# Guía de Seguridad de las TIC
# CCN-STIC 805

# Esquema Nacional de Seguridad
# Política de Seguridad de la Información


Junio 2025

Edita:

centro criptológico nacional



centro criptológico nacional

Firmado digitalmente por CENTRO CRIPTOLOGICO NACIONAL
Fecha: 2025.06.02 08:52:37 +02'00'

Fecha de Edición: junio de 2025

La Agencia Estatal de Administración Digital del Ministerio para la Transformación Digital y de la Función Pública ha participado en la redacción y revisión de este documento.

**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**

# PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Es precisamente el Esquema Nacional de Seguridad el que fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de información de su ámbito de aplicación (entidades del sector público, organizaciones del sector privado prestadores de servicios competenciales a las anteriores, incluyendo su cadena de suministro, así como los sistemas de información que tratan información clasificada), y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Secretaria de Estado
Directora del Centro Criptológico Nacional

# ÍNDICE

# 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. 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.
4. En esta Guía se emplea el término "entidad" para hacer referencia tanto a entidades públicas como privadas que, como prestadores de servicios o de suministros de las anteriores, se encuentran dentro del ámbito de aplicación del ENS y deben tener aprobada una Política de Seguridad, según el ámbito de aplicación del artículo 2 del antedicho Real Decreto 311/2022, de 3 de mayo.
5. 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.
6. El ENS se refiere en varios puntos a la Política de Seguridad, a saber:

   La política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas. En concreto, este artículo indica que: *"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.*

7. Por otro lado, en el artículo 2 del ENS, se incorpora la obligatoriedad de que los prestadores de servicios en el ámbito de aplicación del ENS cuenten también con una Política, así indica que: "*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".*
8. También se hace referencia a la Política como documento donde la entidad debe definir las responsabilidades de los diferentes roles el 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*."
9. 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".*

10. En el artículo 13 del ENS se hace referencia a la necesidad de dar publicidad a la Política de Seguridad, al objeto de que todos los interesados, internos y externos a la organización de que se trate, puedan conocer el alcance del compromiso adquirido y sus responsables:

    *"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 (…)"*

11. 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."*

12. 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.*
13. Esta guía propone un modelo genérico de Política de Seguridad de la Información. El contenido se detalla en la sección 3. La sección 4 da pautas para desarrollar dicho contenido, y el Anexo C muestra un ejemplo que se puede tomar como base para particularizarlo a casos concretos.
14. Además del modelo general del Anexo C, pueden existir especialidades en los diferentes Perfiles de Cumplimiento Específico (PCE) publicados por el CCN.
15. 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 el contenido establecido en el ENS y las recomendaciones o interpretaciones que realice el CCN.

## 2. PRINCIPIOS DE SEGURIDAD

16. En la toma de decisiones en materia de seguridad se deben tener en cuenta los principios básicos enunciados en el Esquema Nacional de Seguridad. Esto es especialmente relevante cuando se elabora la Política de Seguridad de la Información, que establece el marco para el resto de los desarrollos normativos. El ENS establece los siguientes principios básicos:
    - 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.

## 3. CONTENIDO

17. Secciones típicas de una Política de Seguridad de la Información:
    1. Misión u objetivos de la organización.
    2. Principios de la Política
    3. Marco normativo.
    4. Organización de seguridad.
        - Definición de comités y roles unipersonales.
        - Funciones.
        - Responsabilidades.
        - Mecanismos de coordinación
        - Procedimientos de designación de personas
    5. Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
    6. Concienciación y formación.
    7. Gestión de riesgos.

- Plan de análisis.
- Criterios de evaluación de riesgos (metodología).
- Directrices de tratamiento.
- Proceso de aceptación del riesgo residual.
- Integración con el análisis de riesgos en protección de datos.

**8.** Proceso de revisión de la política de seguridad.

18. Estos puntos se desarrollan a continuación.

## 3.1 MISIÓN DE LA ENTIDAD

19. Se describirá la razón de la existencia de <entidad> y los servicios que presta.

## 3.2 MARCO NORMATIVO

20. 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.

## 3.3 ORGANIZACIÓN DE LA SEGURIDAD

21. Se describirá el modelo de gobernanza elegido por la organización, teniendo en cuenta el artículo 11 del ENS. El modelo podrá ser bien el general de la Guía CCN-STIC 801, el modelo básico o extendido de la Guía de Buenas Prácticas en materia de ciberseguridad o de alguno de los perfiles de cumplimiento específico que puedan serle de aplicación o el relacionado con las entidades que gestionan sistemas con información clasificada. La entidad debe elegir el modelo de gobernanza, como una medida más del ENS, de forma motivada.
22. 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.
23. 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.
24. Se deben describir los roles unipersonales y órganos colegiados, detallando su composición y puestos, en materia de seguridad de la información. En particular, se describirá el puesto que corresponde a la figura del Responsable de la Seguridad de la información, detallando sus funciones y responsabilidades.

25. Cuando la entidad trate datos personales y deba designar un Delegado de Protección de Datos, se tendrá en cuenta esta figura entre los roles. Sin perjuicio de otras figuras relacionadas con otra normativa como NIS2 o la relacionada con las infraestructuras críticas o la inteligencia artificial.
26. Cuando la entidad actúe como encargado del tratamiento o contrate con prestadores, incluyendo los relacionados con el uso de la nube, deberá identificar el rol del Punto de Contacto o POC.

## 3.4 DIRECTRICES DE ESTRUCTURACIÓN DOCUMENTAL

27. A grandes rasgos, se definen los instrumentos que se utilizarán para el desarrollo de la Política en la <entidad>.

## 3.5 CONCIENCIACIÓN Y FORMACIÓN

28. El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de <entidad> y a todas las actividades, de acuerdo con el principio de Seguridad como proceso integral recogido en el Artículo 6 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

## 3.6 GESTIÓN DE RIESGOS

29. El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 7 del ENS. De acuerdo con el apartado 1.1 d) del Anexo III del ENS se revisará y aprobará anualmente.
30. En esta sección se debe plasmar el compromiso de <entidad> y la obligación de los responsables de los sistemas de realizar análisis de riesgos atender a sus conclusiones y gestionar los riesgos por encima de umbral asumible acordado por la entidad
31. El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente según lo establecido en el Artículo 10 del ENS.
32. La gestión de riesgos debe contemplar también los derivados de la normativa de protección de datos, contando con el asesoramiento del Delegado de Protección de Datos.

## 3.7 PROCESO DE APROBACIÓN Y REVISIÓN

33. La Política de Seguridad de la Información es un documento que será aprobado formalmente por la Alta Dirección de la Organización u órgano con competencias. La Política se aprobará mediante una resolución o acuerdo que obligará a la entidad tanto internamente como frente a terceros (al afectar la seguridad de la información a los intereses de las penas que se relacionan con dicha entidad), por

lo que deberá ser objeto de publicación, en páginas web, portales de transparencia o boletines oficiales, en función de la normativa sectorial que le sea de aplicación.

34. Así mismo estará sujeto a un proceso de revisión regular que lo adapte a nuevas circunstancias, técnicas u organizativas, y evite que quede obsoleto.

35. Por ello se establecerá un proceso organizativo que asegure que regularmente se revisa la oportunidad, idoneidad, completitud y precisión de lo que la Política establezca y sea sometido a aprobación formal por la Alta Dirección.

36. El proceso de elaboración y aprobación debe explicitarse en la misma Política, sin perjuicio, de que, al tratarse de una aprobación mediante resolución o acuerdo, esté sometida a los trámites establecidos para la aprobación de resoluciones en las entidades dentro del alcance del ENS.

## 4. PAUTAS DE ELABORACIÓN DE LA POLÍTICA DE SEGURIDAD

37. 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.

38. 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.

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

40. 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 y 40 como accesibilidad, facilidad de uso, interoperabilidad.

41. 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.

# 5. ANEXO C. EJEMPLO DE POLÍTICA

## 1. APROBACIÓN Y ENTRADA EN VIGOR

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

Esta Política se 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>.

## 2. INTRODUCCIÓN

<Entidad> depende de los sistemas de información para alcanzar sus objetivos, Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o la disponibilidad de los servicios prestados.

El objetivo último de la seguridad de la información es garantizar que la entidad pueda cumplir con sus objetivos, desarrollar sus funciones o competencias y prestar los servicios para la cual se ha sido constituida la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La <entidad> debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

## 3. ALCANCE

Esta política se aplica a todos los sistemas de información de <entidad> a las personas que conforman la organización y a los prestadores de servicios o proveedores de soluciones TIC de la <entidad>.

## 4. MISIÓN

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

Los objetivos en materia de seguridad que la <entidad> pretende garantizar con la presente Política serán:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes de la <entidad> respecto a la seguridad de la información. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmita a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

## 5. PRINCIPIOS RECTORES DE LA POLÍTICA

- 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 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, danto 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 implementa medios la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, 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.

## 6. MARCO NORMATIVO

Las principales normas que afectan a esta Política[1] 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*).

## 7. ORGANIZACIÓN DE LA SEGURIDAD

*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*

### 6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES [2]

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: <…>.

### 6.2. ROLES: FUNCIONES Y RESPONSABILIDADES[3]

*NOTA: cada entidad debe detallar los puestos o perfiles de puestos de cada responsable y las principales funciones a desarrollar, además de la posible existencia de grupos de trabajo.*

### 6.3. PROCEDIMIENTOS DE DESIGNACIÓN

Los miembros del Comité de Seguridad de la Información serán designados por_____.

El Responsable de la Información será designado a propuesta del Comité de Seguridad por_____ .

El Responsable del Servicio será designado a propuesta del Comité de Seguridad por_____

---

[1] El marco normativo actualizado debe incluir la lista de leyes, reglamentos y otra normativa nacional o internacional que afectan a la entidad incluirán los relacionados con las competencias/funciones de la entidad podrá incluirse en Anexo.

[2] La guía CCN-STIC 801 puede usarse como modelo.

[3] La Guía CCN-STIC 801 puede usarse como modelo, sin perjuicio de las peculiaridades que puedan afectarle en los Perfiles de Cumplimiento Específico.

El Responsable de la Seguridad será designado por_____.

Los nombramientos podrán ser revisados cada dos años, pudiendo realizarse antes cuando el puesto quede vacante o por un incumplimiento reiterado de sus funciones, previo apercibimiento. La <entidad> debe disponer de un mecanismo que permita la sustitución de los responsables designados en caso de ausencias de larga duración o aquellas de menor duración pero que puedan provocar ineficiencias en las funciones de cada uno de ellos que afecten al sistema.

### 6.4 RESOLUCIÓN DE CONFLICTOS

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*).

## 7. TRATAMIENTO DE DATOS PERSONALES EN LA ENTIDAD

<entidad> trata datos de carácter personal, según se describe en el Registro de Actividades del Tratamiento. La <entidad> deberá evaluar los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado

El análisis de riesgos será reevaluado de forma periódica, contando con el asesoramiento y supervisión que realice el Delegado de Protección de Datos, y, en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizar, en su caso, una evaluación de impacto. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales.

## 8. GESTIÓN DE RIESGOS

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.

Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del Delegado de Protección de Datos, además se coordinarán los planes del tratamiento del riesgo.

## 9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa/se integra junto con otras políticas de la <entidad> en diferentes materias:

- *Listar referencias a otras políticas.*

Esta Política se desarrollará por medio de normativa de seguridad que aborde aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la <entidad> que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible por diversos medios a disposición de los usuarios en_____.

## 10. OBLIGACIONES DEL PERSONAL

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.TERCERAS PARTES /PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES

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 productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

En la adquisición de derechos de uso de activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las Guía de desarrollo.

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 y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos. 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 representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

## 12. GESTIÓN DE INCIDENTES DE SEGURIDAD

La <entidad> dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes

enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

### 13. APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR/EFECTIVIDAD

Las modificaciones de la presente Política que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Seguridad de la Información, que deberá revisarla anualmente.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por la persona u órgano con las debidas competencias, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.

## 6. ANEXO D. HERRAMIENTAS PARA IMPLEMENTAR LA POLÍTICA

Tomado de la guía NIST SP 800-100, *An Introduction to Computer Security: The NIST Handbook, October 1995*.

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.