centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 805

Esquema Nacional de Seguridad
Política de Seguridad de la Información



Noviembre 2026

Edita:

centro criptológico nacional

© Centro Criptológico Nacional, 2026

Firmado digitalmente por CCN
Fecha: 2026.11.12 12:59:42 +01'00'

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 4

2 REQUISITOS NORMATIVOS 5

3 PAUTAS GENERALES PARA LA ELABORACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 9

4 RECOMENDACIONES DE CONTENIDO 10

4.1 OBJETO Y ÁMBITO DE APLICACIÓN 11

4.2 MISIÓN Y FINES DE LA ENTIDAD. 11

4.3 MARCO NORMATIVO. 11

4.4 PRINCIPIOS DE SEGURIDAD. 11

4.5 ORGANIZACIÓN DE SEGURIDAD. 12

4.6 DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA, SU GESTIÓN Y ACCESO. 13

4.7 CONCIENCIACIÓN Y FORMACIÓN. 13

4.8 GESTIÓN DE RIESGOS Y MEJORA CONTINUA. 13

4.9 GESTIÓN DEL PERSONAL Y PROFESIONALIDAD. 14

4.10 RELACIONES CON TERCEROS. 14

4.11 AUDITORIAS. 14

4.12 RESOLUCIÓN DE CONFLICTOS. 14

4.13 REVISIÓN Y ACTUALIZACIÓN. 15

4.14 SANCIONES POR INCUMPLIMIENTO. 15

ANEXO A. MARCOS NORMATIVOS A INTEGRAR 16

ANEXO A.1. PROTECCIÓN DE DATOS PERSONALES 16

ANEXO A.1.1. REQUISITOS NORMATIVOS 16

ANEXO A.1.2. RECOMENDACIONES DE CONTENIDO 19

ANEXO A.2. INTELIGENCIA ARTIFICIAL 22

ANEXO A.2.1. REQUISITOS NORMATIVOS 22

ANEXO A.2.2. RECOMENDACIONES DE CONTENIDO 23

ANEXO B. EJEMPLO DE POLÍTICA DE SEGURIDAD 26

ANEXO C. HERRAMIENTAS PARA IMPLEMENTAR LA POLÍTICA 32

1 INTRODUCCIÓN

1. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares. Se espera que cada organización las particularice para adaptarlas a su entorno singular.
2. La Política de Seguridad de la Información se define en el glosario del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) como el conjunto de directrices plasmadas en un documento que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.
3. El ENS establece una serie de directrices relacionadas con la Política de Seguridad de la Información, las cuales se desarrollan con detalle en el punto 2 REQUISITOS NORMATIVOS que deberán ser tenidos en cuenta en el desarrollo de la Política. Asimismo, deberán considerarse, cuando resulten aplicables, las obligaciones derivadas de otros marcos normativos europeos y nacionales, transversales y sectoriales, en materias tales como protección de datos personales, ciberseguridad, inteligencia artificial, resiliencia operativa digital, resiliencia de entidades críticas o información clasificada.
4. La Política de Seguridad de la Información debe dar respuesta a las necesidades de la entidad de disponer de un modelo de gobernanza de la seguridad que defina de forma clara las responsabilidades, funciones y mecanismos de toma de decisiones en materia de seguridad. Asimismo, debe proporcionar un marco que permita a la organización adaptarse de manera continua a un entorno tecnológico en constante evolución, caracterizado por la aparición de nuevas tecnologías, cambios normativos y amenazas cada vez más sofisticadas.
5. En este documento se emplean las denominaciones «Política de Seguridad» y «Política de Seguridad de la Información» como términos equivalentes, excepto en aquellos lugares en donde se manifieste explícitamente alguna diferencia.
6. En esta Guía se emplea el término «entidad» para hacer referencia a las entidades del sector público comprendidas en el artículo 2 del Real Decreto 311/2022, de 3 de mayo, y a las entidades del sector privado en los supuestos previstos en su artículo 2.3. La aplicación a contratistas y a su cadena de suministro se determinará conforme a dicho precepto y al análisis de riesgos correspondiente.
7. Además del contenido de esta Guía, los sistemas de información de las organizaciones que manejan información clasificada deberán tener en cuenta las Guías específicas publicadas como la CCN-STIC 201 en relación con el modelo de gobernanza.
8. Esta guía ofrece pautas para elaborar una Política de Seguridad de la Información, sin imponer una metodología única.

a. Se establecen una serie de directrices generales para su elaboración en el punto 3 PAUTAS GENERALES PARA LA ELABORACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

b. Se establecen directrices específicas a tener en cuenta en cada uno de los puntos de la Política de Seguridad de la Información en el apartado 4 RECOMENDACIONES DE CONTENIDO.

c. Se ofrece un modelo general de política de seguridad en el Anexo B EJEMPLO DE POLÍTICA DE SEGURIDAD, sin perjuicio de que puedan existir especialidades en los diferentes perfiles de cumplimiento específico (PCE) publicados por el CCN.

9. La Política podrá integrarse con otras como las relacionadas con el cumplimiento de la Directiva NIS2 o el RGPD o aquellas derivadas del despliegue de la inteligencia artificial en la entidad, debiendo, en todo caso, respetar los requisitos exigibles del ENS y considerar las guías y criterios técnicos publicados por el CCN, de acuerdo con su naturaleza y alcance. Los aspectos a tener en cuenta en caso de que resulten de aplicación otros ámbitos normativos se establecen en el Anexo A MARCOS NORMATIVOS A INTEGRAR.

2 REQUISITOS NORMATIVOS

10. El ENS se refiere en varios puntos a la Política de Seguridad, a saber:

11. La aprobación de la política se regula en el artículo 12.2 y siguientes del ENS para las entidades del sector público. Por su parte, el artículo 2.3 exige que, en las entidades privadas a las que resulte aplicable el ENS, la aprobación corresponda al órgano que ostente las máximas competencias ejecutivas. El artículo 12 dispone, para el sector público, lo siguiente:

«2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente.

No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización.

3. En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento. Los organismos públicos y entidades pertenecientes al sector público institucional estatal podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del Departamento con el que mantenga la relación de vinculación, dependencia o adscripción, o bien quedar comprendidos en el ámbito subjetivo de la política de seguridad de este. También

podrán contar con su propia política de seguridad, aprobada por el órgano competente, coherente con la del Departamento del que dependan o al que estén adscritos, los centros directivos de la propia Administración General del Estado que gestionen servicios bajo la declaración de servicios compartidos.

4. La Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital dispondrá de su propia política de seguridad, que será aprobada por la persona titular de la misma.

5. Los municipios podrán disponer de una política de seguridad común elaborada por la entidad local comarcal o provincial que asuma la responsabilidad de la seguridad de la información de los sistemas municipales».

12. Por otra parte, el artículo 2.3 del ENS extiende expresamente a las entidades privadas comprendidas en su ámbito de aplicación la obligación de contar con una política de seguridad, en los siguientes términos:

    «Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas».

13. También se hace referencia a la Política como documento donde la entidad debe definir las responsabilidades de los diferentes roles del ENS en la entidad, así el artículo 11 sobre la diferenciación de responsabilidades señala que:

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

14. El contenido concreto de la Política de Seguridad se desarrolla en el capítulo III y, en concreto, en el artículo 12:

    «1. La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

    a) Los objetivos o misión de la organización.

    b) El marco regulatorio en el que se desarrollarán las actividades.

    c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.

    d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.

    e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

f) Los riesgos que se derivan del tratamiento de los datos personales. (…)

6. La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad.

h) Mínimo privilegio.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de la actividad y detección de código dañino.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

ñ) Mejora continua del proceso de seguridad.

7. Los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos».

15. La Política de Seguridad establece el marco para el resto de los desarrollos normativos, por lo que debe tener en cuenta los siguientes principios básicos establecidos en el ENS:

- Artículo 5. Principios básicos del Esquema Nacional de Seguridad.
- Artículo 6. La seguridad como un proceso integral.
- Artículo 7. Gestión de la seguridad basada en los riesgos.
- Artículo 8. Prevención, detección, respuesta y conservación.
- Artículo 9. Existencia de líneas de defensa.
- Artículo 10. Vigilancia continua y reevaluación periódica.
- Artículo 11. Diferenciación de responsabilidades.

16. El artículo 13.2 del ENS exige que la política de seguridad sea conocida por todas las personas que formen parte de la organización e identifique inequívocamente a los responsables de su cumplimiento. Este precepto no establece, por sí solo, una obligación general de publicación externa de la política:

    «2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones (…)»

17. También se hace referencia a la Política en el Anexo II Medidas de Seguridad del ENS en referencia al Marco organizativo [org]

    Política de seguridad [org.1]

    «La política de seguridad, que se aprobará de conformidad con lo dispuesto en el artículo 12 de este Real Decreto, se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente:

    [org.1.1] Los objetivos o misión de la organización.

    [org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades.

    [org.1.3] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

    [org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.

    [org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

    Aplicación de la medida. - - -

    Categoría BÁSICA: org.1.

    Categoría MEDIA: org.1.

    Categoría ALTA: org.1.»

18. También se hace referencia en otros apartados como:

    «a. [op.acc.6.1] Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten».

    «b. [mp.info.2.2] La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema».

    «c. [mp.info.2.3] La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad

requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I».

«d. ANEXO III. 1. Objeto de la auditoría, apartado 1.1 a) Que la política de seguridad define los roles y funciones de los responsables del sistema, la información, los servicios y la seguridad del sistema de información».

19. En caso de que en la Política de Seguridad de la Información se desee tener en cuenta otros ámbitos normativos europeos y/o nacionales, tanto de carácter transversal como sectorial, en materias tales como protección de datos personales, ciberseguridad, inteligencia artificial, resiliencia operativa digital, resiliencia de entidades críticas o información clasificada deberán tenerse en cuenta los aspectos descritos en el Anexo A MARCOS NORMATIVOS A INTEGRAR que puedan resultar de aplicación.

3 PAUTAS GENERALES PARA LA ELABORACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

20. Además del modelo general de esta Guía podrá encontrar modelos por sectores en los diferentes perfiles de cumplimiento publicados, sin perjuicio de que pueda recurrir a servicios profesionales expertos. La Política podrá integrar otros compromisos de la entidad derivados de otra normativa relacionada con la seguridad de la información, como los sistemas que gestionan información clasificada, la de protección de datos, inteligencia artificial o ciberseguridad (NIS2), atendiendo a las especialidades de la consideración de cada entidad como esencial o importante, siempre que, en todo caso, se respeten los requisitos recogidos en el ENS y en esta Guía.

21. También podrán incluirse referencias al desarrollo o utilización de los sistemas de inteligencia artificial por parte de los desarrolladores, proveedores, importadores o responsables de despliegue, cuando el contenido sea compatible, de acuerdo con el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial u otras normas de desarrollo de este.

22. El texto se redactará en un lenguaje claro y será accesible a las diferentes personas.

23. El texto de la Política debe respetar los principios de neutralidad tecnológica (evitando las referencias a soluciones tecnológicas concretas), adaptabilidad al proceso tecnológico, pudiendo referenciarse otros contenidos en las Leyes 39/2015 y 40/2015 como accesibilidad, facilidad de uso, interoperabilidad.

24. La Política deberá ser objeto de revisión y adaptación continuada, siguiendo el procedimiento descrito en la misma. Con carácter general, serán adaptaciones a modificaciones normativas que le afecten o los ajustes necesarios ante la detección de incongruencias o ineficiencias en el funcionamiento de la entidad. Para evitar modificaciones reiteradas por cambios normativos se evitará la trascripción literal de artículos y el marco normativo se incorporará como un anexo.

4 RECOMENDACIONES DE CONTENIDO

25. Secciones típicas de una Política de Seguridad de la Información:
    1. Objeto y ámbito de aplicación (obligatorio).
    2. Misión y fines de la entidad (obligatorio).
    3. Marco normativo (obligatorio).
    4. Principios de seguridad (obligatorio).
    5. Organización de seguridad (obligatorio).
        - Definición de comités, grupos de trabajo y su funcionamiento.
        - Identificación y designación de roles.
        - Funciones y responsabilidades.
        - Mecanismos de coordinación.
        - Procedimientos de designación y renovación.
    6. Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso (obligatorio).
    7. Concienciación y formación (recomendable).
    8. Gestión de riesgos y mejora continua (obligatorio parcial[1]).
    9. Gestión del personal y profesionalidad (recomendable).
    10. Relaciones con terceros (recomendable).
    11. Auditorias (recomendable).
    12. Resolución de conflictos (recomendable).
    13. Revisión y actualización (recomendable).
    14. Sanciones por incumplimiento (recomendable).
26. El contenido de cada uno de los puntos dependerá del tipo de entidad y del marco normativo aplicable. En caso de que se deseen tener en cuenta otros ámbitos normativos dentro del alcance de la Política de Seguridad de la Información en materias tales como protección de datos personales, ciberseguridad, inteligencia artificial, resiliencia operativa digital, resiliencia de entidades críticas o información clasificada deberán tenerse en cuenta los aspectos descritos en el Anexo A MARCOS NORMATIVOS A INTEGRAR.

[1] Art. 12.1.f) Los riesgos que se derivan del tratamiento de los datos personales.

4.1 OBJETO Y ÁMBITO DE APLICACIÓN

27. La definición del objeto de la Política de Seguridad de la Información debe estar alineada con la misión y fines de la entidad.

28. Para la correcta definición del ámbito de aplicación es necesario delimitar con claridad qué pretende regular la política, qué activos, procesos, servicios, sistemas de información, instalaciones y personas quedan sujetos a sus disposiciones, y cuál es su alcance dentro de la organización. Una correcta definición evita incertidumbres sobre su aplicación, facilita la asignación de responsabilidades y contribuye a garantizar un marco de seguridad coherente y alineado con las necesidades de la organización.

4.2 MISIÓN Y FINES DE LA ENTIDAD.

29. Se describirá la razón de la existencia de la entidad, así como sus fines.

30. La Política de Seguridad de la Información debe estar plenamente alineada con la misión, los fines y los objetivos estratégicos de la organización, de manera que la seguridad actúe como un elemento habilitador de la actividad y contribuya a la prestación eficaz de los servicios. Esta alineación garantiza que las decisiones y medidas de seguridad se adopten en función de las necesidades del negocio, los riesgos existentes y el valor de la información que soporta el cumplimiento de la misión organizativa.

4.3 MARCO NORMATIVO.

31. El objetivo es plasmar por escrito las responsabilidades que la entidad pueda tener por su naturaleza legal, por su obligación a atender normativa nacional o sectorial y por obligaciones contraídas con terceros, con indicación de las normas correspondientes.

32. La Política de Seguridad de la Información no necesariamente debe incorporar un listado exhaustivo de toda la normativa, regulaciones y obligaciones aplicables a la organización, ya que dicho conjunto puede variar con el tiempo y requerir actualizaciones frecuentes. No obstante, al menos, se deben identificar los principales ámbitos normativos que resultan de aplicación y reflejar el compromiso de la organización de mantener un registro o inventario de requisitos legales, regulatorios y contractuales permanentemente actualizado, que sirva de referencia para garantizar el cumplimiento y la adecuación continua de las medidas de seguridad.

4.4 PRINCIPIOS DE SEGURIDAD.

33. La Política de Seguridad de la Información debe reflejar el compromiso de la organización con el cumplimiento de los principios y requisitos mínimos establecidos en el ENS, así como de los distintos marcos normativos que puedan resultar de aplicación. También debe recogerse el compromiso de que van a ser desarrollados e

implementados a través de la Política de Seguridad de la Información y su desarrollo normativo.

34. No es necesario incorporar una relación exhaustiva de todos los principios y requisitos mínimos, ni desarrollar el detalle de todos ellos.

4.5 ORGANIZACIÓN DE SEGURIDAD.

35. Se describirá el modelo de gobernanza elegido por la organización, teniendo en cuenta el artículo 11 del ENS, las orientaciones de la Guía CCN-STIC 801 y, cuando proceda, los modelos previstos en perfiles de cumplimiento específico o en la Guía CCN-STIC 201 para entidades que manejan información clasificada.
36. También, en el caso de que la Política se integre con otras, se deberán indicar los roles y la forma de coordinarse entre ellos o de cómo gestionar los posibles conflictos y las causas de incompatibilidad en las designaciones que se realicen.
37. Se debe describir cómo se coordina la entidad para atender a las necesidades de seguridad en sus sistemas de información, tanto TIC como en otras materias y cómo se distribuye la información y se toman decisiones corporativas.
38. Se deben describir aquellos roles unipersonales y órganos colegiados, detallando su composición, funcionamiento y funciones, en materia de seguridad de la información. En los términos del artículo 11 del ENS, deberán diferenciarse los siguientes responsables:
    a. Responsable de Información.
    b. Responsable de Servicio.
    c. Responsable de la Seguridad.
    d. Responsable de Sistema.

    En caso de no realizar la designación del puesto en la Política de Seguridad de la Información, deberán definirse los procedimientos de designación y renovación, de acuerdo con el artículo 12.1.c) del ENS.
39. En caso de establecer Comités y/o grupos de trabajo deberá establecerse para cada uno de ellos al menos:
    a. Integrantes.
    b. Funciones.
    c. Funcionamiento.
40. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección y actúe en los términos del artículo 13.5 del ENS, sin perjuicio de la responsabilidad última de la entidad pública destinataria del servicio.

4.6 DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA, SU GESTIÓN Y ACCESO.

41. La Política de Seguridad de la Información debe establecer la estructura y los niveles de desarrollo normativo que conforman el marco documental de seguridad de la organización, definiendo la jerarquía y relación entre la propia política, las normas de seguridad, los procedimientos, las instrucciones técnicas y demás documentos que resulten necesarios para su implantación. Esta definición facilita una aplicación homogénea de los requisitos de seguridad, asegura la coherencia entre los distintos documentos y permite adaptar las medidas y directrices a las necesidades operativas de la organización, garantizando al mismo tiempo una adecuada gobernanza, mantenimiento y actualización del marco normativo de seguridad conforme a los principios y requisitos del ENS.
42. La Política de Seguridad de la Información debe definir claramente las responsabilidades asociadas a cada nivel de desarrollo normativo, estableciendo qué órganos o responsables tienen la competencia para elaborar, revisar, aprobar, mantener y actualizar la política, las normas, los procedimientos y el resto de la documentación de seguridad. Esta asignación de responsabilidades contribuye a reforzar la gobernanza de la seguridad, garantiza la adecuada supervisión y control del marco normativo y asegura que cada documento sea aprobado por el nivel organizativo con la autoridad y capacidad de decisión acordes a su alcance e impacto dentro de la organización.

4.7 CONCIENCIACIÓN Y FORMACIÓN.

43. Debe recoger el compromiso de la organización de promover programas continuos de formación y acciones de concienciación adaptadas a los distintos perfiles y riesgos existentes, asegurando el mantenimiento y actualización de las competencias necesarias para desempeñar sus funciones de forma segura.

4.8 GESTIÓN DE RIESGOS Y MEJORA CONTINUA.

44. Debe reflejar el compromiso de la organización con la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar a la información, los servicios y los sistemas de información.
45. Debe determinarse el marco general para la revisión periódica de los riesgos, la supervisión de la eficacia de las medidas de seguridad implantadas, el seguimiento de incidentes, vulnerabilidades y desviaciones detectadas, así como la adopción de acciones correctivas y de mejora.
46. Debe describirse el procedimiento de aceptación del riesgo residual, precisando las responsabilidades y la competencia decisoria de los responsables de la información y de los servicios afectados.
47. Compromiso de la organización de mantener actualizado el análisis de riesgos en función de los cambios que puedan producirse en el entorno, las amenazas, la

tecnología y los requisitos legales y organizativos, en línea con los principios y exigencias del ENS.

4.9 GESTIÓN DEL PERSONAL Y PROFESIONALIDAD.

48. Garantizar que todas las personas con acceso a la información, a los sistemas o a los servicios de la organización dispongan de las competencias, conocimientos y nivel de concienciación adecuados para desempeñar sus funciones de forma segura.
49. Asimismo, debe definir el compromiso de la organización con la selección, asignación de responsabilidades, formación, capacitación y actualización continua del personal, así como con la aplicación de las medidas necesarias para asegurar el cumplimiento de las obligaciones de seguridad durante todo el ciclo de vida de la relación profesional.
50. De este modo, se contribuye a reducir los riesgos derivados del factor humano, fortalecer la cultura de seguridad y asegurar la disponibilidad de personal cualificado para la protección eficaz de la información y de los servicios, conforme a los principios y requisitos del ENS.

4.10 RELACIONES CON TERCEROS.

51. Se debe incorporar el compromiso de la organización de establecer los requisitos de seguridad en los procesos de contratación.
52. Se deben incorporar los mecanismos de comunicación necesarios en caso de que no sea posible el cumplimiento de alguno de dichos requisitos por parte del proveedor, entre los que debe encontrarse la definición de un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información.

4.11 AUDITORIAS.

53. Se deben establecer los principios y directrices generales que aseguren una evaluación independiente que verifique de forma periódica el grado de cumplimiento de los requisitos de seguridad, las obligaciones legales y reglamentarias aplicables, así como de las medidas establecidas en el ENS.
54. Se debe reflejar la función de auditoría dentro del modelo de gobernanza de la organización, garantizando la independencia exigible de acuerdo con el ENS y, en su caso, con el modelo de líneas de defensa adoptado.

4.12 RESOLUCIÓN DE CONFLICTOS.

55. Se deben establecer las vías que se estiman oportunas para la resolución de conflictos que puedan surgir de la aplicación de la Política de Seguridad de la Información y su marco normativo de desarrollo.

56. Se debe asegurar que las discrepancias pueden ser evaluadas y resueltas a través de un proceso objetivo, documentado y alineado con los objetivos de la organización.

4.13 REVISIÓN Y ACTUALIZACIÓN.

57. Se deben establecer los mecanismos de revisión y actualización oportunos para la propia Política de Seguridad de la Información.

4.14 SANCIONES POR INCUMPLIMIENTO.

58. Se recomienda referenciar aquellos mecanismos a activar en caso de incumplimiento de la Política de Seguridad de la Información y su desarrollo normativo.

Anexo A. MARCOS NORMATIVOS A INTEGRAR

Anexo A.1. PROTECCIÓN DE DATOS PERSONALES

Anexo A.1.1. Requisitos normativos

El artículo 3 del ENS establece que para aquellos sistemas de información que traten datos personales y les resulte de aplicación el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018 (LOPDGDD) o la Ley Orgánica 7/2021, según corresponda, se deberá:

> *«2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.*
>
> *3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.»*

El artículo 5 del RGPD recoge los principios relativos al tratamiento de datos personales:

> *«1. Los datos personales serán:*
>
> *a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);*
>
> *b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);*
>
> *c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);*
>
> *d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);*
>
> *e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);*

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).»

El artículo 32 del RGPD establece la necesidad de asegurar la seguridad del tratamiento:

«1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.»

La disposición adicional primera de la Ley Orgánica 3/2018, sobre medidas de seguridad en el ámbito del sector público, establece que:

«1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.»

El artículo 35.1 del RGPD establece cuándo debe realizarse una evaluación de impacto relativa a la protección de datos:

«1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.»

El artículo 37 del RGPD establece la necesidad de designar un DPD en los siguientes supuestos:

«1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:
a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Anexo A.1.2. Recomendaciones de contenido

Apartado	Contenido específico
Objeto y ámbito de aplicación	Revisar y adaptar el objeto de la política para que tenga en cuenta el objeto desde el punto de vista de protección de datos personales. Incluir dentro del ámbito de aplicación de la política, en caso de ser necesario, aquellos activos, procesos, servicios, sistemas de información, instalaciones y personas que dada su actividad quedan sujetos al marco normativo en materia de protección de datos personales.
Misión y fines de la entidad	
Marco normativo	Incluir como ámbito normativo a tener en cuenta la privacidad y protección de datos personales.
Principios de seguridad	Recoger el compromiso de la organización con los principios y requisitos establecidos en la legislación en materia de protección de datos personales, así como el compromiso de que van a ser desarrollados e implementados. Se debe recoger la obligatoriedad de adoptar soluciones que garanticen simultáneamente los principios de seguridad de la información y los de protección de datos personales.
Organización de seguridad	Se debe recoger el modelo de gobernanza elegido por la organización siguiendo las directrices marcadas en la Guía CCN-STIC 801 en materia de protección de datos personales (Comités, grupos de trabajos, roles, funciones, etc.). Las posiciones jurídicas que, según los tratamientos realizados, pueden corresponder a la entidad son: • Responsable de Tratamiento: identificar en la entidad quién desarrolla dichas responsabilidades. • Encargado de Tratamiento: identificar en la entidad quién desarrolla dichas responsabilidades. • Corresponsable de Tratamiento: identificar en la entidad quién desarrolla dichas responsabilidades. La política debe recoger si la entidad desarrolla alguno de dichos actores y a alto nivel en que situaciones los desarrolla. Por otro lado, la política también podría recoger, en su modelo de gobernanza, que roles dentro de la organización desarrollan las actividades asociadas a las responsabilidades de la entidad.

Apartado	Contenido específico
	Cuando proceda la designación de un delegado de protección de datos (artículos 37 a 39 del RGPD), se indicarán sus funciones y mecanismos de coordinación, respetando su independencia funcional.
Estructuración de la documentación	En caso de considerarse necesario, tener en cuenta las particularidades de la documentación necesaria en materia de protección de datos personales como puedan ser políticas, normas, modelos o procedimientos.
Concienciación y formación	Se debe recoger la necesidad de incluir los aspectos necesarios en materias de protección de datos personales.
Gestión de riesgos y mejora continua	Incluir los riesgos derivados del tratamiento de datos personales y gestionarlos desde un punto de vista integral. Tener en cuenta el rol del Delegado de Protección de Datos dentro de la gestión de riesgos.
Gestión de personal y profesionalidad	Incluir aquellos conocimientos y/o experiencia necesaria desde el punto de vista de protección de datos dentro de la gestión del personal y profesionalidad.
Relaciones con terceros	Incluir las responsabilidades oportunas de comunicación con entidades externas desde el punto de vista de protección de datos personales como puedan ser los organismos de control o a entidades a las que se presten servicios que incluyan el tratamiento de datos personales. En el caso de entidades que presten sus servicios a la organización que desarrolla la política incluir aquellos requisitos relativos a protección de datos personales como Encargadas de Tratamiento, así como establecer los canales de comunicación adecuados de asesoramiento con el DPD.
Auditorias	Incluir los aspectos relativos de protección de datos dentro del alcance de las labores de auditoría garantizando su independencia, tal y como se recoge en la guía CCN STIC 801. Tener en cuenta la función de supervisión del DPD dentro del proceso de auditoría.
Resolución de conflictos	Tener en cuenta dentro de los mecanismos de gestión de conflictos aquellos roles necesarios desde el punto de vista de protección de datos.
Revisión y actualización	En caso de ser necesario, tener en cuenta los requisitos de revisión y actualización necesarios desde el punto de vista de protección de datos personales.

Apartado	Contenido específico
Sanciones por incumplimiento	En caso de ser necesario, particularizar los mecanismos a activar en caso de incumplimientos en materia de protección de datos personales.

Tabla 1 Recomendaciones de contenido protección de datos personales

Anexo A.2. INTELIGENCIA ARTIFICIAL

Anexo A.2.1. Requisitos normativos

El artículo 17.1 del Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial, RIA) dispone que los proveedores de sistemas de IA de alto riesgo deben establecer:

> *"1. Los proveedores de sistemas de IA de alto riesgo establecerán un sistema de gestión de la calidad que garantice el cumplimiento del presente Reglamento. Dicho sistema deberá consignarse de manera sistemática y ordenada en documentación en la que se recojan las políticas, los procedimientos y las instrucciones e incluirá, al menos, los siguientes aspectos:"*

El anexo XI, sección 1, punto 1.b), del RIA recoge, entre los elementos de la documentación técnica exigida a los proveedores de modelos de IA de uso general, el siguiente:

> *"b) las políticas de usos aceptables aplicables;"*

El artículo 15, apartados 1 y 5, del RIA establece la necesidad de implementar medidas de seguridad adecuadas:

> *"1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera uniforme en esos sentidos durante todo su ciclo de vida.*
>
> *….*
>
> *La solidez de los sistemas de IA de alto riesgo puede lograrse mediante soluciones de redundancia técnica, tales como copias de seguridad o planes de prevención contra fallos.*
>
> *…..*
>
> *5. Los sistemas de IA de alto riesgo serán resistentes a los intentos de terceros no autorizados de alterar su uso, sus resultados de salida o su funcionamiento aprovechando las vulnerabilidades del sistema.*
>
> *Las soluciones técnicas encaminadas a garantizar la ciberseguridad de los sistemas de IA de alto riesgo serán adecuadas a las circunstancias y los riesgos pertinentes.*
>
> *Entre las soluciones técnicas destinadas a subsanar vulnerabilidades específicas de la IA figurarán, según corresponda, medidas para prevenir, detectar, combatir, resolver y controlar los ataques que traten de manipular el conjunto de datos de entrenamiento («envenenamiento de datos»), o los componentes entrenados previamente utilizados en el entrenamiento («envenenamiento de modelos»), la información de entrada diseñada para hacer que el modelo de IA cometa un error («ejemplos adversarios» o «evasión de modelos»), los ataques a la confidencialidad o los defectos en el modelo."*

Anexo A.2.2. Recomendaciones de contenido

Apartado	Contenido específico
Objeto y ámbito de aplicación	Revisar y adaptar el objeto de la política para que tenga en cuenta el objeto desde el punto de vista de los sistemas IA. Incluir dentro del ámbito de aplicación de la política, en caso de ser necesario, aquellos activos, procesos, servicios, sistemas de información, instalaciones y personas que dada su actividad quedan sujetos al marco normativo en materia de sistemas de inteligencia artificial. Analizar e incluir el rol o roles de la entidad desde el punto de vista del RIA. En caso de actuar como Responsables de Despliegue deberán tenerse en cuenta las indicaciones de los proveedores.
Misión y fines de la entidad	-
Marco normativo	Incluir como ámbito normativo a tener en cuenta los sistemas de inteligencia artificial.
Principios de seguridad	Recoger el compromiso de la organización con los principios y requisitos establecidos en la legislación en materia de inteligencia artificial, así como el compromiso de que van a ser desarrollados e implementados. Se debe recoger la obligatoriedad de adoptar soluciones que garanticen simultáneamente los principios de seguridad de la información y los de los sistemas de inteligencia artificial.
Organización de seguridad	Se debe recoger el modelo de gobernanza elegido por la organización siguiendo las directrices marcadas en la Guía CCN-STIC 801 en materia de inteligencia artificial, coordinándolas con el modelo de seguridad de la información (comités, grupos de trabajo, roles y funciones). Según la actividad que desarrolle la entidad, se identificarán las posiciones relevantes previstas en el RIA (artículo 3), entre otras: • Proveedor. • Responsable de Despliegue. • Representante autorizado. • Importador. • Operador (término que engloba las posiciones definidas por el RIA, no una función adicional necesariamente diferenciada). • Distribuidor.

Apartado	Contenido específico
	La política debe recoger si la entidad desarrolla alguno de dichos actores y a alto nivel en que situaciones los desarrolla. Por otro lado, la política también podría recoger, en su modelo de gobernanza, que roles dentro de la organización desarrollan las actividades asociadas a las responsabilidades de la entidad.
Estructuración de la documentación	En caso de considerarse necesario, tener en cuenta las particularidades de la documentación necesaria en materia de IA como puedan ser políticas, normas, modelos o procedimientos.
Concienciación y formación	Se debe recoger la necesidad de incluir los aspectos necesarios en materia de sistemas de IA.
Gestión de riesgos y mejora continua	Incluir los riesgos asociados a los sistemas de IA y gestionarlos desde un punto de vista integral. En función del rol o roles desarrollados por la entidad, tener en cuenta el nivel de riesgo asociado a los sistemas IA utilizados.
Gestión de personal y profesionalidad	Incluir aquellos conocimientos y/o experiencia necesaria desde el punto de vista de IA dentro de la gestión del personal y profesionalidad.
Relaciones con terceros	Teniendo en cuenta el rol o roles desarrollados por la entidad dentro del ciclo de vida de sistemas IA: • Incluir las responsabilidades oportunas de comunicación con entidades externas desde el punto de vista de IA como puedan ser los organismos de control o a entidades a las que se presten servicios que incluyan el manejo de IA. • En el caso de entidades que presten sus servicios a la organización que desarrolla la política, se deben incluir aquellos requisitos relativos a los sistemas IA.
Auditorias	Incluir los aspectos relativos de IA dentro del alcance de las labores de auditoría garantizando su independencia, tal y como se recoge en la guía CCN STIC 801. Tener en cuenta la función de supervisión que pueda ser desarrollada en el entorno de IA dentro del modelo de gobernanza y los mecanismos de comunicación.
Resolución de conflictos	Tener en cuenta dentro de los mecanismos de gestión de conflictos aquellos roles necesarios desde el punto de vista de IA.

Apartado	Contenido específico
Revisión y actualización	En caso de ser necesario, tener en cuenta los requisitos de revisión y actualización necesarios desde el punto de vista de IA.
Sanciones por incumplimiento	En caso de ser necesario, particularizar los mecanismos a activar en caso de incumplimientos en materia de IA.

Tabla 2 Recomendaciones de contenido Inteligencia Artificial

Anexo B. EJEMPLO DE POLÍTICA DE SEGURIDAD[2]

1. Objeto y ámbito de aplicación (obligatorio).

   La presente Política de Seguridad de la Información tiene por objeto establecer los principios, directrices y responsabilidades necesarias para garantizar la protección de la información y de los servicios que la soportan, preservando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Asimismo, proporciona el marco de referencia para la gestión de la seguridad de la información en la organización, promoviendo el cumplimiento de los requisitos legales, normativos y operativos aplicables, así como la gestión continua de los riesgos que puedan afectar al logro de sus objetivos.

   Esta política se aplica a los sistemas de información comprendidos en su ámbito, al personal de <entidad> y a los prestadores de servicios y proveedores respecto de las obligaciones de seguridad que les resulten aplicables en virtud del ENS, de sus contratos y de la normativa correspondiente.

2. Misión y fines de la entidad (obligatorio).

   Describir los objetivos de servicio de <entidad> (funciones que desarrolla, servicios que presta).

3. Marco normativo (obligatorio).

   Las principales normas que afectan a esta Política son:

   - Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
   - (además de todas aquellas que conforman el marco legal de actuación de la entidad).

   NOTA: La entidad identificará las disposiciones legales, reglamentarias y obligaciones contractuales que resulten aplicables a sus funciones y servicios. La relación pormenorizada podrá mantenerse en un anexo o inventario normativo actualizado.

4. Principios de seguridad (obligatorio).

   - Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente
   - Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la

[2] La propuesta de política se asume la existencia de un comité de seguridad alineado con lo especificado en la Guía CCN STIC 801, en caso de no existir ese comité se debería modificar la redacción indicando la figura u órgano que realizaría dicha función.

información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

- Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.
- Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, dando una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.
- Existencia de líneas de defensa, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.
- Vigilancia continua y reevaluación periódica: la entidad implementará medios para detectar actividades o comportamientos anómalos y responder a ellos, así como mecanismos de evaluación continua del estado de seguridad de los activos. Existirá, además, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- Diferenciación de responsabilidades, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

5. Organización de seguridad (obligatorio).

NOTA: este apartado puede completarse en estructura de mayor tamaño con otros roles vinculados a la ciberseguridad descritos en otras normas, Guías o recomendaciones publicadas.

5.1. Definición de comités, grupos de trabajo y su funcionamiento.

El Comité de Seguridad de la Información estará formado por <…>. NOTA: Aquí aparecen cargos corporativos y designaciones de departamentos dentro de la entidad, cuando proceda.

El Secretario del Comité de Seguridad de la Información será <…> y tendrá como funciones <…>.

El Comité de Seguridad de la Información reportará a <…>.

El Comité de Seguridad de la Información tendrá las siguientes funciones: <…>.

NOTA: desarrollar el funcionamiento del Comité de Seguridad de la Información.

NOTA: desarrollar estructura análoga en caso de que existan grupos de trabajo.

5.2. Identificación y designación de roles y funciones asociadas.

NOTA: cada entidad debe detallar los puestos o perfiles de puestos de cada responsable y las principales funciones a desarrollar. Como mínimo, se identificarán los responsables de la información, del servicio, de la seguridad y del sistema, detallando sus funciones y los procedimientos de designación y renovación, de acuerdo con los artículos 11 y 12.1.c) del ENS.

5.3. Mecanismos de coordinación.

NOTA: cada entidad debe detallar los mecanismos de coordinación establecidos entre los distintos actores participantes en la organización de la seguridad.

6. Procedimientos de designación y renovación.

NOTA: en caso de que los distintos roles o responsables no hayan sido identificados orgánicamente en la política deberá especificarse el procedimiento de designación y renovación a seguir en la organización. Pueden especificarse aspectos como la periodicidad de revisión de los nombramientos, mecanismos de sustitución en casos de indisponibilidad.

7. Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso (obligatorio).

NOTA: cada entidad debe detallar la estructura documental de su marco normativo, así como los responsables de su desarrollo y aprobación. También se deben especificar las obligaciones del personal sobre el conocimiento y cumplimiento de la misma.

8. Concienciación y formación (recomendable).

<entidad> promoverá un programa continuo de concienciación y formación en seguridad de la información, adecuado a las funciones y responsabilidades del personal, con el fin de garantizar el conocimiento y cumplimiento de las normas, procedimientos y buenas prácticas aplicables, fomentando una cultura de seguridad que contribuya a la protección de la información y a la reducción de los riesgos de seguridad.

9. Gestión de riesgos y mejora continua (obligatorio parcial).

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios en la información manejada.
- Cuando se produzcan cambios en los servicios prestados.

- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

10. Gestión del personal y profesionalidad (recomendable).

    Todos los miembros de <entidad> tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad de la <entidad> a través del Comité de Seguridad y del área de personal de disponer los medios necesarios para que la información llegue a los afectados.

    Todos los miembros de <entidad> atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de <entidad>, en particular a los de nueva incorporación.

    Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11. Relaciones con terceros (recomendable).

    Cuando <entidad> preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

    Cuando <entidad> utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de soluciones se concretarán los requisitos de conformidad con el ENS que resulten aplicables conforme a su artículo 2.3 y al alcance del contrato.

En la contratación de servicios en la nube se tendrán en cuenta las medidas aplicables del anexo II del ENS y las guías técnicas correspondientes.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que la <entidad> pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al órgano competente para decidir sobre la contratación y, en su caso, aceptar expresamente los riesgos residuales dentro de sus atribuciones. Esta aceptación no dispensa del cumplimiento de requisitos legales o de seguridad preceptivos.

12. Auditorias (recomendable).

    <entidad> realizará auditorías y revisiones periódicas de la seguridad de la información, con el fin de verificar el cumplimiento de la normativa aplicable, las políticas internas y los controles de seguridad establecidos, identificar oportunidades de mejora y contribuir al mantenimiento de un nivel adecuado de protección de la información y de los servicios que la soportan. Las auditorías de conformidad con el ENS se realizarán con el alcance, la periodicidad y las garantías de independencia establecidos en su artículo 31 y en el anexo III, cuando resulten aplicables.

13. Resolución de conflictos (recomendable).

    En el caso de conflictos entre los diferentes responsables, el Comité de Seguridad de la Información podrá dirimir las discrepancias (NOTA: se podrán establecer peculiaridades en la resolución de conflictos según las especialidades regulatorias de cada entidad).

14. Revisión y actualización (recomendable).

    El Comité de Seguridad de la Información promoverá la revisión anual de esta Política y elevará al órgano competente las propuestas de modificación que considere necesarias. Cualquier modificación de la Política deberá ser formalmente aprobada por el órgano competente, conforme al artículo 12 del ENS.

    En particular, los cambios en los principios, el ámbito de aplicación, la estructura de gobernanza o las responsabilidades requerirán la aprobación del órgano competente y su comunicación a las personas afectadas.

La sustitución de la Política será propuesta por el Comité de Seguridad de la Información y aprobada por la persona u órgano competente, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.

15. Sanciones por incumplimiento (recomendable).

    El incumplimiento de esta Política podrá dar lugar, en su caso, a las medidas disciplinarias, laborales o contractuales que procedan conforme al régimen jurídico aplicable, con observancia de los procedimientos y garantías correspondientes. La Política no podrá crear por sí misma infracciones o sanciones no previstas en las normas aplicables.

16. APROBACIÓN Y ENTRADA EN VIGOR

    Texto aprobado el día <día> de <mes> de <año> por <órgano que la aprueba>.

    Esta Política de Seguridad de la Información está vigente desde la fecha de aprobación (o publicación para las entidades que sea obligatoria su publicación oficial) y hasta que sea reemplazada por una nueva Política.

    Este texto deroga al anterior, que fue aprobado el día <día> de <mes> de <año> por <órgano que lo aprobó>.

Anexo C. HERRAMIENTAS PARA IMPLEMENTAR LA POLÍTICA

Tomado de la GUÍA NIST SP 800-100 (Information Security Handbook: A Guide for Managers).

Dado que la Política de Seguridad está escrita a un nivel muy amplio, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto. Para ello se utilizan otros instrumentos que reciben diferentes nombres, siendo comunes los siguientes:

- Normas de seguridad (*security standards*) que en el ámbito de la administración pública se podrán equiparar a instrucciones de servicio.
- Guías de seguridad (*security guides*).
- Procedimientos de seguridad (*security procedures*).

Las normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

Las guías tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

Los procedimientos (operativos) de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Las organizaciones no siempre separan nítidamente estos diferentes tipos de herramientas, sino que a veces se generan manuales y reglamentos de seguridad que tienen un poco de todos los elementos anteriormente mencionados, buscando siempre una mayor efectividad en la concienciación y formación de los usuarios del sistema.

Si bien los manuales y reglamentos de carácter mixto pueden servir como herramientas importantes, a menudo es útil distinguir claramente entre lo que es política (abstracta) y su aplicación concreta. De esta forma se es más flexible y se consigue una cierta uniformidad de resultados incluso cuando cambia la tecnología o los mecanismos empleados.