado a facilitar la comprensión e integración de los distintos roles en escenarios en los que intervienen terceros.

En todo caso, la intervención de terceros no desplaza la responsabilidad de la entidad sobre el gobierno, supervisión y control de la seguridad en relación con los servicios que recibe o con la información que gestiona. El Responsable de la Seguridad de la entidad deberá mantener una posición organizativa que permita el adecuado ejercicio de sus funciones, participando en todas las cuestiones relevantes de seguridad y manteniendo una comunicación real y efectiva con el Titular de la entidad u órgano de dirección.

Conforme al modelo de gobernanza adoptado por la entidad al amparo del ENS, corresponderá al Responsable de la Seguridad identificar riesgos, proponer las medidas que resulten necesarias, supervisar su implantación y reportar sobre el estado de la seguridad, incluyendo, cuando proceda, los aspectos que afecten a servicios prestados por terceros.

Las medidas de seguridad que deban aplicarse en servicios externalizados o soluciones suministradas por terceros deberán incorporarse a los correspondientes instrumentos jurídicos o contractuales, de forma compatible con la política de seguridad de la entidad y con los requisitos que resulten exigibles conforme al ENS.

Cuando el tercero preste servicios que impliquen la operación, administración o soporte técnico de sistemas de información de la entidad, el reparto de funciones entre la entidad y el prestador deberá quedar expresamente definido. En particular, el instrumento jurídico correspondiente deberá precisar qué funciones corresponden al tercero respecto de la administración técnica, operación o mantenimiento de los sistemas implicados, sin perjuicio de que la entidad conserve en todo caso sus funciones de dirección, supervisión y control conforme a su propio modelo de gobernanza.

5 RESOLUCIÓN DE CONFLICTOS

La diferenciación de funciones entre los distintos responsables no presupone la existencia de conflictos entre ellos, sino una distribución ordenada de competencias conforme al Esquema Nacional de Seguridad. En este modelo, el Responsable de la Seguridad y el Responsable del Sistema ejercen funciones distintas, complementarias e independientes, orientadas respectivamente a la determinación y supervisión de las medidas de seguridad, y a la operación y mantenimiento del sistema.

Del mismo modo, la distribución de funciones entre la Dirección, los Responsables de la Información y del Servicio y, en su caso, los restantes responsables, delegados, administradores u órganos de apoyo, debe entenderse como un sistema ordenado de atribución de competencias, en el que cada figura interviene dentro de su respectivo ámbito funcional.

La concurrencia de distintos roles en la definición de necesidades, en la propuesta de medidas, en la supervisión de su implantación o en la operación de los sistemas no implica una situación de conflicto, sino la necesidad de una adecuada coordinación conforme al modelo de gobernanza establecido por la entidad.

Cuando en la aplicación de dichas funciones puedan surgir discrepancias de carácter técnico, operativo u organizativo, estas deberán canalizarse mediante los mecanismos internos de coordinación y, en su caso, elevarse al órgano de dirección competente, al que corresponde la adopción de las decisiones que procedan. El mecanismo concreto de resolución de controversias debe figurar en la Política de Seguridad de la Información de la organización.

6 GESTIÓN DEL PERSONAL

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.

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.

De conformidad con lo dispuesto en el art. 15, el personal relacionado con los sistemas de información deberá ser formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad.

Los programas de formación y concienciación deberán adaptarse a las responsabilidades y funciones de cada puesto de trabajo, prestando especial atención a los responsables definidos en el artículo 11 del ENS.

7 NOMBRAMIENTOS

Es función del Titular de la entidad o del órgano de dirección, 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.

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.

8 ANEXO A: MARCOS NORMATIVOS A INTEGRAR

8.1 PROTECCIÓN DE DATOS PERSONALES

Esta sección recoge los principales puntos de conexión entre el Esquema Nacional de Seguridad y el Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), así como con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que lo complementa en el ordenamiento interno. La relación específica entre la protección de datos personales y el ENS, además de lo previsto en su artículo 3, encuentra un punto de conexión expreso en la disposición adicional primera de la LOPDGDD.

Las entidades, en función de si determinan los fines y medios del tratamiento o si tratan datos personales por cuenta de otro, podrán actuar, respectivamente, como responsables o encargados del tratamiento, debiendo cumplir en cada caso las obligaciones que les correspondan conforme al RGPD y a la LOPDGDD. Asimismo, cuando varias entidades determinen conjuntamente los fines y medios del tratamiento, deberá atenderse al régimen de corresponsabilidad, articulando de forma clara la distribución de funciones, responsabilidades y puntos de contacto frente a los interesados. A estos efectos, estas figuras deben entenderse como posiciones jurídicas asociadas a la entidad, no como cargos internos equivalentes a los previstos en el ENS.

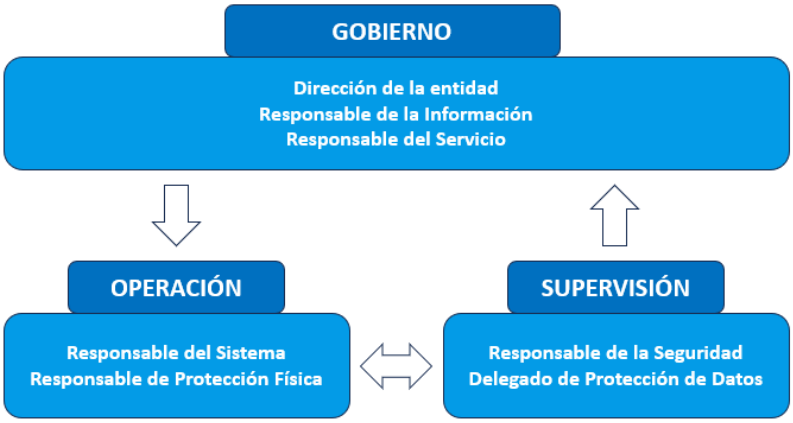
Por lo que se hace necesario que la organización, dentro de su modelo de gobernanza, determine las responsabilidades internas que considere oportunas para poder abordar con garantías las responsabilidades asociadas a cada posición jurídica.

Cuando los sistemas de información traten datos personales, deberá atenderse a lo dispuesto en el artículo 32 del RGPD, que exige al responsable y al encargado aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta, entre otros factores, el estado de la técnica, los costes de aplicación, la naturaleza del tratamiento y los riesgos para los derechos y libertades de las personas físicas. En el ámbito de las Administraciones Públicas, la AEPD ha señalado expresamente que deberá utilizarse el Esquema Nacional de Seguridad para seleccionar las medidas que deban implantarse, adaptando los criterios de determinación del riesgo a las particularidades del tratamiento de datos personales.

8.1.1 BLOQUES DE RESPONSABILIDAD

A los efectos de su integración en el modelo de gobernanza de la seguridad, las posiciones jurídicas definidas por el RGPD —responsable, encargado y, en su caso, corresponsable— no deben entenderse como funciones internas equivalentes a las previstas en el ENS, sino como posiciones jurídicas de la entidad de las que derivan obligaciones específicas. En consecuencia, y una vez realizado un análisis de contexto, corresponde a cada entidad traducir tales obligaciones a su propio modelo organizativo, distribuyéndolas entre los tres bloques de responsabilidad que se han definido

previamente, de forma coherente con el papel que asuma en cada tratamiento y con la naturaleza de los riesgos asociados.



8.1.1.1 Gobierno y dirección

Corresponde al ámbito de Gobierno y dirección la adopción de las decisiones estratégicas en materia de protección de datos, la aprobación de las medidas generales necesarias para garantizar el cumplimiento del RGPD y la LOPDGDD, y la asignación de recursos suficientes para ello.

En este nivel deben situarse, entre otras, las decisiones relativas a la identificación del papel que la entidad asume como responsable, encargado o corresponsable, la aprobación de las políticas generales de protección de datos, la integración de la protección de datos desde el diseño y por defecto, y la adopción de medidas organizativas que permitan garantizar y demostrar el cumplimiento del Reglamento. A estos efectos, resultan especialmente relevantes el artículo 24 del RGPD, sobre responsabilidad del responsable del tratamiento, y el artículo 25 del RGPD, sobre protección de datos desde el diseño y por defecto.

El registro de actividades de tratamiento constituye un elemento básico de la gobernanza en materia de protección de datos y un instrumento de conexión entre la organización del tratamiento y las medidas de seguridad aplicables.

El artículo 30.1 del RGPD exige al responsable del tratamiento un registro de actividades que incluya, entre otros extremos, finalidades, categorías de interesados y de datos, destinatarios, transferencias internacionales y, cuando sea posible, plazos de supresión y una descripción general de las medidas de seguridad. El artículo 30.2 establece un registro específico, de contenido diferente, para el encargado del tratamiento. Ambos deberán constar por escrito, inclusive en formato electrónico, sin perjuicio de las excepciones legalmente previstas. El artículo 31.2 de la Ley Orgánica 3/2018 exige a los sujetos enumerados en su artículo 77.1 hacer público, por medios electrónicos, el inventario de sus actividades de tratamiento con la información legalmente indicada.

La dirección debe garantizar la designación del Delegado de Protección de Datos (DPD) cuando sea obligatoria conforme al artículo 37.1 del RGPD o al artículo 34 de la Ley Orgánica 3/2018; en particular, para autoridades u organismos públicos, con la

excepción de los tribunales en el ejercicio de su función judicial. Fuera de esos supuestos podrá designarse voluntariamente.

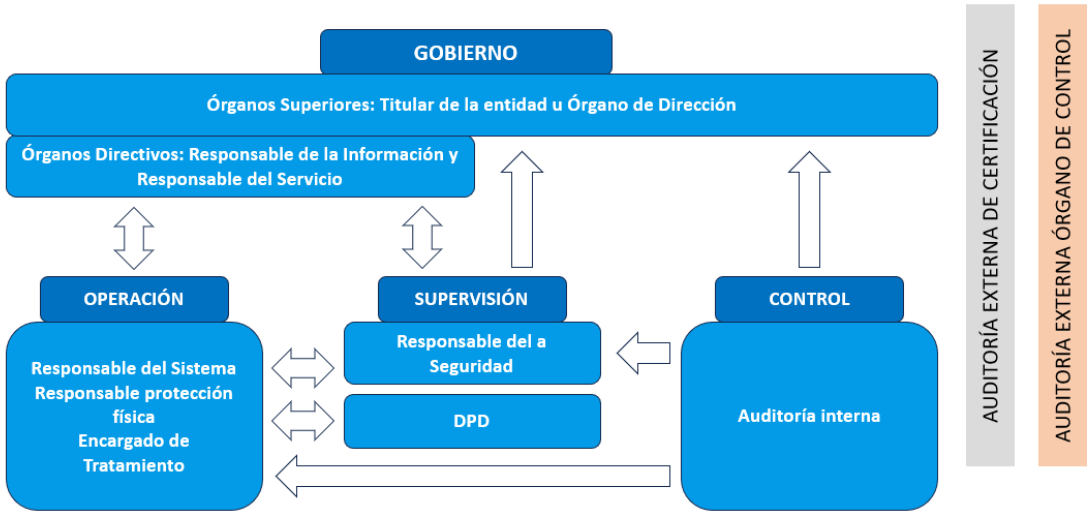
La dirección debe asegurar la correcta integración del DPD exigiendo respetar las garantías de posición previstas en el artículo 38 del RGPD, de forma que participe de manera adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales, disponga de los recursos necesarios para el desempeño de sus funciones, no reciba instrucciones en cuanto al ejercicio de las mismas y rinda cuentas directamente al más alto nivel jerárquico del responsable o del encargado.

En línea con lo dispuesto para el Esquema Nacional de Seguridad, el bloque de Gobierno puede establecer, como instrumento adicional de garantía, una función de auditoría o revisión independiente del cumplimiento de la normativa de protección de datos y de su integración en el modelo general de gobernanza de la seguridad.

Aunque el RGPD no impone una estructura interna de auditoría en términos equivalentes al modelo de tres líneas, sí exige que el responsable pueda demostrar el cumplimiento del Reglamento, mantenga documentación suficiente, conserve evidencia de las medidas adoptadas y documente tanto las violaciones de seguridad como las evaluaciones de impacto realizadas. A estos efectos, resultan especialmente relevantes el artículo 24, sobre responsabilidad proactiva; el artículo 30, sobre registro de actividades; el artículo 33.5, sobre documentación de las violaciones de seguridad; y el artículo 35, sobre evaluaciones de impacto.

Sobre esta base, se recomienda que la entidad valore la conveniencia de prever una función de control independiente, en proporción a sus riesgos y características, mediante auditoría interna o, en su caso, por terceros, con reporte adecuado al órgano de dirección, que permita verificar si las posiciones jurídicas asumidas por la entidad se han identificado correctamente, si las funciones se han distribuido de forma coherente entre los distintos bloques, si las medidas implantadas y supervisadas son suficientes y si la organización dispone de la documentación y evidencias necesarias para acreditar el cumplimiento del RGPD y de la LOPDGDD.

Esta revisión independiente no sustituye la función del DPD, pero la complementa desde la lógica general del modelo de gobernanza propuesto.



8.1.1.2 Supervisión

Corresponde a este bloque de responsabilidad la función de asesoramiento, propuesta, control y supervisión del cumplimiento de la normativa de protección de datos, de la seguridad del tratamiento y de la adecuación de las medidas implantadas por la primera línea.

En este bloque de supervisión la legislación establece la necesidad de que el DPD debe participar de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales con el objetivo de desarrollar adecuadamente las funciones encomendadas en el artículo 39 del RGPD. En este bloque se incluyen funciones tales como:

- Asesoramiento en el encaje jurídico del tratamiento y sobre la posición jurídica asumida por la entidad (Responsable, encargado o corresponsable).
- Supervisión de la protección de datos desde el diseño y por defecto.
- El asesoramiento de los análisis de riesgos y de las evaluaciones de impacto desde el punto de vista de la privacidad. Incluyendo como afectan dichos análisis a los requisitos de seguridad establecidos para la información y servicios.
- La supervisión del registro de actividades de tratamiento.
- Seguimiento y asesoramiento en la correcta gestión de incidentes con afectación a datos personales y la emisión de criterio sobre la suficiencia de las medidas adoptadas.

El DPD debe participar en los órganos de apoyo en la toma de decisiones del modelo de gobernanza como puedan ser los Comités o los grupos de trabajos que puedan resultar de aplicación.

En determinadas circunstancias, y con carácter excepcional, no resulta incompatible que el Delegado de Protección de Datos coincida con el Responsable de la Seguridad del ENS, siempre que concurran los requisitos de capacitación exigibles, no exista conflicto de intereses y se adopten las medidas organizativas necesarias para garantizar su independencia en el ejercicio de las funciones que le atribuye la normativa de protección de datos. Esta posibilidad exige examinar y documentar individualmente los conflictos de intereses que pudieran surgir, especialmente si quien ocupa ambos cargos diseña o decide medidas de tratamiento que posteriormente deba supervisar como DPD, de acuerdo con el artículo 38.6 del RGPD.

En aquellos ámbitos no atribuidos normativamente al DPD, la entidad podrá asignar funciones de coordinación y apoyo al Responsable de la Seguridad, cuando resulten compatibles con sus competencias, capacitación e independencia. Esta distribución interna no altera las obligaciones que el RGPD atribuye al responsable o al encargado del tratamiento ni las funciones independientes del DPD previstas en sus artículos 38 y 39.

Las principales funciones serían:

- Cuando el sistema trate datos personales, el Responsable de la Seguridad podrá incorporar al diseño de los controles los requisitos de seguridad que determine el responsable o 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.

- Prestar apoyo técnico y organizativo en los análisis de riesgos y, cuando corresponda, en las evaluaciones de impacto relativas a la protección de datos, aportando criterios para la valoración y la implantación de controles de seguridad. La obligación de realizar la evaluación de impacto, cuando sea exigible, corresponde al responsable del tratamiento conforme al artículo 35.1 del RGPD, con el asesoramiento del DPD previsto en el artículo 35.2.
- Determinación de medidas de seguridad que considere necesarias para satisfacer los requisitos marcados por el Responsable de Tratamiento y supervisión de su implantación.
- Apoyo a la unidad competente en la preparación o actualización del Registro de Actividades de Tratamiento, sin sustituir las responsabilidades del artículo 30 del RGPD.
- Asesoramiento sobre las cláusulas contractuales vinculadas a las medidas de seguridad de los tratamientos, coordinándose con las unidades jurídicas, de contratación y de protección de datos competentes.
- Colaboración técnica, cuando proceda, en la preparación de cláusulas informativas y políticas de privacidad que deban aprobar las unidades competentes en materia jurídica y de protección de datos.
- Participación, desde la perspectiva de seguridad de los sistemas, en los procedimientos de ejercicio de derechos y de gestión y notificación de violaciones de seguridad de los datos personales, sin desplazar las competencias del responsable o encargado del tratamiento ni las funciones del DPD.

8.1.1.3 Operación

Corresponde a este bloque de responsabilidad la ejecución material de las operaciones de tratamiento, la implantación efectiva de las medidas técnicas y organizativas aplicables y la gestión ordinaria de los sistemas y procesos que traten datos personales. En este bloque se sitúan, en particular, las funciones de explotación y administración de los sistemas de información, la aplicación práctica de las medidas de seguridad, la ejecución de controles, el deber de información, la gestión de accesos, la conservación de registros y la operativa vinculada al cumplimiento de las instrucciones dadas por el Responsable de la Seguridad de la Información.

Cuando la entidad actúe como encargada del tratamiento, este bloque de responsabilidad deberá asegurar que el tratamiento se realiza únicamente siguiendo instrucciones documentadas del responsable, que se aplican las medidas de seguridad acordadas y que se facilita la asistencia necesaria para el cumplimiento de las obligaciones del responsable, en los términos que correspondan conforme al artículo 28 del RGPD.

Cuando la entidad actúe como responsable, este bloque asumirá la implantación efectiva de las decisiones y requisitos definidos por el Responsable de la Seguridad de la Información y aprobados por el ámbito de Gobierno y la correcta ejecución de las

medidas derivadas del análisis de riesgos, de las evaluaciones de impacto y de la gestión ordinaria del tratamiento.

8.1.2 RELACIONES CON TERCEROS

8.1.2.1 Órganos de control

De conformidad con las funciones atribuidas al Delegado de Protección de Datos en el artículo 39 del RGPD, entre las que se incluyen: cooperar con la autoridad de control y actuar como punto de contacto con dicha autoridad para cuestiones relativas al tratamiento, incluida la consulta previa prevista en el artículo 36, así como para cualquier otra consulta que resulte pertinente, la organización podrá, en el marco de su modelo de gobernanza, asignar al DPD funciones adicionales de interlocución con la autoridad de control.

La organización dentro de su modelo de gobernanza puede optar por asignar al DPD la potestad de comunicación de brechas de seguridad, así como cualquier otra interacción con el órgano de control.

La autoridad de protección de datos competente depende de la naturaleza del tratamiento y del ámbito de competencias. En los tratamientos sujetos al RGPD y a la Ley Orgánica 3/2018 ejercerán sus funciones la Agencia Española de Protección de Datos y, en su ámbito propio, las autoridades autonómicas competentes. Para los tratamientos regulados por la Ley Orgánica 7/2021, de 26 de mayo, su artículo 48 identifica como autoridades de protección de datos a la AEPD y a las autoridades autonómicas en los términos previstos en dicho precepto. Deben distinguirse de los tratamientos con fines jurisdiccionales realizados por juzgados, tribunales y fiscalías, sometidos a la supervisión del Consejo General del Poder Judicial y de la Fiscalía General del Estado en sus respectivos ámbitos competenciales, conforme al artículo 236 octies de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

8.1.2.2 Interesados

Dentro del modelo de gobernanza se deben establecer los canales adecuados para ver quién se encarga de la interacción con los interesados, bien para comunicar brechas, bien para la gestión de ejercicios de derechos o consultas.

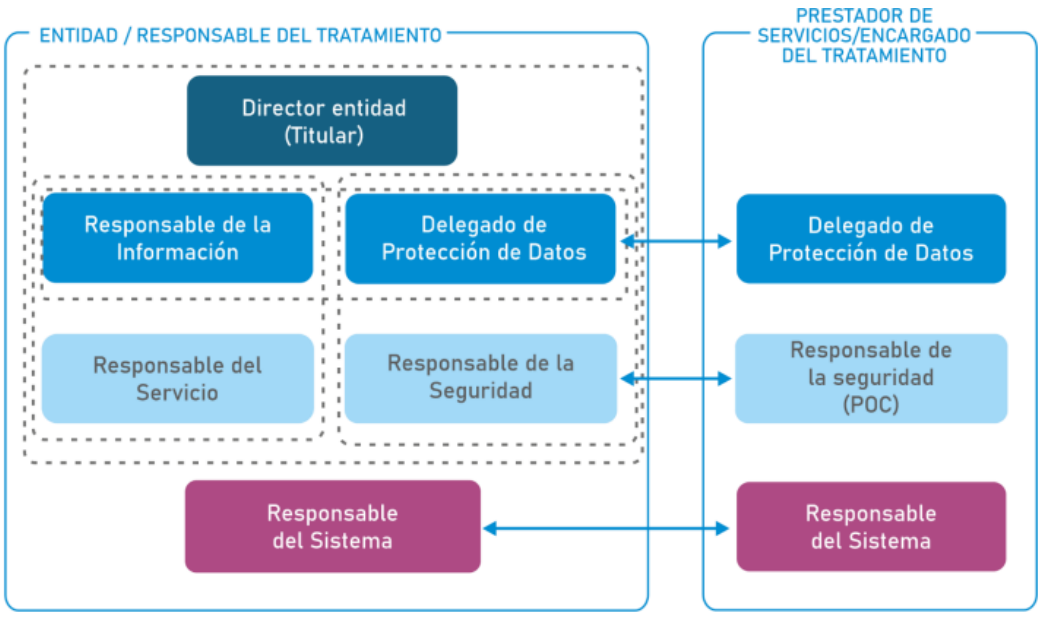
8.1.2.3 Encargados de tratamiento

La relación entre el responsable y el encargado del tratamiento deberá formalizarse, con carácter previo al inicio de cualquier tratamiento de datos personales, mediante el correspondiente contrato de encargo de tratamiento o acto jurídico equivalente, conforme a lo dispuesto en el artículo 28 del RGPD y la LOPDGDD.

Estos contratos constituyen un elemento esencial para garantizar el control del responsable sobre los tratamientos realizados por terceros y deberán contemplar, al menos:

- La definición precisa del objeto, duración, naturaleza y finalidad del tratamiento, así como las categorías de datos personales y de interesados afectados.
- La obligación del encargado de tratar los datos exclusivamente conforme a las instrucciones documentadas del responsable, sin destinarlos a fines propios.
- El compromiso de garantizar la confidencialidad de las personas autorizadas para tratar los datos.
- La adopción de medidas técnicas y organizativas adecuadas al riesgo, debidamente alineadas con el Esquema Nacional de Seguridad cuando resulte de aplicación.
- La regulación de la subcontratación (subencargados), incluyendo las condiciones para su autorización y las garantías exigibles.
- La asistencia al responsable en el cumplimiento de sus obligaciones, especialmente en materia de ejercicio de derechos, evaluaciones de impacto, consultas previas y gestión de incidentes.
- El establecimiento de mecanismos que permitan al responsable llevar a cabo verificaciones, auditorías o inspecciones, directamente o a través de terceros.
- La determinación del destino de los datos una vez finalizada la prestación del servicio, contemplando su devolución o supresión conforme a lo establecido normativamente.

Adicionalmente, la entidad deberá integrar la gestión de estos contratos dentro de su modelo de gobernanza, definiendo procedimientos para su inventario, revisión periódica, actualización y control, asegurando su coherencia con el marco normativo aplicable (RGPD, LOPDGDD) y con las políticas de seguridad de la información derivadas del ENS.



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

La presente distribución tiene carácter orientativo y responde a una lógica de integración de la normativa de protección de datos en el modelo de gobernanza ya definido por la entidad sobre la base del ENS. Su finalidad es facilitar la trazabilidad entre las obligaciones jurídicas que el RGPD y la LOPDGDD atribuyen a la entidad según la posición que asuma en cada tratamiento y las funciones internas que deben desplegarse para garantizar su cumplimiento, sin que ello suponga alterar la naturaleza de las figuras previstas en la normativa de protección de datos ni crear nuevas figuras internas obligatorias fuera de aquellas que la propia entidad determine en ejercicio de su potestad de autoorganización.

8.1.3 GESTIÓN DE RIESGOS

En materia de protección de datos, para la realización de análisis de riesgos y evaluaciones de impacto en la protección de datos (EIPD), resulta necesario emplear catálogos de amenazas específicamente orientados a la privacidad y a la salvaguarda de los derechos y libertades de las personas físicas.

Estos análisis deben ir más allá de la seguridad técnica convencional, incorporando riesgos como la pérdida de control sobre los datos, la discriminación o el uso indebido de la información personal, y alineándose con los criterios y metodologías establecidos por la Agencia Española de Protección de Datos (AEPD), cuyas directrices constituyen la referencia para garantizar un enfoque adecuado y conforme al RGPD.

Dicho análisis debe integrarse dentro del análisis global de riesgos de seguridad de la información, asegurando que, junto a los riesgos propios de la seguridad, se incorporen y valoren específicamente los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales. Esta integración debe permitir una visión conjunta y coherente del riesgo, teniendo en cuenta la distinta naturaleza de ambos tipos de riesgos, de modo que las medidas de seguridad y controles adoptados den respuesta tanto a las amenazas técnicas como a los impactos potenciales sobre las personas.

De este modo, y de conformidad con lo dispuesto en el art. 3 del Esquema Nacional de Seguridad, las medidas que se implanten podrán abordar de forma unificada el catálogo completo de riesgos identificado, sin perjuicio de la necesidad de incorporar controles específicos orientados a la protección de datos personales y a la garantía efectiva de los derechos y libertades de los interesados.

8.2 INTELIGENCIA ARTIFICIAL

Esta sección recoge los principales puntos de conexión entre el Esquema Nacional de Seguridad y el Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, en adelante, Reglamento de Inteligencia Artificial o RIA[1].

[1] **Nota importante.** Actualización normativa (a octubre de 2026). El Reglamento (UE) 2024/1689 ha sido modificado por el Reglamento (UE) 2026/1744 del Parlamento Europeo y del Consejo, de 8 de julio de 2026 (Ómnibus digital sobre IA). Conforme al artículo 113, en su redacción vigente, el capítulo III,

El RIA establece un marco jurídico uniforme para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial en la Unión Europea. Su finalidad es promover una inteligencia artificial centrada en el ser humano y fiable, garantizando un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, al tiempo que se favorece la innovación.

La relación entre el RIA y el ENS no se articula mediante una remisión general y expresa equivalente a la prevista en la normativa de protección de datos. No obstante, ambos marcos presentan importantes ámbitos de convergencia, especialmente en lo relativo a la gobernanza, la gestión de riesgos, la seguridad de los sistemas, la trazabilidad, la gestión de incidentes, la supervisión, la continuidad, la gestión de proveedores y la conservación de evidencias.

En particular, cuando un sistema de IA forme parte de un sistema de información incluido dentro del ámbito de aplicación del ENS, deberán aplicarse las medidas de seguridad correspondientes a su categoría. Dichas medidas podrán contribuir al cumplimiento de determinadas obligaciones del RIA, en especial las relativas a la exactitud, la solidez, la ciberseguridad, el registro de eventos, la vigilancia posterior a la comercialización y la gestión de incidentes. Esta integración no supone que el cumplimiento del ENS determine por sí solo la conformidad con el RIA, puesto que este último incorpora requisitos adicionales asociados, entre otros aspectos, a la calidad y gobernanza de los datos, la transparencia, la supervisión humana, la evaluación de conformidad y la protección de los derechos fundamentales.

Las entidades podrán actuar, según la posición que ocupen en la cadena de valor y la actividad que desarrollen, como proveedores, responsables del despliegue, importadores, distribuidores, representantes autorizados, fabricantes de productos o proveedores de modelos de IA de uso general. Una misma entidad podrá ocupar distintas posiciones respecto de diferentes sistemas de IA o, incluso, acumular varias posiciones respecto de un mismo sistema cuando concurran las circunstancias previstas en el RIA.

Asimismo, un importador, distribuidor, responsable del despliegue u otro tercero podrá pasar a ser considerado proveedor de un sistema de IA de alto riesgo cuando comercialice el sistema bajo su propio nombre o marca, efectúe una modificación sustancial o altere su finalidad prevista de modo que pase a considerarse de alto riesgo.

Estas figuras deben entenderse como posiciones jurídicas de la entidad, de las que derivan obligaciones específicas, y no como cargos internos equivalentes a los previstos en el ENS. En consecuencia, resulta necesario que cada organización determine, dentro

secciones 1, 2 y 3, salvo el artículo 6.5, se aplicará desde el 2 de diciembre de 2027 a los sistemas de alto riesgo del artículo 6.2 y anexo III, y desde el 2 de agosto de 2028 a los del artículo 6.1 y anexo I. Estos aplazamientos no pueden extrapolarse a todas las obligaciones del Reglamento: deberán atenderse los restantes hitos del artículo 113 y las disposiciones transitorias del artículo 111, así como la normativa sectorial aplicable.

de su modelo de gobernanza, las responsabilidades internas necesarias para poder asumir con garantías las obligaciones correspondientes a cada posición jurídica.

8.2.1 BLOQUES DE RESPONSABILIDAD

A los efectos de su integración en el modelo de gobernanza de la seguridad, las posiciones jurídicas definidas por el RIA no deben entenderse como funciones internas equivalentes a las previstas en el ENS. Se trata de posiciones de la entidad dentro del ciclo de vida y de la cadena de valor de los sistemas de IA, de las que derivan obligaciones cuyo alcance depende del tipo de sistema, su finalidad prevista, su clasificación de riesgo y el contexto en el que se desarrolla, comercializa o utiliza.

En consecuencia, una vez identificado el contexto y los sistemas de IA afectados, corresponde a cada entidad:

- Determinar la posición o posiciones jurídicas que ocupa respecto de cada sistema o modelo de IA.
- Clasificar los sistemas conforme al RIA.
- Identificar las obligaciones aplicables.
- Traducir dichas obligaciones a su modelo organizativo.
- Distribuirlas entre los bloques de Gobierno y dirección, Supervisión y Operación.
- Establecer mecanismos de coordinación con las funciones de seguridad, protección de datos, cumplimiento, contratación, asesoría jurídica, control interno y gestión de riesgos.

Esta distribución deberá realizarse considerando que el RIA no establece, con carácter general, la obligación de designar internamente una figura equivalente a un "responsable de inteligencia artificial". La entidad podrá crearla en ejercicio de su potestad de autoorganización, pero su existencia no alterará las posiciones jurídicas ni las responsabilidades atribuidas por el Reglamento a la propia entidad.

8.2.1.1 Gobierno y dirección

Corresponde al ámbito de Gobierno y dirección la adopción de las decisiones estratégicas relativas al desarrollo, adquisición, puesta en servicio y utilización de sistemas de IA, así como la aprobación del marco general de gobernanza necesario para garantizar el cumplimiento del RIA.

En este nivel deben situarse, entre otras, las siguientes responsabilidades:

- Aprobar la política corporativa de gobernanza y uso responsable de la IA.
- Determinar el nivel de tolerancia al riesgo asociado al uso de sistemas de IA.
- Aprobar los criterios para identificar y clasificar los sistemas y modelos de IA.
- Decidir si la entidad actúa como proveedor, responsable del despliegue, importador, distribuidor, representante autorizado u otro operador.
- Aprobar la introducción o utilización de sistemas de IA de alto riesgo.

- Asignar los recursos humanos, técnicos, económicos y organizativos necesarios.
- Garantizar que el personal y demás personas que utilicen sistemas de IA por cuenta de la entidad dispongan de un nivel suficiente de alfabetización en materia de IA, considerando sus conocimientos, experiencia, formación y el contexto de uso.
- Integrar la gobernanza de la IA en el modelo general de seguridad, gestión de riesgos, protección de datos, contratación y control interno.
- Asegurar, cuando resulte exigible, la realización y validación interna de las evaluaciones de impacto relativas a los derechos fundamentales cuya responsabilidad corresponde a los responsables del despliegue comprendidos en el artículo 27 del RIA.
- Asegurar la implantación de mecanismos de supervisión humana y que las personas designadas dispongan de autoridad, competencia, formación y recursos adecuados.
- Aprobar las condiciones bajo las cuales puedan realizarse modificaciones, adaptaciones o cambios de finalidad en los sistemas de IA.
- Establecer criterios para la suspensión, retirada o sustitución de sistemas que no sean conformes o presenten un riesgo inaceptable.
- Resolver los conflictos entre objetivos operativos, eficiencia, seguridad, protección de derechos fundamentales y cumplimiento normativo.

A su vez, la organización deberá mantener un **inventario de sistemas y modelos de IA** que permita identificar, al menos:

- La denominación y finalidad prevista del sistema.
- Las unidades responsables de su adquisición, desarrollo y utilización.
- El proveedor y los demás operadores de la cadena de valor.
- La posición jurídica asumida por la entidad.
- La clasificación del sistema conforme al RIA.
- Los procesos, servicios y sistemas de información en los que se integra.
- Las categorías de personas o colectivos potencialmente afectados.
- La información y los datos utilizados.
- La documentación contractual y técnica aplicable.
- Las evaluaciones de riesgos, impacto y conformidad realizadas.
- Los mecanismos de supervisión humana.
- Los incidentes, reclamaciones y medidas correctoras asociados.

Cuando la entidad actúe como proveedor de sistemas de IA de alto riesgo, el ámbito de Gobierno y dirección deberá garantizar la existencia de un sistema de gestión de la calidad que cubra de forma coherente el conjunto del ciclo de vida del sistema. Este

sistema deberá integrar, entre otros elementos, la estrategia de cumplimiento, los procedimientos de diseño y desarrollo, la gestión de datos, la evaluación de riesgos, la evaluación de conformidad, la gestión de modificaciones, la vigilancia posterior a la comercialización, la notificación de incidentes graves y la conservación de documentación y evidencias.

Cuando resulte exigible, la dirección deberá asegurar que el sistema sea registrado en la base de datos de la Unión Europea o en los registros nacionales correspondientes. En particular, antes de utilizar determinados sistemas de IA de alto riesgo, las autoridades, órganos u organismos públicos responsables del despliegue deben cumplir las obligaciones de registro previstas en el RIA.

Aunque el RIA no impone con carácter general una estructura organizativa basada en el modelo de tres líneas, sí exige que los operadores puedan demostrar el cumplimiento de sus obligaciones, mantengan la documentación correspondiente, conserven registros, realicen las evaluaciones exigibles y cooperen con las autoridades competentes.

En línea con lo dispuesto para el Esquema Nacional de Seguridad, se recomienda que el bloque de Gobierno valore el establecimiento de una función de control independiente que permita revisar el cumplimiento del RIA y su integración en el modelo general de gobernanza de la seguridad.

Sobre esta base, la entidad puede prever una función de control independiente, atendiendo a su riesgo, naturaleza y dimensión, mediante auditoría interna o, en su caso, mediante terceros, con reporte adecuado al órgano de dirección, que permita verificar:

- Si se han identificado correctamente los sistemas y modelos de IA.
- Si se ha determinado adecuadamente la posición jurídica de la entidad.
- Si los sistemas se han clasificado correctamente.
- Si las funciones se han distribuido de forma coherente entre los distintos bloques.
- Si se han realizado las evaluaciones exigibles.
- Si las medidas técnicas, organizativas y contractuales implantadas son suficientes.
- Si existen mecanismos efectivos de supervisión humana.
- Si la entidad dispone de documentación y evidencias suficientes.
- Si se gestionan adecuadamente los incidentes, reclamaciones y medidas correctoras.
- Si los cambios realizados sobre los sistemas pueden constituir una modificación sustancial.
- Si se cumplen las obligaciones de vigilancia y seguimiento durante todo el ciclo de vida.

Cuando exista, esta función de control independiente deberá coordinarse con las auditorías del ENS, las revisiones en materia de protección de datos y las restantes funciones de control interno, evitando duplicidades y procurando reutilizar las evidencias comunes cuando ello sea posible.

8.2.1.2 Supervisión

Corresponde a este bloque la función de asesoramiento, propuesta, coordinación, control y supervisión del cumplimiento del RIA, de la seguridad de los sistemas de IA y de la adecuación de las medidas implantadas por la primera línea.

Dado que el RIA no establece con carácter general una figura interna obligatoria equivalente al Delegado de Protección de Datos, la entidad deberá determinar qué órgano, unidad o función asume la coordinación de las obligaciones en materia de IA. Esta función podrá configurarse como una responsabilidad específica o atribuirse a una unidad existente, siempre que cuente con la independencia funcional, capacitación, autoridad y recursos adecuados.

En este bloque se incluyen, entre otras, las siguientes funciones:

- Asesorar sobre el ámbito de aplicación del RIA.
- Identificar la posición jurídica asumida por la entidad.
- Asesorar sobre la clasificación de los sistemas de IA y, en particular, sobre su consideración como sistemas prohibidos, de alto riesgo, sujetos a obligaciones específicas de transparencia o de riesgo mínimo.
- Supervisar el inventario de sistemas y modelos de IA.
- Proponer políticas, normas y procedimientos internos.
- Coordinar los análisis de riesgos y las evaluaciones de impacto.
- Coordinar o prestar apoyo a la elaboración de la evaluación de impacto relativa a los derechos fundamentales cuando resulte exigible, sin perjuicio de que la obligación jurídica establecida en el artículo 27 del RIA corresponda al responsable del despliegue en los supuestos previstos en dicho artículo.
- Verificar que las personas designadas para la supervisión humana prevista en el artículo 14 del RIA, que es distinta de la supervisión organizativa de la seguridad establecida en el ENS disponen de competencia, formación, autoridad e independencia suficientes.
- Supervisar los mecanismos de alfabetización en materia de IA.
- Verificar el cumplimiento de los requisitos de información y transparencia.
- Coordinar la gestión de reclamaciones, incidentes graves y situaciones de no conformidad.
- Asesorar a los órganos de contratación sobre los requisitos que deben incorporarse en pliegos, contratos y acuerdos.
- Participar en la evaluación de proveedores y de la cadena de suministro.

- Supervisar los cambios realizados sobre los sistemas y valorar cuándo pueden constituir una modificación sustancial.
- Coordinar la cooperación con las autoridades competentes y los organismos de evaluación de la conformidad.
- Promover la conservación de la documentación y de las evidencias de cumplimiento.

Cuando el sistema de IA implique el tratamiento de datos personales, el Delegado de Protección de Datos deberá participar de forma adecuada y en tiempo oportuno en las cuestiones que afecten a la protección de datos. Su intervención no se extiende automáticamente al conjunto de las obligaciones del RIA, pero resulta especialmente relevante en materia de gobernanza de datos, tratamientos biométricos, elaboración de perfiles, decisiones automatizadas, transparencia, evaluación de impacto y derechos de las personas.

El RIA se aplica sin perjuicio del RGPD y no sustituye las obligaciones que correspondan a proveedores o responsables del despliegue cuando actúen como responsables o encargados del tratamiento.

El Delegado de Protección de Datos podrá formar parte de los comités o grupos de trabajo de gobernanza de la IA. No obstante, la atribución de funciones adicionales deberá respetar su independencia y evitar la existencia de conflictos de intereses.

Se propone que el Responsable de la Seguridad participe en este bloque respecto de las funciones vinculadas con la seguridad de los sistemas de información y, en particular, en las siguientes:

- Identificación de los sistemas de información que soportan o integran sistemas de IA.
- Determinación del ámbito de aplicación del ENS y de la categoría correspondiente.
- Traslado de los riesgos derivados de la IA al análisis de riesgos de seguridad.
- Propuesta de requisitos de seguridad aplicables a la información, los servicios, los modelos, los datos y las infraestructuras.
- Supervisión de la implantación de medidas de exactitud, solidez, resiliencia y ciberseguridad.
- Coordinación de la gestión de vulnerabilidades, incidentes y continuidad.
- Supervisión de los mecanismos de registro, trazabilidad y conservación de evidencias.
- Valoración de los riesgos asociados a proveedores, servicios en la nube, modelos externos, interfaces de programación y componentes de terceros.
- Evaluación del impacto de las modificaciones del sistema sobre su seguridad.
- Coordinación con las funciones responsables de protección de datos, cumplimiento y gestión de riesgos.

No obstante, la seguridad de los sistemas de IA no debe limitarse a la protección de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. También deberá considerar, en función del sistema, la calidad de los datos, la exactitud de los resultados, la presencia de sesgos, la capacidad de supervisión humana, la robustez frente a errores y manipulaciones, el comportamiento fuera de distribución, la degradación del modelo y los efectos sobre los derechos fundamentales.

8.2.1.3 Operación

Corresponde a este bloque la ejecución material de las actividades de diseño, desarrollo, adquisición, integración, puesta en servicio, utilización, mantenimiento y retirada de los sistemas de IA.

En este bloque se sitúan, en particular:

- Los equipos de desarrollo y ciencia de datos.
- Las unidades de tecnologías de la información.
- Los administradores de sistemas y plataformas.
- Las unidades responsables de datos.
- Los responsables funcionales de los procesos.
- Los usuarios profesionales de sistemas de IA.
- Los responsables de la contratación y gestión operativa de proveedores.
- Las personas encargadas de la supervisión humana.
- Los equipos de soporte y mantenimiento del sistema.

Cuando la entidad actúe como proveedor de un sistema de IA de alto riesgo, este bloque deberá ejecutar las medidas necesarias para:

- Aplicar el sistema de gestión de riesgos durante todo el ciclo de vida.
- Garantizar la gobernanza y calidad de los datos.
- Elaborar y mantener la documentación técnica.
- Implementar mecanismos de registro automático de eventos.
- Facilitar la información y las instrucciones de uso.
- Diseñar mecanismos eficaces de supervisión humana.
- Garantizar niveles adecuados de exactitud, solidez y ciberseguridad.
- Ejecutar la evaluación de conformidad aplicable.
- Registrar el sistema cuando corresponda.
- Implantar la vigilancia posterior a la comercialización.
- Comunicar incidentes graves y aplicar medidas correctoras.
- Conservar la documentación y las evidencias durante los plazos exigibles.

Cuando la entidad actúe como responsable del despliegue de un sistema de IA de alto riesgo, este bloque deberá asegurar, entre otros aspectos, que:

- El sistema se utiliza conforme a las instrucciones del proveedor.
- Los datos de entrada bajo el control de la entidad son pertinentes y suficientemente representativos para la finalidad prevista.
- Se aplica una supervisión humana efectiva.
- Se conservan los registros generados automáticamente durante el plazo que corresponda.
- Se realiza un seguimiento del funcionamiento del sistema.
- Se informa al proveedor o distribuidor cuando existan riesgos o incidentes.
- Se suspende la utilización cuando el sistema pueda presentar un riesgo.
- Se cumplen las obligaciones de información a las personas afectadas.
- El responsable del despliegue efectúa la evaluación de impacto relativa a los derechos fundamentales cuando y en los términos en que resulte exigible conforme al artículo 27 del RIA.
- Se efectúa el registro previo en la base de datos correspondiente, cuando proceda.

La supervisión humana no debe configurarse como una mera validación formal de las salidas del sistema. Las personas encargadas deberán comprender las capacidades y limitaciones del sistema, detectar anomalías, interpretar adecuadamente sus resultados, evitar sesgos de automatización y disponer de autoridad suficiente para no utilizar, ignorar, anular, revertir o interrumpir el sistema cuando resulte necesario.

Cuando las decisiones adoptadas por la entidad se basen principalmente en las salidas de determinados sistemas de IA de alto riesgo y produzcan efectos jurídicos o afecten significativamente a las personas, la operativa deberá permitir proporcionar explicaciones claras y significativas, en los supuestos previstos en el artículo 86 del RIA.

8.2.2 RELACIONES CON TERCEROS

8.2.2.1 Cadena de suministro

El Reglamento de Inteligencia Artificial establece una distribución de obligaciones a lo largo del ciclo de vida de los sistemas de IA, atendiendo a la posición jurídica que cada organización ocupa respecto de su desarrollo, introducción en el mercado, puesta en servicio, distribución o utilización. A estos efectos, el RIA distingue, entre otras, las figuras de proveedor, responsable del despliegue, importador, distribuidor, representante autorizado, fabricante de un producto y proveedor de modelos de IA de uso general.

Estas figuras deben entenderse como posiciones jurídicas de las organizaciones que participan en la cadena de valor del sistema de IA y no como cargos o funciones internas

equivalentes a los definidos en el Esquema Nacional de Seguridad. Cada organización deberá identificar la posición o posiciones que asume en relación con cada sistema de IA y determinar las obligaciones que se derivan de ellas, trasladándolas a su modelo interno de gobernanza y a los correspondientes bloques de Gobierno y dirección, Supervisión y Operación.

La posición jurídica de una organización no depende únicamente de la denominación que le hayan atribuido las partes en el contrato, sino de las actividades que efectivamente desarrolla y del grado de control que ejerce sobre el sistema de IA. En particular, determinadas actuaciones realizadas por un importador, distribuidor, responsable del despliegue u otro tercero, como comercializar un sistema de IA de alto riesgo bajo su propio nombre o marca, introducir una modificación sustancial o cambiar su finalidad prevista, pueden hacer que dicha organización pase a ser considerada proveedor y deba asumir las obligaciones correspondientes a esta posición.

Por ello, las relaciones entre las distintas organizaciones que intervienen en el ciclo de vida del sistema de IA deberán formalizarse de manera que permitan delimitar claramente sus respectivas posiciones jurídicas, responsabilidades y obligaciones. Esta formalización deberá asegurar la disponibilidad y transmisión de la información, documentación y evidencias necesarias para que cada parte pueda cumplir las obligaciones que le correspondan en materia de gestión de riesgos, gobernanza de datos, documentación técnica, evaluación de conformidad, transparencia, supervisión humana, exactitud, solidez, ciberseguridad, registro de eventos, vigilancia posterior a la comercialización y gestión de incidentes.

La distribución contractual de funciones no podrá utilizarse para excluir, limitar o trasladar aquellas obligaciones que el RIA atribuya directamente a cada operador. No obstante, los contratos, acuerdos y demás instrumentos jurídicos deberán concretar los mecanismos de cooperación necesarios para garantizar su cumplimiento, especialmente cuando una organización dependa de información, documentación técnica, registros, componentes, modelos o servicios proporcionados por otra entidad.

La aplicación del RIA no resulta incompatible con las obligaciones establecidas por el Reglamento General de Protección de Datos y por el Esquema Nacional de Seguridad. Estos marcos normativos deberán aplicarse de forma coordinada y acumulativa cuando concurran sus respectivos ámbitos de aplicación. El propio RIA establece un marco orientado a proteger la salud, la seguridad y los derechos fundamentales, sin sustituir las obligaciones que resulten aplicables en materia de protección de datos personales o seguridad de la información.

En consecuencia, cuando un sistema de IA trate datos personales, las organizaciones que participen en su ciclo de vida deberán determinar, además de la posición que ocupan conforme al RIA, si actúan como responsables, encargados o corresponsables del tratamiento conforme al RGPD. Ambas calificaciones responden a marcos jurídicos y criterios diferentes, por lo que la posición de proveedor o responsable del despliegue

en el RIA no determina automáticamente la posición que corresponde a la entidad conforme a la normativa de protección de datos.

Del mismo modo, cuando el sistema de IA forme parte de un sistema de información incluido en el ámbito de aplicación del ENS, deberán identificarse la categoría del sistema, los requisitos de seguridad de la información y de los servicios y las medidas de seguridad aplicables. La posición que la organización ocupe con arreglo al RIA no sustituye ni modifica las responsabilidades que deban establecerse conforme al ENS.

Las relaciones con terceros deberán, por tanto, abordarse desde una perspectiva integral que permita determinar simultáneamente:

- La posición de cada organización en el ciclo de vida del sistema de IA conforme al RIA.
- La posición de cada entidad como responsable, encargado o corresponsable del tratamiento conforme al RGPD, cuando se traten datos personales.
- Las funciones y responsabilidades aplicables conforme al ENS, cuando el sistema de información se encuentre dentro de su ámbito de aplicación.
- Las obligaciones derivadas de la normativa sectorial que resulte aplicable.
- Los mecanismos de coordinación, intercambio de información, supervisión y control necesarios para garantizar el cumplimiento conjunto de los diferentes marcos normativos.

Una misma relación entre organizaciones podrá, por tanto, estar sujeta simultáneamente al RIA, al RGPD y al ENS. En estos casos, los contratos y demás instrumentos jurídicos deberán integrar coherentemente los requisitos derivados de los tres marcos, evitando duplicidades y procurando que los controles, evidencias y mecanismos de supervisión puedan ser reutilizados cuando respondan a finalidades compatibles.

No obstante, la integración de los requisitos no implica que el cumplimiento de uno de estos marcos permita presumir automáticamente el cumplimiento de los restantes. Las medidas del ENS podrán contribuir al cumplimiento de los requisitos de exactitud, solidez, ciberseguridad, trazabilidad, continuidad, gestión de cambios e incidentes previstos en el RIA, pero deberán complementarse con los controles específicos que este exige. Del mismo modo, el cumplimiento de las obligaciones del RGPD en materia de responsabilidad proactiva, protección de datos desde el diseño, seguridad del tratamiento o evaluación de impacto podrá aportar elementos relevantes para la gobernanza de los sistemas de IA, sin sustituir las evaluaciones, requisitos y obligaciones propios del RIA.

En particular, cuando resulte necesario formalizar simultáneamente un encargo de tratamiento conforme al artículo 28 del RGPD y una relación entre operadores sujeta al RIA, ambos contenidos podrán incorporarse en un mismo contrato o en instrumentos jurídicos coordinados, siempre que las obligaciones correspondientes a cada marco

puedan identificarse con claridad y no se produzcan contradicciones, lagunas o asignaciones incompatibles.

La organización deberá integrar estas relaciones dentro de su modelo general de gobernanza de terceros, estableciendo procedimientos para su identificación, inventario, evaluación previa, formalización, seguimiento, revisión y terminación. Asimismo, deberá prever mecanismos que permitan detectar cambios en las actividades de las partes que puedan alterar su posición jurídica, especialmente cuando se produzcan modificaciones del sistema, cambios de finalidad, reentrenamientos, actualizaciones relevantes, integraciones con otros sistemas o utilización del sistema bajo el nombre o marca de una organización distinta del proveedor inicial.

La finalidad de esta integración es asegurar que las responsabilidades se encuentren claramente delimitadas durante todo el ciclo de vida del sistema de IA, que cada organización disponga de la información y de los medios necesarios para cumplir sus obligaciones y que las exigencias del RIA se apliquen de forma coordinada con las derivadas del RGPD, del ENS y del resto del ordenamiento jurídico aplicable.

8.2.3 GESTIÓN DE RIESGOS

La gestión de riesgos constituye uno de los elementos centrales del RIA. En el caso de los sistemas de IA de alto riesgo, el proveedor deberá establecer, implantar, documentar y mantener un sistema de gestión de riesgos como proceso continuo e iterativo durante todo el ciclo de vida del sistema.

Este proceso deberá comprender, al menos:

- La identificación y análisis de los riesgos conocidos y razonablemente previsibles.
- La estimación y evaluación de los riesgos derivados del uso conforme a la finalidad prevista.
- La consideración de los riesgos derivados de usos indebidos razonablemente previsibles.
- La evaluación de otros riesgos a partir de los datos obtenidos durante la vigilancia posterior a la comercialización.
- La adopción de medidas adecuadas y específicas de gestión de riesgos.
- La comprobación de la eficacia de dichas medidas.
- La realización de pruebas apropiadas antes de la introducción en el mercado o puesta en servicio.
- La revisión continuada de los riesgos durante la vida útil del sistema.

El análisis de riesgos de IA deberá integrarse en el análisis global de riesgos de la organización, pero manteniendo la distinción entre las diferentes perspectivas de riesgo:

1. Riesgos para la seguridad de la información y los servicios, abordados mediante el ENS y las metodologías de análisis de riesgos aplicables.

2. Riesgos para la salud y la seguridad de las personas, derivados de errores, fallos, comportamientos inesperados o utilización indebida del sistema.
3. Riesgos para los derechos fundamentales, como la discriminación, la pérdida de autonomía, la afectación a la intimidad, la falta de explicación, las restricciones injustificadas de derechos o las dificultades para impugnar decisiones.
4. Riesgos de cumplimiento, relacionados con una clasificación incorrecta, informaciones insuficientes, falta de registro, incumplimiento de las condiciones de uso o ausencia de evaluación de conformidad.
5. Riesgos operacionales y de terceros, incluidos la dependencia de proveedores, la falta de portabilidad, los cambios no controlados, la indisponibilidad del servicio y la opacidad de componentes externos.

Cuando resulte exigible, la entidad responsable del despliegue deberá realizar una evaluación de impacto relativa a los derechos fundamentales antes de poner en funcionamiento el sistema de IA de alto riesgo. Esta evaluación deberá considerar el contexto concreto de uso, la duración y frecuencia de utilización, las categorías de personas y colectivos afectados, los riesgos específicos para sus derechos y las medidas previstas en caso de materialización. Determinados organismos públicos, entidades privadas que prestan servicios públicos y ciertos responsables del despliegue de sistemas de alto riesgo están sujetos a esta obligación.

La evaluación de impacto relativa a los derechos fundamentales deberá coordinarse, cuando proceda, con:

- El análisis de riesgos del ENS.
- La evaluación de impacto en la protección de datos.
- Los análisis de impacto sobre la seguridad y continuidad de los servicios.
- Las evaluaciones de impacto regulatorio, sectorial o ético.
- Los procedimientos de evaluación de proveedores.
- Las evaluaciones de conformidad del sistema.

Esta coordinación deberá permitir reutilizar información y evidencias, pero no deberá conducir a confundir el objeto de cada evaluación. El análisis de riesgos del ENS se orienta fundamentalmente a la protección de la información y los servicios, mientras que la evaluación del RIA deberá considerar también las consecuencias del sistema sobre la salud, la seguridad y los derechos fundamentales.

En relación con la ciberseguridad, el análisis deberá considerar, además de las amenazas convencionales, aquellas específicamente asociadas a los sistemas de IA, tales como:

- Envenenamiento de datos.
- Manipulación de datos de entrada.
- Ataques adversarios.
- Extracción o inferencia del modelo.

- Fugas de información mediante las salidas.
- Alteración de parámetros o pesos.
- Compromiso de la cadena de suministro.
- Dependencia de modelos o componentes externos.
- Inyección de instrucciones.
- Uso de información no autorizada.
- Degradación del modelo.
- Deriva de datos o conceptos.
- Generación de resultados incorrectos o engañosos.
- Automatización excesiva y confianza indebida en las salidas.

Las medidas del ENS podrán utilizarse como base para dar respuesta a parte de estos riesgos, especialmente en materia de control de acceso, segregación de funciones, protección de las comunicaciones, registro de actividad, gestión de cambios, gestión de vulnerabilidades, continuidad, protección de la cadena de suministro y respuesta ante incidentes.

No obstante, deberán complementarse con controles específicamente orientados a la IA, como la validación de datos y modelos, la evaluación de sesgos, las pruebas de robustez, el seguimiento del rendimiento, la supervisión humana, la trazabilidad de versiones y la detección de cambios en el comportamiento del sistema.

De este modo, los análisis deberán permitir una visión conjunta y coherente de los riesgos, sin perder la distinta naturaleza de los bienes jurídicos protegidos. Las medidas y controles adoptados deberán responder tanto a las amenazas que afecten a la información y a los servicios como a los impactos potenciales de los sistemas de IA sobre las personas, los colectivos, la sociedad y los derechos fundamentales.

9 ANEXO B: MATRIZ RACI ORIENTATIVA Y COORDINACIÓN EN INCIDENTES

Las siguientes matrices tienen carácter exclusivamente orientativo y deberán adaptarse a las competencias y al modelo organizativo de cada entidad. No crean nuevas atribuciones legales ni alteran las previstas en el ENS, el RGPD o el RIA.

En las matrices, A identifica la responsabilidad de decisión o validación de la actividad; R, su ejecución; C, las figuras consultadas; e I, las informadas. Las asignaciones deberán documentarse en la Política de Seguridad, normas o procedimientos internos aplicables.

9.1 GOBIERNO, PLANIFICACIÓN Y GESTIÓN DE RIESGOS

Actividad	A: decisión o validación	R: ejecución	C: consulta	I: información
Aprobación y revisión de la estrategia y de la Política de Seguridad de la Información	Titular de la entidad u órgano de dirección competente	Responsable de la Seguridad	Responsables de la Información, del Servicio y del Sistema; asesoría jurídica	Unidades y personal afectados
Aprobación de prioridades, recursos y presupuesto de seguridad	Titular de la entidad u órgano de dirección competente	Responsable de la Seguridad, con apoyo de la unidad presupuestaria	Responsables de la Información, del Servicio y del Sistema	Unidades ejecutoras
Valoración de la información	Responsable de la Información	Unidad gestora de la información	Responsables de la Seguridad y del Sistema	Responsable del Servicio
Valoración de los servicios	Responsable del Servicio	Unidad gestora del servicio	Responsables de la Seguridad y del Sistema	Responsable de la Información
Determinación de la categoría de seguridad del sistema	Responsable de la Seguridad	Responsable de la Seguridad	Responsables de la Información y del Servicio	Órgano de dirección; Responsable del Sistema
Elaboración y actualización del análisis de riesgos de seguridad de la información	Responsable de la Seguridad	Equipo de análisis de riesgos designado	Responsables de la Información, del Servicio y del Sistema	Órgano de dirección
Formalización de la Declaración de Aplicabilidad y aprobación de las medidas compensatorias que procedan	Responsable de la Seguridad	Responsable de la Seguridad	Responsables de la Información, del Servicio y del Sistema	Órgano de dirección
Aprobación del plan de tratamiento de riesgos y del plan de mejora, incluidas sus prioridades y recursos	Titular de la entidad u órgano de dirección competente	Responsable de la Seguridad	Responsables de la Información, del Servicio y del Sistema; unidad presupuestaria	Unidades ejecutoras
Aceptación del riesgo residual	Responsable de la Información, dentro de su competencia y de los límites aprobados	Responsable de la Seguridad, mediante la preparación de la valoración y propuesta	Responsables de la Información, del Servicio y del Sistema	Órgano de dirección; Responsable del Servicio
Seguimiento del riesgo residual y escalado de desviaciones significativas	Responsable de la Seguridad	Responsable de la Seguridad	Responsable del Sistema	Órgano de dirección; Responsables de la Información y del Servicio

9.2 DOCUMENTACIÓN Y OPERACIÓN

Actividad	A: decisión o validación	R: ejecución	C: consulta	I: información
Elaboración y revisión de la normativa de seguridad	Órgano con competencia de aprobación conforme a la Política de Seguridad de la Información	Responsable de la Seguridad	Responsables de la Información, del Servicio y del Sistema; asesoría jurídica	Personal y terceros afectados
Elaboración y actualización de los procedimientos e instrucciones técnicas de seguridad	Responsable de seguridad y Responsable del Sistema, dentro de su ámbito de aplicación	Administradores de seguridad o Administradores de Sistemas, dentro de su ámbito de aplicación	Unidades responsables de los procesos o actividades a los que les resulte aplicable el procedimiento o instrucción	Personal operador y terceros afectados.
Implantación y operación de medidas de seguridad	Responsable del Sistema, Responsable de Protección Física y unidades competentes	Administradores de Sistemas y Administradores de Seguridad, y unidades competentes, dentro de su ámbito de aplicación	Responsable de la Seguridad	Órgano de dirección; Responsables de la Información y del Servicio

9.3 COORDINACIÓN EN INCIDENTES

En los incidentes, la dirección funcional de la respuesta y la coordinación de comunicaciones corresponde a las funciones que la Política de Seguridad atribuya a la seguridad de la información; los equipos operativos realizan la contención, erradicación y recuperación bajo las competencias del Responsable del Sistema. Las notificaciones a autoridades y destinatarios se efectuarán por los sujetos obligados y los cauces determinados por el artículo 33 del ENS y, cuando proceda, por la legislación de protección de datos y la normativa sectorial. La existencia de un proveedor o de un POC no desplaza la responsabilidad última de la entidad del sector público destinataria de los servicios (artículo 13.5 ENS).