48. SEGURIDAD DE SISTEMAS (2). EL ESQUEMA NACIONAL DE SEGURIDAD. ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD. ESTRATEGIA NACIONAL DE SEGURIDAD. CCN-STIC.

Actualizado a 15/05/2023

Contenido

1 Esquema Nacional de Seguridad (ENS) – RD 311/2022 3

1.1 Ideas principales 3

1.2 Guías de seguridad CCN-STIC 6

2 Adecuación de sistemas al ENS 7

3 Categorización del sistema de acuerdo al ENS 7

3.1 Extra según la guía CCN-STIC-803 8

4 Medidas de seguridad 9

4.1 Marco organizativo 9

4.2 Marco operacional 9

4.3 Medidas de protección 12

5 Instrucciones Técnicas de Seguridad (ITS) 16

5.1 ITS de informe del estado de la seguridad 16

5.2 ITS de conformidad con el ENS 16

5.3 ITS de notificación de incidentes de seguridad 17

5.4 ITS de auditoría de seguridad de sistemas de información 18

6 Directiva NIS2, un alto nivel de seguridad común en la UE 18

7 Estrategia de Seguridad Nacional 20

7.1 Seguridad global y vectores de transformación (Cap. 1) 20

7.2 Una España segura y resiliente (Cap. 2) 21

7.3 Riesgos y amenazas a la seguridad nacional (Cap. 3) 22

7.4 Un planteamiento estratégico integrado (Cap. 4) 22

7.5 El Sistema de Seguridad Nacional y la Gestión de Crisis (Cap. 5) 25

1 ESQUEMA NACIONAL DE SEGURIDAD (ENS) – RD 311/2022

1.1 IDEAS PRINCIPALES

En la sección III del preámbulo del RD se establecen los tres objetivos del ENS:

1. Alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital.
2. Introducir el concepto "perfil de cumplimiento específico" para garantizar la adaptación del ENS a la realidad de ciertos colectivos o tipos de sistemas, buscando una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.
3. Mejorar la capacidad de respuesta ante incidentes, reducir vulnerabilidades y promover la vigilancia continua, de forma completamente alineada con la Directiva NIS2. Además, permitir aplicar sanciones indirectas al ENS.

El nuevo ENS se encuadra dentro del componente 11 del Plan Nacional de Recuperación, Transformación y Resiliencia y de la Agenda España Digital 2025, viéndose complementado con el Centro de Operaciones de Ciberseguridad de la AGE (COCS) (https://www.ccn.cni.es/index.php/en/docman/documentos-publicos/486-ccn-aproximacion-soc-nacionales/file).

Los sistemas que se ven afectados por el ENS, es decir, el **ámbito subjetivo** del ENS es:

- El definido en el artículo 2 de la Ley 40/2015:
  - La Administración General del Estado.
  - Las Administraciones de las Comunidades Autónomas.
  - Las Entidades que integran la Administración Local.
  - El sector público institucional:
    - Organismos públicos y entidades de derecho público vinculados o dependientes de las AAPP.
    - Entidades de derecho privado vinculadas o dependientes de las AAPP cuando ejerzan potestades administrativas.
    - Las Universidades públicas, que se regirán por su normativa específica y, supletoriamente, por las previsiones de Ley 40/2015.
- Sistemas que tratan información clasificada, aplicándoles aquellas medidas adicionales exigidas por compromisos internacionales.
- Sistemas de información de las entidades del sector privado, cuando de acuerdo con la normativa aplicable y en virtud de una relación contractual presten servicios a las entidades del sector público para el ejercicio por éstas de sus competencias y potestades administrativas.

La Guía del Centro Criptológico Nacional de seguridad de las TIC (CCN-STIC) 830 define el ámbito de aplicación del ENS, pero su última actualización es de 2016.

De acuerdo a la Ley 40/2015, las AAPP podrán determinar sistemas a los que NO es de aplicación el ENS si estos:

- No están relacionados con el ejercicio de derechos ni con el cumplimiento de deberes por medios electrónicos.
- No están relacionados con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo.

Las dimensiones de seguridad definidas en el ENS son ACIDT (Anexo I):

- Autenticidad
- Confidencialidad
- Integridad
- Disponibilidad
- Trazabilidad

Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. En el caso de la AGE, cada ministerio contará con su política de seguridad. La SGAD dispondrá de su propia política de seguridad. La política de seguridad se establecerá de acuerdo con los principios básicos definiendo directrices para la estructuración de los documentos de seguridad, su gestión y acceso y se desarrollará aplicando los siguientes requisitos mínimos, en proporción a los riesgos identificados en cada sistema.

Principios básicos (capítulo II, artículo 5 del ENS):

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en los riesgos.
c) Prevención, detección, respuesta y conservación.
d) Existencia de líneas de defensa.
e) Vigilancia continua (nuevo con respecto al RD 3/2010).
f) Reevaluación periódica.
g) Diferenciación de responsabilidades.

Requisitos mínimos (capítulo III, artículo 12 del ENS):

a) Organización e implantación del proceso de seguridad (se mantienen los 4 responsables: de información, de servicio, de seguridad y de sistema).
b) Análisis y gestión de los riesgos (ver herramienta PILAR del CCN-CERT).
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 (aquellos servicios que se contraten a terceros han de asegurar la conformidad con el ENS; esto es nuevo con respecto al RD 3/2010).
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito (ver herramienta CARLA).
k) Prevención ante otros sistemas de información interconectados (ver herramienta REYES).
l) Registro de la actividad (ver herramientas MONICA y GLORIA) y detección de código dañino (ver herramientas ADA, MARTA y MARIA) (la detección es nueva con respecto al RD 3/2010).
m) Incidentes de seguridad (ver herramienta LUCIA). Definir criterios de clasificación, procedimientos, cauces de comunicación y registro de actuación.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad (ver herramienta IRIS).

El RD proporciona cierta flexibilidad de cara a que el ámbito subjetivo se adapte eficaz y eficientemente al ENS. El artículo 28 y el último apartado del artículo 12 dejan la puerta abierta a la exigencia de los requisitos mínimos en proporción a los riesgos identificados en cada sistema. También se da la posibilidad de modificar las medidas de seguridad a aplicar (Anexo II) relacionadas. Además, prevalecerán las medidas

del análisis y gestión de riesgos (AGR) y, en su caso, de la evaluación de impacto de protección de datos (EIPD), en caso de que resulten agravadas. Se remarca la asignación de responsabilidades y el establecimiento de mecanismos de resolución de conflictos.

Las medidas de seguridad se encuentran descritas en el Anexo II. Se aplican a los marcos organizativo y operacional, así como a las medidas de protección. La relación de las medidas aplicadas en el organismo formará parte del documento "Declaración de Aplicabilidad" (artículo 28).

En línea con el segundo de los objetivos del ENS definidos en el preámbulo, se permite la implementación de perfiles de cumplimiento del ENS específicos para determinadas entidades o sectores de actividad concretos. Hay que recordar que, según el ámbito subjetivo, el ENS se ha de aplicar más allá de las fronteras de la AGE.

De la misma manera, para poder implementar determinadas soluciones tecnológicas o plataformas suministradas por terceros, se podrán implementar esquemas de acreditación de entidades y validación de personas, que garanticen la seguridad de estas soluciones/plataformas. Los servicios externalizados deberán proporcionar un punto o persona de contacto (POC).

Los profesionales tendrán que tener en cuenta la seguridad durante todo el ciclo de vida del sistema de información hasta su desmantelamiento.

Para poder aplicar estos perfiles de cumplimiento específicos y los esquemas de acreditación, el CCN ha de validarlos de acuerdo a las Instrucciones Técnicas de Seguridad (ITS) y las guías del *Computer Emergency Response Team* del CCN o CCN-CERT (artículo 30).

Auditoría de seguridad (Cap. IV artículo 31 y Anexo III): Mínimo cada 2 años (auditoría ordinaria), y además siempre que se produzcan modificaciones sustanciales en el sistema que puedan repercutir en la seguridad (auditoría extraordinaria). Los sistemas de categoría BÁSICA no necesitan realizar auditoría de seguridad, basta con que realicen una autoevaluación. Los resultados de la auditoría de seguridad serán presentados al responsable del sistema y al responsable de seguridad. El responsable de seguridad analizará la auditoría y pedirá al responsable del sistema que adopte las medidas adecuadas. El plazo mínimo de 2 años puede ampliarse a 3 meses más por impedimentos de fuerza mayor.

Informe de estado de seguridad de los sistemas (Cap. IV artículo 32): El CCN establecerá los procedimientos y herramientas para recopilar la información sobre el estado de seguridad de los sistemas de las distintas AAPP. La Comisión Sectorial de Administración Electrónica (CSAE) elaborará con dicha información un perfil general del estado de la seguridad en las entidades titulares de los sistemas de información comprendidos en el ámbito de aplicación del artículo 2. Se desarrolla en una ITS.

Respuesta a incidentes de seguridad (Cap. IV artículo 33): Las AAPP deberán notificar los incidentes al CCN-CERT. En el caso de un operador con incidencia en la Defensa Nacional, se avisará al ESPDEF-CERT. Las organizaciones del sector privado que prestan servicio a entidades públicas avisarán al INCIBE-CERT.

CCN-CERT. Prestación de servicios (Cap. IV artículo 33): El CCN-CERT, en relación a la respuesta a incidentes de seguridad a las entidades del sector público, prestará a las AAPP servicios de soporte y resolución de incidentes de seguridad, elaborará las guías CCN-STIC, ofrecerá formación en seguridad informática, recomendaciones, herramientas, etc.

Normas de conformidad (Cap. V artículo 38): Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas de las declaraciones de conformidad y distintivos de seguridad que tengan. Es desarrollado en una ITS.

Los sistemas de categoría MEDIA o ALTA precisarán de una auditoría de certificación de conformidad de ENS (además de la auditoría de seguridad nombrada anteriormente). Los sistemas de categoría BÁSICA sólo requerirán una autoevaluación para su declaración de conformidad.

Categorización de los sistemas (Cap. VII artículo 40 y Anexo I): Los sistemas se categorizan como BAJO/MEDIO/ALTO en cada una de las dimensiones ACIDT en función del impacto que tendría un incidente de seguridad sobre la capacidad de la organización y sus activos para:

- ✓ Alcanzar sus objetivos.
- ✓ Proteger los activos a su cargo.
- ✓ Cumplir sus obligaciones diarias de servicio.
- ✓ Respetar la legalidad vigente.
- ✓ Respetar los derechos de las personas.

1.2 GUÍAS DE SEGURIDAD CCN-STIC

Las guías CCN-STIC son normas, instrucciones, guías y recomendaciones elaboradas para el mejor cumplimiento de lo establecido en el ENS. Se organizan en series, siendo la serie 800 relativa al ENS. Son especialmente relevantes:

- ✓ CCN-STIC-801. Responsabilidades y Funciones en el ENS – Define los diferentes roles.
- ✓ CCN-STIC-802. Auditoría del ENS.
- ✓ CCN-STIC-803. Valoración de Sistemas en el ENS – Desarrolla cómo realizar la categorización.
- ✓ CCN-STIC-804. ENS. Guía de implantación.
- ✓ CCN-STIC-805. Esquema Nacional de Seguridad. Política de seguridad de la información.
- ✓ CCN-STIC-806. Plan de Adecuación al ENS.
- ✓ CCN-STIC-808. Verificación de Cumplimiento del ENS – Publicada en noviembre de 2022.
- ✓ CCN-STIC-823. Utilización de servicios en la nube.
- ✓ CCN-STIC-824. Informe nacional del estado de seguridad de los sistemas TIC.
- ✓ CCN-CSTIC-830. Ámbito de aplicación del ENS.

Cabe destacar la publicación en 2018 de las guías:

- ✓ CCN-STIC-819. Medidas Compensatorias.
- ✓ CCN-STIC-834. Protección ante Código Dañino en el ENS.
- ✓ CCN-STIC-831. Registro de la actividad de los usuarios.
- ✓ CCN-STIC-837. ENS. Seguridad en Bluetooth.

Desde 2018 a 2023 se destacan las siguientes guías:

- ✓ CCN-STIC-888C. Guía de configuración segura para Contenedores.
- ✓ CCN-STIC-809. Declaración, certificación y aprobación provisional de conformidad con el ENS y distintivos de cumplimiento.
- ✓ CCN-STIC-881 Guía de Adecuación al ENS para Universidades.
- ✓ CCN-STIC-887F. Guía de respuesta a incidentes en AWS.
- ✓ Múltiples guías de configuración segura de servicios en la nube (AWS, Google, Microsoft, Nextcloud).

En https://www.ccn-cert.cni.es/guias.html puede estudiarse información más detallada de las guías actualizadas, tanto de la serie 800 como del resto de series.

2 ADECUACIÓN DE SISTEMAS AL ENS

En la disposición transitoria única del RD 311/2022 se indica:

- ✓ 24 meses desde la entrada en vigor (5/5/2022)

La forma de realizar dicha adecuación se encuentra desarrollada en la Guía CCN-STIC-806 (actualizada en junio de 2020). El Plan de Adecuación será elaborado por el Responsable de Seguridad del Sistema.

3 CATEGORIZACIÓN DEL SISTEMA DE ACUERDO AL ENS

Los activos podemos dividirlos en dos tipos: información y servicios. La determinación de la categoría de un sistema se efectuará en función de la valoración del impacto que tendría un incidente que afectará a la seguridad de esos activos con perjuicio para alguna de las dimensiones ACIDT.

Estas valoraciones corresponderán al Responsable de la Información o al Responsable del Servicio, según el tipo de activo. La categorización la realizará el Responsable del Sistema.

La asignación de una determinada categoría de seguridad determina el equilibrio entre la importancia de la información que maneja o los servicios que presta y el esfuerzo de seguridad requerido. Implica proporcionalidad entre los riesgos y las medidas de seguridad. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

	BAJO	MEDIO	ALTO
Tipo de perjuicio	LIMITADO	GRAVE	MUY GRAVE
Servicio	Reducción apreciable de capacidad sin interrupción.	Reducción significativa de capacidad sin interrupción.	Anulación de capacidad.
Activos	Daño menor.	Daño significativo.	Daño muy grave o irreparable.
Ley o regulación	Incumplimiento formal subsanable.	Incumplimiento material o formal no subsanable.	Incumplimiento grave.
Perjuicio a individuo	Menor reparable.	Significativo de difícil reparación.	Perjuicio grave de difícil reparación o imposible reparación.

Nota: Incumplimiento formal implica que la ley o regulación se cumple, aunque con errores de forma. El incumplimiento material significa que no se cumple con la obligación expresada en la norma.

Si un sistema maneja diferentes informaciones y presta diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para esa dimensión en cada servicio. Por último, la categoría del sistema será la mayor de las categorías de todas sus dimensiones.

3.1 EXTRA SEGÚN LA GUÍA CCN-STIC-803

Cuadro resumen:

1º: por disposición legal o administrativa: ley, decreto, orden, reglamento. Y luego ya...						
	CONFIDENCIALIDAD: Porque su revelación causaría... **INTEGRIDAD**: Porque su manipulación o modificación no autorizada causaría **AUTENTICIDAD**: Porque la falsedad en su origen o en su destinatario causaría					
	Nº personas que deben conocerlo (solo aplica confidencialidad)	Un daño...	Incumplimiento ... de una norma (N/A autenticidad)	Pérdidas €€..	Daño reputacional..	Protestas
ALTO	Nº reducido de personas	Grave, de difícil reparación	Grave	Elevadas	Grave	Masivas (alteración seria orden púb)
MEDIO	Sólo para trabajar con autorización	Importante, aunque subsanable	Material o formal	Importantes	Importante	Públicas (alteración orden público)
BAJO	No deben conocerla personas ajentas a la org	Algún perjuicio	Leve	Apreciables	Apreciable	Múltiples individuales
Sin valorar (CONFIDENCIALIDAD): información de carácter público, accesible por cualquier persona						
Sin valorar (AUTENTICIDAD): cuando origen/destino es irrelevante (conocido por otros medios/difusión anónima x.e.)						
Sin valorar (INTEGRIDAD): cuando los errores en su contenido carecen de consecuencias o son fácil y rápidamente reparables						
	TRAZABILIDAD					
	Porque la incapacidad para rastrear un acceso a la información					
	Impediría/dificultaría notablemente la capacidad para subsanar un error...	Dificultaría ... la capacidad para perseguir delitos	Facilitaría ... la comisión de delitos ...			
ALTO	Grave	Notablemente	Enormemente Graves			
MEDIO	Importante	Notablemente (¿?)	Nada en los puntos			
BAJO	No notablemente	Nada en los puntos	N/A			
Sin valorar (TRAZABILIDAD): cuando no se pueden producir errores de importancia (o son fácilmente reparables por otros medios) o no se pueden perpetrar delitos relevantes (o su investigación es fácil por otros medios)						
	DISPONIBILIDAD					
	RTO (tiempo máximo que el servicio puede permanecer interrumpido)					
ALTO	< 4 horas					
MEDIO	4h - 1 d					
BAJO	1d - 5d					
Sin valorar	> 5 días					

Puesto que la categorización de un sistema puede ocasionar que las medidas a aplicar sean excesivas en algunos casos, es posible desagregarlo en varios subsistemas, siempre que puedan delimitarse la información y los servicios afectados.

Con carácter general, los requisitos de seguridad de otros sistemas que dependan de los servicios prestados por el sistema analizado, serán requisitos del sistema analizado. Si un sistema maneja información de terceros o presta servicio a terceros (un organismo público o una entidad privada), serán estos terceros los que deberán valorar la información o los servicios.

La categoría del sistema será la mayor de las categorías de las 5 dimensiones ACIDT.

Las medidas de seguridad se dividen en tres grupos:

- Marco organizativo - Relacionado con la organización global de la seguridad.
- Marco operacional - Protege la operación del sistema.
- Medidas de protección - Protegen un activo en concreto.

Las medidas seleccionadas utilizando el Anexo II constituirán la Declaración de Aplicabilidad, que deberá ser firmada por el Responsable de Seguridad.

Suele comenzarse por analizar los activos de tipo Información, dado que los activos de tipo Servicio heredarán de estos sus niveles de Confidencialidad e Integridad. Por otro lado, la dimensión Trazabilidad a menudo hereda su categoría de la dimensión Autenticación. En el caso de la Disponibilidad, se suele elegir el nivel en función del *Recovery Time Objective* (RTO): si es menor de 4h se considera ALTO; hasta las 24h MEDIO; hasta 1 semana BAJO; si es mayor de 1 semana SIN VALORACIÓN.

Para aplicar las medidas de seguridad contempladas en el Anexo II previamente hay que hacer un Análisis de Riesgos con el objetivo de determinar los activos, amenazas, vulnerabilidades y el impacto. Para ello se puede utilizar la herramienta PILAR.

4 MEDIDAS DE SEGURIDAD

4.1 MARCO ORGANIZATIVO

Se aplican siempre (desde categoría básica). Implica la existencia de una Política, de Normativa y Procedimientos de Seguridad, así como de un Proceso de autorización para el uso de aplicaciones, equipos, instalaciones, medios, etc.

4.2 MARCO OPERACIONAL

En la tabla de las páginas siguientes, la columna “Por categoría o dimensiones” indica si la medida se exige atendiendo al nivel de seguridad de una o más dimensiones de seguridad, o atendiendo a la categoría de seguridad del sistema. Las celdas en amarillo indican que se empieza a aplicar en categoría media o superior. Las celdas en rojo son sólo de aplicación en categoría alta o requieren seguridad superior en categoría media.

			Nivel de dimensiones de seguridad		
	Medidas de seguridad	Por categoría o dimensiones	BAJO	MEDIO	ALTO
			Categoría del sistema de seguridad		
			BÁSICA	MEDIA	ALTA
Planificación	Análisis de riesgos	Categoría	Informal	(+R1) Semiformal.	(+R2) Formal.
	Arquitectura de seguridad	Categoría	Documentada; esquema de líneas de defensa; sistema de identificación y autenticación de usuarios.	(+R1) SGSI.	(+R1+R2+R3) Actualización y aprobación periódica SGSI y controles técnicos.
	Adquisición de nuevos componentes	Categoría	Según las conclusiones del análisis de riesgos, acorde a la arquitectura y teniendo en cuenta necesidades técnicas, de formación y financiación.		
	Dimensionamiento / gestión de la capacidad	D	Estudio de necesidades relativas a procesamiento, almacenamiento, comunicación, personal e instalaciones.	(+R1) Mejora continua.	
	Componentes certificados	Categoría	No aplica.	Según el CPSTIC[1] del CCN. Refuerzo con medidas TEMPEST y lista de componente SW.	
Control de Acceso	Identificación	T A	Sistemas previstos en ley 39/2015.	(+R1) Identificación avanzada.	
	Requisitos de acceso	C I T A	El acceso a los recursos estará limitado a los derechos que establezca el responsable del recurso.		(+R1) Implementación de privilegios.
	Segregación de funciones y tareas	C I T A	No aplica.	Una tarea crítica necesita de 2 o más personas. Desarrollo y operación, autorización y control en personas distintas.	(+R1) Segregación rigurosa.
	Procesos de gestión de derechos de acceso	C I T A	Atiende a los principios de: Acceso prohibido por defecto; Mínimo privilegio; Conocer y compartir la información necesaria e indispensable; Revisión periódica; Política de acceso específica para acceso remoto.		
	Mecanismo de autenticación (usuarios externos)	C I T A	(+[R1|R2|R3|R4]) Gestión de credenciales. R1 = Contraseñas.	(+[R2|R3|R4]+R5) R2 = Contraseña + OTP[2]. R3 = Certificado + 2FA[3] + Registro previo presencial o telemático. R4 = Certificados en dispositivo físico. R5 = Registro de accesos.	
	Mecanismo de autenticación (usuarios de la organización)	C I T A	(+[R1|R2|R3|R4]+R8+R9) R8 = 2FA desde zona no controlada (Internet). R9 = Acceso remoto.	(+[R1|R2|R3|R4]+R5+R8+R9)	(+[R1|R2|R3|R4]+R5+R6+R7+R8+R9) R6 = Ventana de acceso. R7 = Suspensión por no utilización.

[1] CPSTIC: Catálogo de Productos de Seguridad TIC
[2] OTP: *One Time Password*
[3] 2FA: *2 Factor Authentication*

Explotación	Inventario de activos	Categoría	Actualizado con responsable de cada activo identificado (lista de componentes no es obligatorio, pero sí muy necesario).		
	Configuración de seguridad	Categoría	Cuentas estándar deshabilitadas y mínima funcionalidad.		
	Gestión de la configuración de seguridad	Categoría	Continuamente.	(+R1) Mantenimiento regular de la configuración.	(+R1+R2+R3) Responsable de configuración y copias de seguridad.
	Mantenimiento y actualizaciones de seguridad	Categoría	Seguimiento continuo, aplicación de parches / actualizaciones priorizada.	(+R1) Pruebas en preproducción.	(+R1+R2) Prevención de fallos.
	Gestión de cambios	Categoría	No aplica.	Planificación y pruebas de aceptación.	(+R1) Prevención de fallos.
	Protección frente a código dañino	Categoría	Software de detección en tiempo real en todos los equipos.	(+R1+R2) Escaneo periódico y revisión preventiva.	(+R1+R2+R3+R4) Lista blanca y respuesta a incidente (EDR[4]).
	Gestión de incidentes	Categoría	Proceso integral atendiendo a lo dispuesto en la LOPDGDD.	(+R1+R2) Notificación y detección y respuesta.	(+R1+R2+R3) Reconfiguración dinámica.
	Registro de la actividad	T	Registro de auditoría.	(+R1+R2+R3+R4) Revisión de registros; Sincronización del reloj del sistema; Retención de registros; Control de acceso.	(+R1+R2+R3+R4+R5) Revisión automática y correlación de eventos.
	Registro de la gestión de incidentes	Categoría	Se registran los informes y las evidencias relacionadas con un incidente.		
	Protección de claves criptográficas	Categoría	Protegidas a lo largo de todo el ciclo de vida.	(+R1) Algoritmos y parámetros autorizados por el CCN.	
Recursos externos	Contratación y SLAs	Categoría	No aplica.	En la utilización de recursos externos se establece contractualmente un SLA (servicio mínimo admisible).	
	Gestión diaria	Categoría	No aplica.	Medición de obligaciones de servicio.	
	Protección de la cadena de suministro	Categoría	No aplica.	No aplica.	Análisis de impacto, estimación de riesgo y medidas de contención ante un incidente en la cadena de suministro.
	Interconexión de sistemas	Categoría	No aplica.	Intercambio de información y prestación de servicios con otros sistemas.	(+R1) Coordinación de actividades.

[4] EDR: *Endpoint Detection and Response*

Servicios en la nube	Protección de servicios en la nube	Categoría	Los prestadores de servicio han de cumplir medidas de seguridad definidas en guías CCN-STIC (auditoría, transparencia, cifrado y jurisdicción de datos).	(+R1) Servicios certificados.	(+R1+R2) Guías de configuración de seguridad específicas.
Continuidad del servicio	Análisis de impacto	D	No aplica.	Determinación de los elementos críticos en la prestación de servicio y el impacto de una interrupción.	
	Plan de continuidad	D	No aplica.	No aplica.	Identificación de funciones, responsabilidades y actividades; previsión de medios alternativos.
	Pruebas periódicas	D	No aplica.	No aplica.	Búsqueda de errores o deficiencias del plan de continuidad.
	Medios alternativos	D	No aplica.	No aplica.	Disponibilidad de los medios alternativos, tiempo máximo de activación.
Monitorización del sistema	Detección de intrusión	Categoría	Se dispondrá de herramientas de detección.	(+R1) Detección basada en reglas.	(+R1+R2) Procedimientos de respuesta.
	Sistemas de métricas	Categoría	Recopilación de datos para conocer el grado de implantación de medidas de seguridad (informe anual del art. 32).	(+R1+R2) Efectividad del sistema de gestión de incidentes. Eficiencia del sistema de gestión de la seguridad.	
	Vigilancia	Categoría	Se dispondrá de sistema automático de recolección de eventos de seguridad.	(+R1+R2) Correlación de eventos Análisis dinámico de vulnerabilidades en la superficie de exposición.	(+R1+R2+R3+R4+R5+R6) APTs[5]; Observatorios digitales; Minería de datos; Inspecciones de seguridad.

4.3 MEDIDAS DE PROTECCIÓN

[5] APT: Advanced Persistent Threat

			BAJO	MEDIO	ALTO
Protección de las instalaciones e infraestructuras	Áreas separadas con control de acceso	Categoría	CPD organizado por áreas específicas para su función y control de acceso a las mismas.		
	Identificación de personas	Categoría	Registro de entrada y salida de personas a instalaciones del CPD.		
	Acondicionamiento de locales	Categoría	El CPD asegura condiciones de temperatura, humedad, protección del cableado y de amenazas identificadas en gestión de riesgos.		
	Energía eléctrica	D	Tomas eléctricas y luces de emergencia en el CPD.	(+R1) Suministro eléctrico de emergencia.	
	Protección frente a incendios	D	Atendiendo a la normativa industrial.		
	Protección frente a inundaciones	D	No aplica.	CPD protegido frente a incidentes causados por agua.	
	Registro de entrada y salida de equipamiento	Categoría	Anotación de entradas y salidas de equipamiento esencial identificando a la persona que lo autoriza.		
Gestión personal	Caracterización de puesto de trabajo (HPS[6] recomendable)	Categoría	No aplica.	Definición de responsabilidades en materia de seguridad y de requisitos que han de satisfacer las personas que ocupen el puesto de trabajo, en particular, relativo a la confidencialidad.	
	Deberes y obligaciones	Categoría	Información al trabajador de responsabilidades, confidencialidad y medidas disciplinarias.	(+R1) Confirmación expresa.	
	Concienciación	Categoría	Regularmente se ha de concienciar al personal acerca de su papel y responsabilidad en cuanto a la seguridad del sistema.		
	Formación	Categoría	Formación del personal de forma regular en materias de seguridad.		
Protección de los equipos	Puesto de trabajo despejado	Categoría	Únicamente el material necesario en cada momento.	(+R1) Almacenamiento del material en lugar cerrado.	
	Bloqueo de puesto de trabajo (Guía asociada al perfil de cumplimiento o a la categorización)	A	No aplica.	Bloqueo del terminal tras tiempo prudencial sin actividad.	(+R1) Cierre de sesiones.
	Protección de dispositivos portátiles	Categoría	Protección de dispositivos que salgan de las instalaciones. Inventario y procedimiento ante pérdidas.	Protección de dispositivos que salgan de las instalaciones de la unidad. Inventario y procedimiento ante pérdidas.	(+R1+R2) Cifrado de discos. Uso de dispositivos restringido a entornos protegidos.
	Otros dispositivos conectados a la red.	C	Impresoras, escáneres, proyectores, altavoces, IoT, BYOD, configurados de manera segura que garantice el flujo de información de E/S.	(+R1) Productos certificados.	

[6] HPS: Habilitación Personal de Seguridad

Protección de las comunicaciones	Perímetro seguro	Categoría	Debe existir un sistema de protección perimetral que separe la red interna del exterior (ver ITS de Interconexión de SI).		
	Protección de la confidencialidad	C	Uso de VPN cuando la comunicación discurra por redes fuera del dominio de seguridad.	(+R1) Algoritmos y parámetros autorizados.	(+R1+R2+R3) R2 = Dispositivos hardware. R3 = Productos certificados.
	Protección de la integridad y de la autenticidad	I A	Asegurar la autenticidad en comunicaciones con un punto exterior al dominio de seguridad. Prevención de ataques activos al ser detectados: modificación de información en tránsito, inyección de información espuria, secuestro de sesión.	(+R1+R2) R1 = VPN. R2 = Uso de algoritmos y parámetros autorizados por el CCN.	(+R1+R2+R3+R4) R3 = Dispositivos hardware. R4 = Productos certificados.
	Separación de flujos de información en la red.	Categoría	No aplica.	(+[R1|R2|R3]) Tráfico de red segregado. R1 = Segmentación lógica básica (VLANs) de usuarios, servicios y administración.	(+[R2|R3]+R4) R2 = Segmentación lógica avanzada. R3 = Segmentación física. R4 = Puntos de interconexión.
Protección de los soportes de información	Marcado de soportes	C	No aplica.	Los soportes de información llevarán marcas o metadatos que indiquen el nivel de seguridad de la información.	
	Criptografía	C I	No aplica.	Aplica a soportes de información removible. Uso de algoritmos y parámetros autorizados por el CCN.	(+R1+R2) R1 = Productos certificados. R2 = Copias de seguridad.
	Custodia	Categoría	Control de acceso con medidas físicas o lógicas a los soportes de información. Respeto por las condiciones atmosféricas requeridas por el fabricante.		
	Transporte	Categoría	Los dispositivos que son desplazados de lugar han de cumplir los requisitos de seguridad permaneciendo siempre bajo control.		
	Borrado y destrucción	C	Aplica a todo tipo de equipos y soportes que almacenen información.	(+R1) Productos certificados.	
Protección de las aplicaciones informáticas	Desarrollo de aplicaciones	Categoría	No aplica.	(+R1+R2+R3+R4)) El entorno de desarrollo debe ser distinto al de producción sin compartir datos entre ellos. R1 = Mínimo privilegio. R2 = Metodología de desarrollo seguro. R3 = Seguridad desde el diseño. R4 = Datos de pruebas.	
	Aceptación y puesta en servicio	Categoría	Antes del paso a producción se comprobará el correcto funcionamiento de la aplicación.	(+R1) Pruebas realizadas en entorno de preproducción.	

Protección de la información	Datos personales	Categoría	El Responsable de Seguridad recogerá los requisitos de protección de datos fijados por el Responsable del Tratamiento para implantarlos en el sistema, así como riesgos para derechos y libertades según el art. 24 y el art. 32 del RGPD.		
	Calificación de la información	C	No aplica.	Para calificar la información se tendrá en cuenta lo establecido en leyes y tratados internacionales. La información no clasificada se califica como: USO OFICIAL.	
	Firma electrónica	I A	Verificación y validación de firma electrónica durante el tiempo requerido por la actividad administrativa.	(+R1+R2+R3) R1 = Certificados cualificados. R2 = Algoritmos y parámetros autorizados.	(+R1+R2+R3+R4) R3 = Verificación y validación de firma. R4 = Firma electrónica avanzada basada en certificados cualificados junto con 2FA.
	Sellos de tiempo	T	No aplica.	No aplica.	Aplicados si se necesita evidencia electrónica en el futuro.
	Limpieza de documentos	C	Retirada de información adicional en campos ocultos, metadatos, comentarios o revisiones.		
	Copias de seguridad	D	La periodicidad y plazos de retención se determinan en la normativa interna de la organización.	(+R1) Pruebas de recuperación.	(+R1+R2) Protección de las copias de seguridad.
Protección de servicios	Protección del correo electrónico	Categoría	Proteger a la organización de spam, código dañino, applets. Limitar el uso como soporte de comunicaciones privadas. Formación y concienciación.		
	Protección de servicios y aplicaciones web	Categoría	(+[R1|R2]) Control de acceso a información que lo requiera. Prevención de ataques: modificación de URL, RFI[7], robo de cookies, SQL injection, XSS[8].	(+[R1|R2]) R1 = Auditorías de seguridad. R2 = Auditorías de seguridad avanzada.	(+R2+R3) R3 = Protección de las cachés.
	Protección de la navegación web	Categoría	La navegación por Internet de usuarios internos se protegerá con normativa de utilización, formación y concienciación y evitando visitas a webs maliciosas.		(+R1) Monitorización.
	Protección frente a denegación de servicio	D	No aplica.	Medidas preventivas Sistema dimensionado con holgura y tecnologías instaladas que prevengan ataques conocidos.	(+R1) Detección y reacción.

[7] RFI: *Remote File Injection*
[8] XSS: *Cross-Site Scripting*

5 INSTRUCCIONES TÉCNICAS DE SEGURIDAD (ITS)

Disposición adicional segunda. Desarrollo del ENS.

Las instrucciones técnicas de seguridad (ITS) tendrán en cuenta las normas armonizadas por la UE aplicables. El CCN elaborará y difundirá las correspondientes guías CCN-CSTIC.

En el anterior ENS (RD 3/2010) se definía una lista de ITS a desarrollar. En el actual ENS no se especifican, si no que se deja abierta la creación de nuevas y la actualización de las existentes. Actualmente hay 4:

a) Informe del estado de la seguridad (actualizada en 2020).
b) Notificación de incidentes de seguridad (publicada en 2018).
c) Auditoría de la seguridad de los sistemas de información (publicada en 2018).
d) Conformidad con el ENS (publicada en 2016).

Las ITS se pueden encontrar en:
https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/Instrucciones-Tecnicas.html

La Secretaria de Estado de Digitalización e Inteligencia Artificial (SEDIA), a propuesta de la CSAE e iniciativa del CCN, aprobará las ITS de obligado cumplimiento. Se publicarán mediante resolución de la SEDIA.

5.1 ITS DE INFORME DEL ESTADO DE LA SEGURIDAD

Establece las condiciones relativas a la recopilación y comunicación de datos que permitan conocer las principales variables de la seguridad de la información de los sistemas comprendidos en el ámbito de aplicación del ENS, y confeccionar un perfil general del estado de la ciberseguridad en las AAPP, al objeto de dar adecuada respuesta al mandato del artículo 32 del ENS. Para ello, el CCN ha desarrollado el Informe Nacional del Estado de Seguridad (la herramienta **INES**), que facilita la labor de todos los organismos.

El detalle queda recogido en las siguientes guías CCN-STIC:

- ✓ CCN-STIC-815. Indicadores y métricas en el ENS.
- ✓ CCN-STIC-824. Informe nacional del estado de seguridad de los sistemas TIC. Es aquí donde se indica que **se prevé recopilar** las métricas (medidas de seguridad op.mon.2) **anualmente.**
- ✓ CCN-STIC-844. Manual de Usuario de INES.

5.2 ITS DE CONFORMIDAD CON EL ENS

Establece los criterios y procedimientos para la determinación de la conformidad con el ENS y para la publicidad de dicha conformidad, al objeto de poder dar adecuada respuesta al mandato del Capítulo V, Normas de conformidad, del Real Decreto 311/2022; en particular, determina los mecanismos de obtención y ulterior publicidad de las declaraciones de conformidad y los distintivos de seguridad de los que sean acreedores y que se hubieren obtenido respecto al cumplimiento del ENS. SE puede encontrar más información sobre esta cuestión en la Guía CCN-STIC-809 Declaración, Certificación y Aprobación Provisional de conformidad con el ENS y Distintivos de cumplimiento.

De acuerdo al ENS, los sistemas de categoría **BÁSICA** sólo requerirán de una **autoevaluación** para su declaración de conformidad, mientras que los sistemas de categoría **MEDIA O ALTA** precisarán de una **auditoría formal** para su certificación de conformidad. Tanto la autoevaluación como la auditoría formal se realizarán **al menos cada 2 años**.

En la ITS se especificará además cómo se dará **publicidad** a la conformidad:

- BÁSICA exponiendo el Distintivo de Declaración de Conformidad en la sede electrónica, que incluirá un enlace al documento de Declaración de Conformidad correspondiente, que también permanecerá accesible a través de dicha sede electrónica.

- MEDIA y ALTA lo mismo, solo que en este caso la conformidad será expedida por una entidad certificadora y se completará mediante un Distintivo de Certificación de Conformidad.

Las entidades certificadoras serán acreditadas por la Entidad Nacional de Acreditación en España (ENAC). A continuación, se muestran algunos distintivos de Certificación de Conformidad con el ENS

5.3 ITS DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

Se publica mediante la Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la ITS de notificación de incidentes de seguridad. Esta establece los criterios y procedimientos para la notificación al CCN por parte de las entidades que forman parte de los ámbitos subjetivos de aplicación de las leyes 39/2015 y 40/2015 de aquellos incidentes que tengan un impacto significativo en la seguridad de la información que manejan y los servicios que prestan en relación con la categoría del sistema.

La notificación será obligatoria en el caso de incidentes con nivel de impacto Alto, Muy alto y Crítico. La instrucción también determina las evidencias a entregar en el caso de incidentes nivel Alto, Muy alto y Crítico, la obligación de remisión de estadísticas de incidentes, la notificación de impactos recibidos, el desarrollo de herramientas automatizadas para facilitar las notificaciones y el régimen legal de las notificaciones y comunicación de información, más una disposición adicional con precisiones sobre la notificación cuando el incidente afecte a datos personales. Sus aspectos más relevantes son la determinación de:

- Los criterios que permiten determinar el nivel de impacto del incidente.
- En qué condiciones es obligatoria la notificación.
- Las evidencias que podrá recabar el CCN-CERT para la investigación de incidentes de seguridad significativos.
- La obligación de las AAPP de elaborar estadísticas de incidentes de seguridad y remitirlas al CCN-CERT, junto con el resto de información enviada respecto a los incidentes.
- Las herramientas automatizadas disponibles para realizar las notificaciones previstas en esta ITS. En particular, se cita el Listado Unificado de Coordinación de Incidentes y Amenazas (LUCIA), herramienta desarrollada por el CCN con el propósito de automatizar los mecanismos de notificación, comunicación e intercambio de información sobre incidentes de seguridad, de acuerdo a lo establecido en la Guía CCN-STIC-817.
- El marco legal aplicable a las notificaciones y comunicaciones de informaciones.
- El apartado 10 añade una disposición adicional en la que se recogen varios aspectos relativos a la protección de datos. Cuando el incidente afecte a datos personales la notificación a la autoridad de control competente se realizará con independencia del nivel de impacto del incidente en el ENS.

5.4 ITS DE AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

Se publica mediante la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la ITS de auditoría de la seguridad de los sistemas de información. Tiene por objeto establecer las condiciones para la realización de las auditorías, ordinarias o extraordinarias, previstas en el artículo 31 del ENS. Las auditorías deben realizarse para determinar el grado de conformidad con el ENS y deben permitir a sus responsables adoptar las medidas oportunas para subsanar las deficiencias encontradas y, en su caso, posibilitar la obtención de la correspondiente **certificación de conformidad**.

Cabe recordar que, para obtener esta certificación, los sistemas de información de categoría MEDIA o ALTA precisarán superar una auditoría de seguridad, al menos cada dos años. Asimismo, los **informes de auditoría** emitidos podrán ser requeridos por el CCN-CERT ante cualquier agresión recibida en los sistemas de información de las AAPP.

Para el desarrollo de las auditorías, la Resolución señala que deberán realizarse conforme a la propia ITS y, cuando corresponda, a las normas nacionales e internacionales sobre auditorías, entre ellas:

- ✓ Guía CCN-STIC-802 Auditoría del ENS.
- ✓ Guía CCN-STIC-804 ENS. Guía de implantación.
- ✓ Guía CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS.

6 DIRECTIVA NIS2, UN ALTO NIVEL DE SEGURIDAD COMÚN EN LA UE

Conocida también como NIS2, el 27 de diciembre de 2022 se publicó la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) 910/2014 y la Directiva (UE) 2018/1972, y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

La directiva NIS2 propone sustituir la directiva NIS y reforzar así los requisitos de seguridad, abordar la seguridad de las cadenas de suministro, racionalizar las obligaciones de información e introducir medidas de supervisión más rigurosas y requisitos de aplicación más estrictos, incluyendo sanciones armonizadas en toda la UE. La propuesta de ampliación del ámbito de aplicación de la NIS2, obligando efectivamente a más entidades y sectores a tomar medidas, contribuiría a aumentar el nivel de ciberseguridad en Europa a largo plazo.

La propuesta de NIS2 se fija 3 objetivos generales:

1) Aumentar el nivel de ciberresiliencia de un amplio conjunto de empresas que operan en la UE en todos los sectores relevantes, estableciendo normas que garanticen que todas las entidades públicas y privadas del mercado interior (que cumplen funciones importantes para la economía y la sociedad en su conjunto) estén obligadas a adoptar medidas adecuadas de ciberseguridad. Por ejemplo, la propuesta amplía considerablemente el ámbito de la directiva actual, añadiendo nuevos sectores como las telecomunicaciones, las plataformas de medios sociales y la administración pública. Establece que todas las medianas y las grandes entidades activas que operan en los sectores cubiertos por el marco NIS2 tienen que cumplir con las reglas de seguridad de la propuesta, y elimina la posibilidad de que los Estados miembros adapten los requisitos en determinados casos (lo que había provocado una gran fragmentación con la aplicación de NIS1). Se suprime la distinción que se hacía entre los operadores de servicios esenciales (OES) y los proveedores de servicios digitales (DSP), que actualmente se dividen en tres categorías: mercados en línea, motores de búsqueda y proveedores de servicios en la nube. Por último, se aborda por primera vez la ciberseguridad de la cadena de suministro de las TIC (de especial importancia en el caso del IoT).
2) Reducir las incoherencias en materia de resiliencia en el mercado interior en los sectores ya cubiertos por la directiva, alineando más:

i. el ámbito de aplicación de facto
ii. los requisitos de seguridad y notificación de incidentes
iii. las disposiciones que rigen la supervisión nacional y su aplicación
iv. las capacidades de las autoridades competentes de los Estados miembros.

La propuesta incluye una lista de 7 elementos clave que todas las empresas deben abordar o aplicar como parte de las medidas que adopten, incluida la respuesta a incidentes, la seguridad de la cadena de suministro, el cifrado y la divulgación de vulnerabilidades. Además, la propuesta prevé un enfoque en dos fases para la notificación de incidentes. Las empresas afectadas tienen 24 horas desde que tienen conocimiento de un incidente para presentar un informe inicial, seguido de un informe final a más tardar un mes después. En cuanto a la aplicación, establece una lista mínima de sanciones administrativas siempre que las entidades infrinjan las normas relativas a la gestión de los riesgos de ciberseguridad o sus obligaciones de notificación establecidas en la Directiva NIS. Estas sanciones incluyen instrucciones vinculantes, la orden de aplicar las recomendaciones de una auditoría de seguridad, la orden de adecuar las medidas de seguridad a los requisitos de la NIS, y multas administrativas (de hasta 10 millones de euros o el 2 % del volumen de negocios total de las entidades en todo el mundo, lo que sea mayor).

3) Mejorar el nivel de conocimiento conjunto de la situación y la capacidad colectiva de prepararse y responder:
   i. tomando medidas para aumentar el nivel de confianza entre autoridades competentes
   ii. compartiendo más información
   iii. estableciendo normas y procedimientos en caso de incidente o crisis a gran escala.

   Las nuevas normas propuestas mejoran la forma en que la UE previene, gestiona y responde a los incidentes y crisis de ciberseguridad a gran escala, introduciendo responsabilidades claras, una planificación adecuada y una mayor cooperación de la UE. La directiva revisada establecería un marco de gestión de crisis de la UE, exigiendo a los Estados miembros que adopten un plan y designen a las autoridades nacionales competentes para participar en la respuesta a incidentes y crisis de ciberseguridad a nivel de la UE. La directiva propuesta crearía una Red de Organización de Enlace para Crisis Cibernéticas (EU-CyCLONe) para apoyar la gestión coordinada de los incidentes de ciberseguridad en toda la UE, así como para garantizar el intercambio de información. La directiva propuesta también reforzará el papel del Grupo de Cooperación NIS en la toma de decisiones y en el aumento de la cooperación entre Estados miembros. Los Estados miembros seguirán estando obligados a adoptar una estrategia nacional de ciberseguridad y designar una o varias autoridades nacionales competentes para supervisar el cumplimiento de la Directiva, y designar un *Computer Security Incident Response Team* (CSIRT) para gestionar las notificaciones de incidentes y puntos de contacto únicos (SPOC) para actuar como punto de enlace con otros Estados miembros.

Con el fin de garantizar la coherencia con la legislación de la UE relacionada, la revisión de la Directiva NIS en particular, tiene en cuenta las tres iniciativas siguientes de la Comisión:

1) La revisión de la Directiva sobre la resistencia de las entidades críticas (RCE), que se propuso junto con la propuesta NIS2, con el objetivo de mejorar la resistencia de las entidades críticas contra las amenazas físicas en un gran número de sectores. La propuesta amplía tanto el alcance como la profundidad de la actual directiva de 2008, incluyendo la cobertura de 10 sectores: energía, transporte, banca, infraestructuras de los mercados financieros, sanidad, agua potable, aguas residuales, infraestructuras digitales, administración pública y espacio.
2) La iniciativa sobre una ley de resiliencia operativa digital para el sector financiero (DORA).
3) La iniciativa relativa a un código de red sobre ciberseguridad con normas sectoriales específicas para los flujos eléctricos transfronterizos.

En cuanto a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), vería aumentadas sus responsabilidades dentro de su actual mandato, que implica supervisar la aplicación de la NIS. La ENISA

se encargaría de elaborar un informe cada dos años sobre el estado de la ciberseguridad en la UE y mantener un registro europeo de vulnerabilidades que proporcione acceso a la información sobre las vulnerabilidades de los productos y servicios de las TIC divulgadas voluntariamente por entidades esenciales e importantes y sus proveedores de TIC. Al mismo tiempo, ENISA tendría que crear y mantener un registro, en el que determinados tipos de entidades notificarían si están establecidos en la UE. Estas incluirían proveedores de servicios de sistemas de nombres de dominio, registros de nombres de dominio de primer nivel, proveedores de servicios de computación en la nube, proveedores de servicios de centros de datos, proveedores de redes de distribución de contenidos, así como mercados en línea, motores de búsqueda en línea y plataformas de redes sociales. Se trata de garantizar que estas entidades no se enfrenten a una multitud de diferentes requisitos legales, dado que prestan servicios transfronterizos en un grado especialmente elevado.

7 ESTRATEGIA DE SEGURIDAD NACIONAL

Tras la estrategia de 2017, la nueva estrategia ha sido publicada en 2021. Está estructurada en 5 capítulos:

1) Seguridad global y vectores de transformación.
2) Una España segura y resiliente.
3) Riesgos y amenazas.
4) Un planeamiento estratégico integrado.
5) Un Sistema de Seguridad Nacional y la Gestión de Crisis.

La prevención y la adaptación son claves para lograr un Sistema de Seguridad Nacional eficiente. Esto requiere:

- ✓ Más anticipación: implantación de un sistema de alerta temprana y planes de gestión de crisis.
- ✓ Más integración: coordinación entre las AAPP, la colaboración público-privada y la ciudadanía.
- ✓ Más resiliencia: mitigación de riesgos y fortalecer la resiliencia (capacidad de resistencia, transformación y recuperación ante una situación adversa).

Desarrollo normativo en la Ley de Seguridad Nacional 36/2015. Indica que la Estrategia deberá revisarse cada 5 años, sin embargo, el impacto de la pandemia y el empleo de estrategias híbridas han aconsejado adelantar esta revisión, y de ahí surge esta nueva Estrategia de Seguridad Nacional.

7.1 SEGURIDAD GLOBAL Y VECTORES DE TRANSFORMACIÓN (CAP. 1)

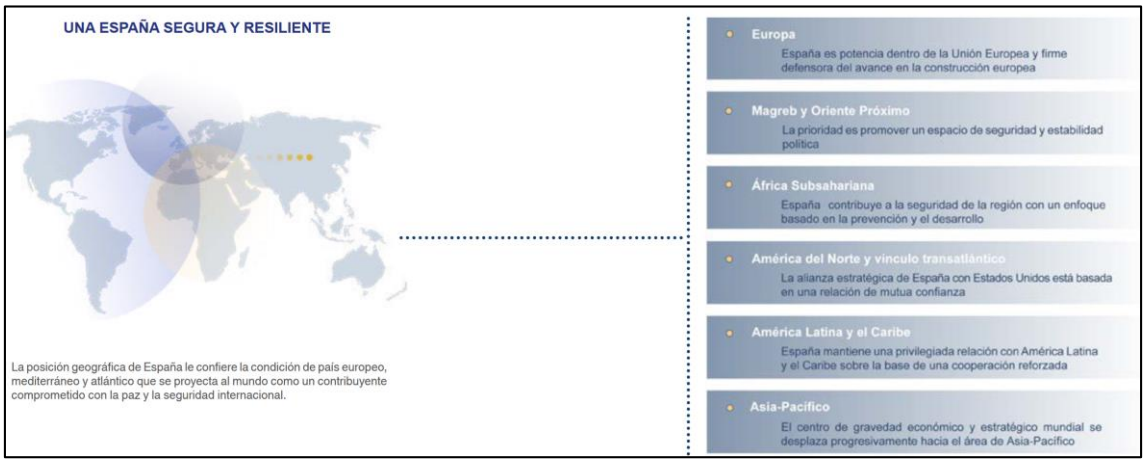
Los vectores de transformación definidos son:

- ✓ Contexto geopolítico, factores que generan un escenario de incertidumbre que incrementa la necesidad de la autonomía estratégica de la UE:
  - Mayor rivalidad geopolítica (EEUU, China, Rusia).
  - Deterioro del multilateralismo.
  - Aumento de estrategias híbridas.
  - Asertividad de potencias regionales.
- ✓ Escenario socio-económico:
  - Aumento de la desigualdad.
  - Medidas proteccionistas.
  - Fragilidad de la cadena de suministros.
  - Polarización social.
- ✓ Transformación digital:
  - Sociedades hiperconectadas.
  - Tecnologías disruptivas.
  - El dato como recurso estratégico de primer orden.
  - Soberanía digital, ética y derechos humanos.

- ✓ Transformación ecológica:
  - Aceleración del cambio climático.
  - Intensificación de fenómenos adversos.
  - Cambio de paradigma energético.
  - Competición por la tecnología renovable.

7.2 UNA ESPAÑA SEGURA Y RESILIENTE (CAP. 2)

El segundo capítulo ofrece un recorrido de las distintas regiones del mundo, trazando un perfil desde la perspectiva española de la seguridad. Desde su identificación como país de condición europea, mediterránea y atlántica, se realiza un recorrido geográfico, donde Europa, Magreb y Oriente Próximo, África Subsahariana, América del Norte, América Latina y el Caribe, y Asia-Pacífico se analizan desde el prisma de la Seguridad Nacional.



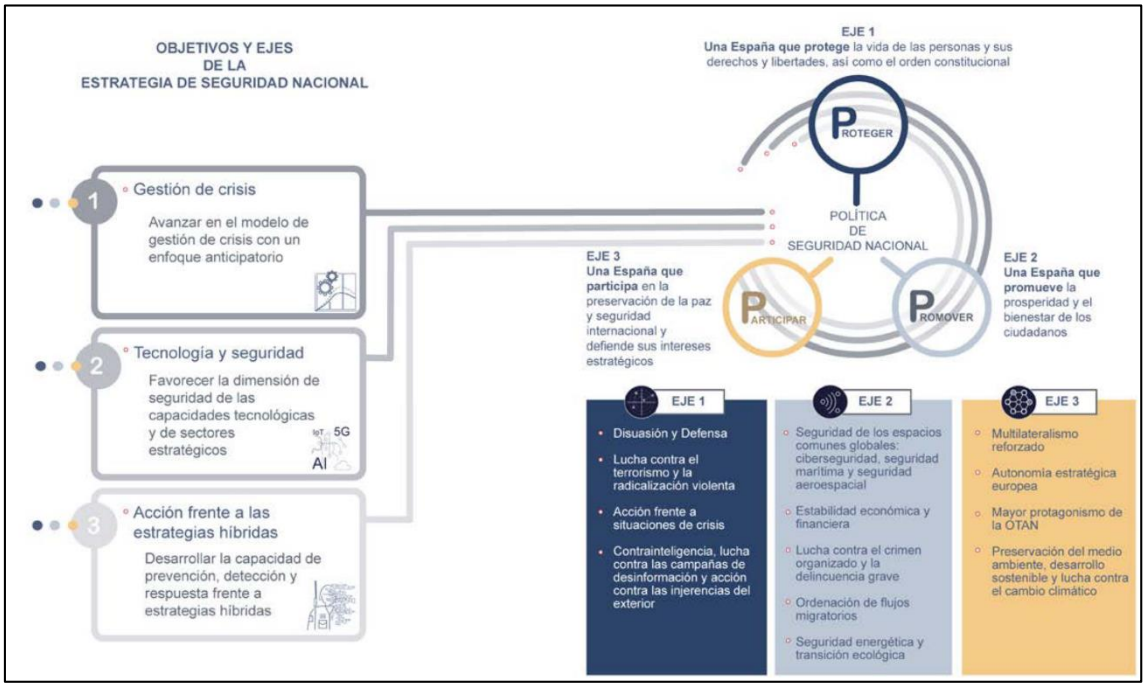
7.3 RIESGOS Y AMENAZAS A LA SEGURIDAD NACIONAL (CAP. 3)

El tercer capítulo describe un mapa de los riesgos y amenazas a la Seguridad Nacional con un enfoque que pone de relieve su dinamismo e interdependencia, en un entorno donde las estrategias híbridas ganan protagonismo. Los riesgos y las amenazas a la Seguridad Nacional no son estáticos, sino que se conciben de una manera dinámica, ya que la interrelación entre ellos puede producir efectos en cascada, como ha ocurrido con la crisis generada por la pandemia.

Figura 3.1. Riesgos y Amenazas a la Seguridad Nacional

7.4 UN PLANTEAMIENTO ESTRATÉGICO INTEGRADO (CAP. 4)

Este capítulo establece los objetivos de la Estrategia: avanzar en materia de gestión de crisis, fortalecer la dimensión de seguridad en sectores estratégicos y desarrollar la prevención, detección y respuesta de España frente a estrategias híbridas. Para ello establece un planteamiento integrado para la Política de Seguridad Nacional con una estructura diseñada por tres ejes estratégicos: proteger, promover y participar. Sobre estos tres ejes se estructuran 33 líneas de acción (L.A.).



Primer eje: Una España que protege la vida de las personas y sus derechos y libertades, así como el orden constitucional.

- ✓ Disuasión y la defensa:
  - **L.A. 1.** Asegurar las capacidades militares necesarias para proporcionar una disuasión creíble y una respuesta eficaz en todo el espectro de la crisis o conflicto, garantizando su sostenibilidad en el tiempo bajo un marco presupuestario suficiente y estable.
  - **L.A. 2.** Reforzar las capacidades de defensa a través de la investigación, el desarrollo y la innovación tecnológica como vectores de ventaja estratégica.
  - **L.A. 3.** Desarrollar el sector industrial de la defensa, la seguridad y el espacio, así como las tecnologías duales, mediante la cooperación público-privada y el aprovechamiento de sinergias con las herramientas existentes en el marco nacional y en las Organizaciones Internacionales de Seguridad y Defensa a las que pertenece España, en particular los Fondos Europeos de Defensa y la Cooperación Estructurada Permanente de la UE.
- ✓ Lucha contra el terrorismo y la radicalización violenta:
  - **L.A. 4.** Desarrollar herramientas y capacidades que refuercen la ejecución de investigaciones en el ámbito de la lucha contra el terrorismo por parte de los organismos implicados, así como reforzar la coordinación de esos organismos.
  - **L.A. 5.** Potenciar el desarrollo e implementación del Plan Estratégico Nacional de Prevención y Lucha Contra la Radicalización Violenta (PENCRAV) y del Plan Estratégico Nacional de Lucha Contra la Financiación del Terrorismo (PENCFIT).
  - **L.A. 6.** Incrementar la contribución española en iniciativas de ámbito internacional relativas al contraterrorismo y promover la capacitación y fortalecimiento de organismos e instituciones con competencias en contraterrorismo en países especialmente afectados.
  - **L.A. 7.** Potenciar las capacidades de prevención en la lucha contraterrorista de las actividades vinculadas al terrorismo y a extremismos violentos, especialmente en Internet y redes sociales.
  - **L.A. 8.** Actualizar el plan de protección y prevención antiterrorista en sus dimensiones interior y exterior.
- ✓ Actuación frente a situaciones de crisis

- **L.A. 9.** Desarrollar el modelo de gestión integral de crisis en el Sistema de Seguridad Nacional a través de la elaboración de un reglamento de gestión de crisis; la implantación de un sistema de alerta temprana basado en indicadores; la creación de un catálogo de recursos y de planes de preparación y disposición de recursos; y el diseño de un Plan de ejercicios de preparación en el marco de la Seguridad Nacional.
- **L.A. 10.** Crear la Reserva Estratégica basada en capacidades nacionales de producción industrial con una triple orientación.
- **L.A. 11.** Modernizar el sistema de vigilancia nacional de Salud Pública a través de la renovación de las tecnologías sanitarias y los sistemas de información. La Estrategia Digital del Servicio Nacional de Salud incluirá medidas para mejorar la prevención, el diagnóstico, la vigilancia y la gestión de la salud en un marco de cogobernanza con las CCAA.
- **L.A. 12.** Elaborar un Plan Integral de Seguridad para Ceuta y Melilla.

✓ Contrainteligencia, lucha contra las campañas de desinformación y acción frente a las injerencias del exterior:
- **L.A. 13.** Elaborar una Estrategia Nacional de Lucha contra las campañas de desinformación.
- **L.A. 14.** Incrementar las capacidades de los Servicios de Inteligencia españoles frente a los ataques de los Servicios de Inteligencia hostiles, en especial en el ciberespacio.
- **L.A. 15.** Potenciar las capacidades de la Oficina Nacional de Seguridad y garantizar un marco legal adecuado para la protección de la información clasificada.
- **L.A. 16.** Reforzar la cooperación internacional en materia de contrainteligencia.

Segundo eje: Una España que promueve la prosperidad y el bienestar de los ciudadanos.

✓ Seguridad de los espacios comunes globales (ciberespacio, marítimo, aéreo y ultraterrestre):
- **L.A. 17.** Avanzar en la integración del modelo de gobernanza de la ciberseguridad en el marco del Sistema de Seguridad Nacional.
- **L.A. 18.** Elaborar escenarios de riesgo y planes de preparación y respuesta para aquellas situaciones que se consideren de especial interés para la Seguridad Nacional en el ámbito de la seguridad marítima.
- **L.A. 19.** Crear la Agencia Espacial Española, con un componente dedicado a la Seguridad Nacional, para dirigir el esfuerzo en materia espacial, coordinar de forma eficiente los distintos organismos nacionales con responsabilidades en el sector espacial y unificar la colaboración y coordinación internacional

✓ Estabilidad económica y financiera:
- **L.A. 20.** Potenciar la modernización y la productividad del ecosistema español industrial, mediante el impulso de la competitividad de sectores estratégicos clave para la Seguridad Nacional, en línea con lo establecido en el Plan de Recuperación, Transformación y Resiliencia.

✓ Lucha contra el crimen organizado y la delincuencia grave:
- **L.A. 21.** Elaborar un plan estratégico de lucha contra el enriquecimiento ilícito de las organizaciones criminales y los delincuentes.
- **L.A. 22.** Desarrollar un plan estratégico específico nacional contra la trata y la explotación de seres humanos.

✓ Ordenación de flujos migratorios:
- **L.A. 23.** Establecer un sistema integral y colaborativo de información a nivel de la AGE, que permita conocer en tiempo oportuno la situación de los flujos de inmigración, los recursos comprometidos en su gestión, así como las necesidades identificadas.
- **L.A. 24.** Fortalecer la relación y los acuerdos con los países de origen y tránsito para lograr una migración ordenada e impedir el tráfico de seres humanos.

- ✓ Seguridad energética y transición ecológica
  - **L.A. 25.** Actualizar la Estrategia de Seguridad Energética Nacional para establecer objetivos y líneas de acción de acuerdo con el contexto de transición ecológica, energética y económica.

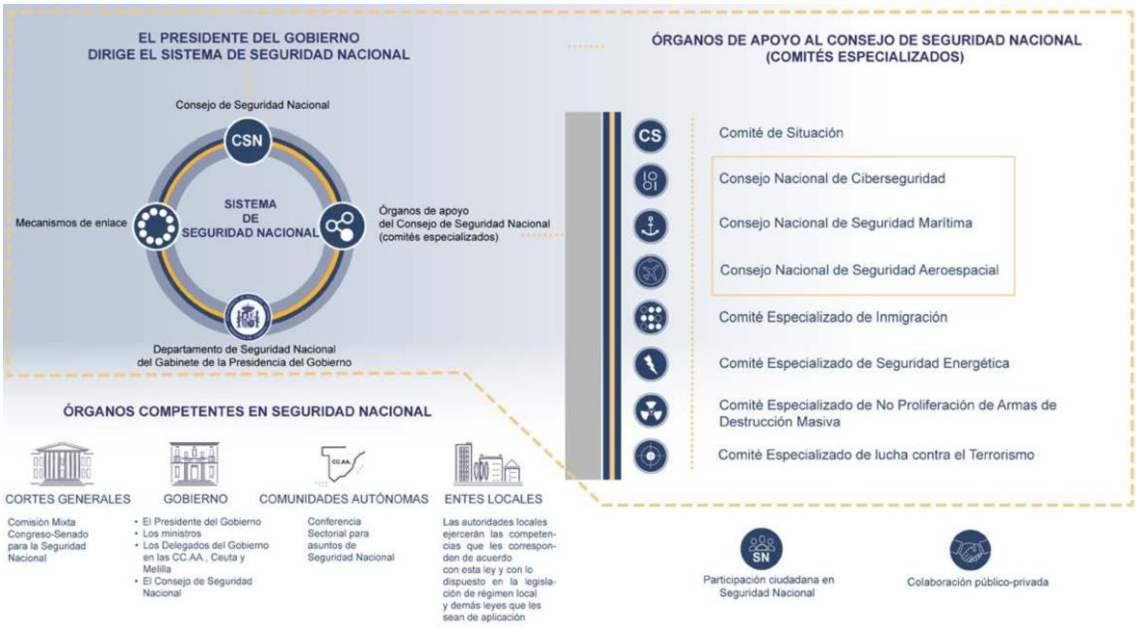
Tercer eje: Una España que participa en la preservación de la paz y seguridad internacional y defiende sus intereses estratégicos.

- ✓ Multilateralismo reforzado:
  - **L.A. 26.** Potenciar la diplomacia preventiva y el papel de España como actor activo y comprometido en la mediación de conflictos en el exterior.
  - **L.A. 27.** Contribuir a la intensificación del apoyo al régimen internacional de no proliferación de armas de destrucción masiva y desarme, a través de la actualización del régimen internacional de control, exportación y verificación.
  - **L.A. 28.** Impulsar la implementación de los objetivos del II Plan Nacional de Acción de Mujeres, Paz y Seguridad de integrar la perspectiva de género y hacer realidad la participación significativa de las mujeres en la prevención, gestión y resolución de conflictos y la consolidación de la paz.
- ✓ Autonomía estratégica europea:
  - **L.A. 29.** Promover un liderazgo decidido en la formulación y el desarrollo de la Política Común de Seguridad y Defensa, en línea con las conclusiones que se obtengan del proceso de revisión de la seguridad europea.
  - **L.A. 30.** Contribuir a reforzar las capacidades estratégicas autónomas de la UE, incluida la construcción de la Europa de la Defensa y el desarrollo de capacidades industriales y tecnológicas europeas.
- ✓ Mayor protagonismo en la OTAN:
  - **L.A. 31.** Participar activamente en la revisión estratégica acometida por la OTAN.
- ✓ Preservación del medio ambiente, desarrollo sostenible y lucha contra el cambio climático:
  - **L.A. 32.** Integrar la Agenda 2030 en las políticas de cooperación al desarrollo, para contribuir a reforzar las capacidades de los países más vulnerables a prepararse frente al cambio climático.
  - **L.A. 33.** Desarrollar los objetivos del área «paz, seguridad y cohesión social» del Plan Nacional de Adaptación al Cambio Climático 2021-2030 relacionados con la prevención de posibles conflictos mediante su detección temprana, con el fin de reconocer aquellas situaciones que puedan suponer amenazas para la paz y la seguridad internacional.

7.5 EL SISTEMA DE SEGURIDAD NACIONAL Y LA GESTIÓN DE CRISIS (CAP. 5)

El quinto capítulo de la Estrategia presenta un modelo integrado para hacer frente a las situaciones de crisis de forma preventiva, ágil y eficaz en el marco del Sistema de Seguridad Nacional.

El Sistema de Seguridad Nacional es el conjunto de órganos, organismos, recursos y procedimientos que posibilitan la acción del Estado en el ejercicio de las funciones para proteger la libertad y el bienestar de sus ciudadanos, garantizar la defensa de España y sus principios y valores constitucionales, y contribuir junto a socios y aliados a la seguridad internacional.



El avance en integración del Sistema se materializa en seis actuaciones concretas:

1) Elaboración del catálogo de recursos de la Seguridad Nacional.
2) Preparación de planes de respuesta para determinados escenarios.
3) Desarrollo de un sistema de respuesta de alerta temprana y análisis.
4) Integración de la información de la Seguridad Nacional a través de soluciones tecnológicas.
5) Mejora de las comunicaciones de la Presidencia del Gobierno.
6) Integración de las CCAA y las ciudades autónomas de Ceuta y Melilla en el Sistema de Seguridad Nacional.