EUROPEAN UNION AGENCY
FOR CYBERSECURITY

MARCO DE EVALUACIÓN DE LAS CAPACIDADES NACIONALES

DICIEMBRE DE 2020

SOBRE LA ENISA

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada por el Reglamento sobre la Ciberseguridad de la UE, la Agencia de la Unión Europea para la Ciberseguridad contribuye a la política de seguridad cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC mediante programas de certificación de la ciberseguridad, coopera con los Estados miembros y con los organismos de la UE y ayuda a Europa a prepararse para los desafíos del mañana en materia de ciberseguridad. A través del intercambio de conocimientos, la creación de capacidades y la sensibilización, la Agencia coopera con sus principales partes interesadas para fortalecer la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para para mantener la seguridad digital de la sociedad y de los ciudadanos de Europa. Para más información, consulte www.enisa.europa.eu.

DATOS DE CONTACTO

Si desea ponerse en contacto con los autores, rogamos escriba a team@enisa.europa.eu.
Las consultas de los medios de comunicación acerca de este informe deben realizarse a través de press@enisa.europa.eu.

AUTORES:

Anna Sarri, Pinelopi Kyranoudi – Agencia de la Unión Europea para la Ciberseguridad (la ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique - Wavestone

AGRADECIMIENTOS

La ENISA desea expresar su agradecimiento y reconocimiento a todos los expertos que han participado y aportado sus valiosas contribuciones a este informe y en especial los siguientes, por orden alfabético:

Administración de Seguridad de la Información (República de Eslovenia), Marjan Kavčič

Agencia de Tecnología de la Información de Malta (Malta), Katia Bonello y Martin Camilleri

Agencia Nacional de Ciberseguridad y de Ciberinformación (República Checa), Veronika Netolická

Autoridad de Seguridad Nacional (Eslovaquia)

Centro Europeo de Ciberdelincuencia - EC3, Adrian-Ionut Bobeica

Centro Europeo de Ciberdelincuencia - EC3, Alzofra Martínez Álvaro

Centro Nacional de Ciberseguridad de Portugal (Portugal), Alexandre Leite y Pedro Matos

Centro para la Ciberseguridad (Bélgica)

CFCS - Centro para la Ciberseguridad (Dinamarca), Thomas Wulff

Departamento de Seguridad Nacional (España), María Mar López Gil

División de Política de Ciberseguridad, Departamento de Medio Ambiente, Clima y Comunicaciones (Irlanda), James Caffrey

Gobierno de Italia (Italia)

Ministerio de Economía y Comunicaciones (Estonia), Anna-Liisa Pärnalaas

Ministerio de Justicia y Seguridad Pública (Noruega), Robin Bakke

Ministerio de Política Digital (Grecia), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali y Sotiris Vasilos

Ministerio Federal del Interior (Alemania), Sascha-Alexander Lettgen

NCTV, Ministerio de Justicia y Seguridad (Países Bajos)

Oficina Estatal Central para el Desarrollo de la Sociedad Digital (Hungría), Marin Ante Pivcevic

Universidad de Oxford - Centro de Capacidad de Ciberseguridad Mundial, Carolin Weisser Harris

La ENISA también quiere agradecer su valiosa contribución a este estudio a todos los expertos que han participado con sus aportaciones, pero que prefieren permanecer en el anonimato.

AVISO LEGAL

AVISO SOBRE LOS DERECHOS DE AUTOR

ISBN: 978-92-9204-478-7

DOI: 10.2824/895115

CATÁLOGO: TP-02-21-253-ES-N

1. ÍNDICE

GLOSARIO TERMINOLÓGICO

ACRÓNIMO	DEFINICIÓN
AELC	Asociación Europea de Libre Comercio
APD	Aviso sobre protección de datos
APP	Asociaciones público-privadas
ARCC	Acuerdo de reconocimiento de criterios comunes
C2M2	Modelo de madurez de las capacidades en ciberseguridad
CMMC	Certificación del Modelo de Madurez de la Ciberseguridad
CSIRT	Equipos de respuesta a incidentes de seguridad informática
DCV	Divulgación coordinada de la vulnerabilidad
EM	Estado Miembro
ENCS	Estrategias nacionales de ciberseguridad
FEN	Funcionarios de enlace nacionales
GAF-SI ARM	Grupo de Altos Funcionarios para la Seguridad de los Sistemas de Información, Acuerdo de Reconocimiento Mutuo
GECC	Grupo europeo de certificación de la ciberseguridad
I+D	Investigación y Desarrollo
IA	Inteligencia artificial
ICM	Índice de ciberseguridad mundial
ICP	Índice de ciberpoder
IIC	Infraestructura de Información Crítica
INET	Instituto Nacional de Estándares y Tecnología
LEA	Fuerzas o cuerpos de seguridad
MC-AI	Modelo de capacidad de auditoría interna para el sector público
MEC	Marco europeo de cualificaciones
MECS	Mes europeo de la ciberseguridad
MMC	Modelo de madurez de la capacidad de ciberseguridad de las naciones
MMCSC	Modelo de madurez de la ciberseguridad comunitaria
MMSI	Modelo de madurez de seguridad de la Información para el marco de ciberseguridad del INNT
MUD	Mercado único digital

NIS	Seguridad de las Redes y la Información
OECS	Organización Europea para la Ciberseguridad
OSE	Operadores de servicios esenciales
PYMES	Pequeñas Y medianas empresas
Q-C2M2	Modelo catarí de madurez de la capacidad en ciberseguridad
RGPD	Reglamento General de Protección de Datos
SDG	Servicio digital del Gobierno
SGIP	Sistema de gestión de la información de privacidad
TIC	Sector de Tecnologías de la Información y la Comunicación
TMP	Tecnologías para la mejora de la privacidad
TO	Tecnología de operaciones
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones

SÍNTESIS

A medida que el panorama actual de las ciberamenazas sigue extendiéndose y los ciberataques van en aumento en cuanto a intensidad y número, los Estados Miembros de la UE deben responder eficazmente con el desarrollo y la adaptación aún mayor de sus estrategias nacionales de ciberseguridad (ENCS). Desde la publicación de los primeros estudios de la ENISA relacionados con las ENCS en 2012, los Estados miembros de la UE y los países de la AELC han hecho grandes progresos en la elaboración y aplicación de sus estrategias.

Este informe expone la labor que la ENISA ha llevado a cabo para la elaboración de un marco de evaluación de las capacidades Nacionales (MECN).

El marco tiene la finalidad de proporcionar a los Estados Miembros una autoevaluación de su nivel de madurez mediante la evaluación de sus objetivos de ENCS, que les ayudará a mejorar y crear capacidades en materia de ciberseguridad tanto a nivel estratégico como operativo.

En él se esboza una visión representativa sencilla del nivel de madurez de la ciberseguridad del Estado Miembro. El MECN es un instrumento que ayuda a los Estados Miembros a:

- Proporcionar información útil para la elaboración de una estrategia a largo plazo (por ejemplo, buenas prácticas, directrices);
- Ayudar a identificar los elementos que faltan en la ENCS;
- Ayudar a seguir creando capacidades en ciberseguridad;
- Respaldar la responsabilidad de las medidas políticas;
- Dar credibilidad ante el público en general y los asociados internacionales;
- Apoyar la divulgación y mejorar la imagen pública como organización transparente;
- Ayudar a anticipar los problemas que se avecinen;
- Ayudar a identificar los aprendizajes obtenidos y las buenas prácticas;
- Proporcionar una referencia sobre la capacidad de ciberseguridad en toda la UE que propicie los debates; y
- Ayudar a evaluar las capacidades nacionales en ciberseguridad.

Este marco se diseñó con el apoyo de expertos de la ENISA en la materia y representantes de 19 Estados Miembros y países de la AELC[1] El público objetivo de este informe se compone por responsables en la formulación de políticas, expertos y funcionarios gubernamentales o que

[1] Se entrevistó a representantes de los siguientes Estados Miembros y países de la AELC: Alemania, Bélgica, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Grecia, Hungría, Irlanda, Italia, Liechtenstein, Malta, Noruega, Países Bajos, Portugal, República Checa y Suecia.

participan en el diseño, la aplicación y la evaluación de una ENCS y, a un nivel más amplio, de las capacidades en ciberseguridad.

El marco de evaluación de las capacidades nacionales abarca 17 objetivos estratégicos y se estructura en torno a cuatro grupos principales:

- Grupo nº. 1: Gobernabilidad y normas de ciberseguridad
  1. Elaborar un plan nacional de cibercontingencia
  2. Establecer medidas de seguridad de base
  3. Asegurar la identidad digital y fomentar la confianza en los servicios públicos digitales

- Grupo nº. 2: Creación de la capacidad y concienciación
  4. Organizar ejercicios de ciberseguridad
  5. Establecer una capacidad de respuesta a incidentes
  6. Aumentar la concienciación de los usuarios
  7. Reforzar los programas educacionales y de formación
  8. Fomentar la I+D
  9. Incentivar que el sector privado invierta en medidas de seguridad
  10. Mejorar la ciberseguridad de la cadena de suministros

- Grupo nº. 3: Jurídico y normativo
  11. Proteger la infraestructura de la información crítica, los OSE y los LPD
  12. Abordar la ciberdelincuencia
  13. Establecer mecanismos de notificación de incidentes
  14. Reforzar la privacidad y la protección de datos

- Grupo n.º 4: Cooperación
  15. Establecer una asociación público-privada
  16. Institucionalizar la cooperación entre los organismos públicos
  17. Comprometerse con la cooperación internacional

1. INTRODUCCIÓN

La Directiva sobre la Seguridad de las Redes y la Información NIS, publicada en julio de 2016, exige que los Estados Miembros de la UE adopten una estrategia nacional sobre la seguridad de las redes y los sistemas de información, también conocida como ENCS (Estrategia Nacional sobre Ciberseguridad), tal como se establece en los artículos 1 y 7. En este contexto, una ENCS se define como un marco que establece principios estratégicos, directrices, objetivos estratégicos, prioridades, políticas adecuadas y medidas reglamentarias. El objetivo previsto de una ENCS es alcanzar y mantener un alto nivel de seguridad de las redes y de los sistemas que permita así a los Estados Miembros mitigar las posibles amenazas. Además, la ENCS también puede ser un catalizador del desarrollo industrial y del progreso económico y social.

En la Ley de Ciberseguridad de la Unión Europea se establece que la ENISA promoverá la difusión de buenas prácticas en la definición y aplicación de una ENCS a través del respaldo a los Estados Miembros en la adopción de la Directiva NIS y de la reunión de información útil sobre sus experiencias. Con este fin, la ENISA ha elaborado varios instrumentos que ayuden a los Estados Miembros a que elaboren, apliquen y evalúen sus estrategias nacionales de ciberseguridad (ENCS).

Como parte de su mandato, la ENISA tiene el propósito de elaborar un marco de autoevaluación de las capacidades nacionales que midan el nivel de madurez de las diferentes ENCS. Este informe tiene como objetivo la presentación del estudio realizado en la definición del marco de autoevaluación.

1.1 ALCANCE Y OBJETIVOS DEL ESTUDIO

El principal objetivo de este estudio es crear un marco de autoevaluación de las capacidades nacionales (denominado posteriormente como MANC) que mida el nivel de madurez de las capacidades en materia de ciberseguridad de los Estados Miembros. Más concretamente, el marco debe facultar a los Estados Miembros para:

- Dirigir la evaluación de sus capacidades nacionales en ciberseguridad.
- Aumentar la conciencia del nivel de madurez del país;
- Identificar las áreas de mejora; y
- Construir capacidades de ciberseguridad.

Este marco debe ayudar a los Estados Miembros, y en particular a los encargados de formular políticas nacionales, a que realicen un ejercicio de autoevaluación con el fin de mejorar las capacidades nacionales en ciberseguridad.

1.2 ENFOQUE METODOLÓGICO

El enfoque metodológico que se usa para elaborar el marco de autoevaluación de la capacidad nacional se basa en cuatro fases principales:

1. **Investigación documental:** La primera fase consiste en realizar un amplio examen de la bibliografía que reúna las buenas prácticas relativas a la elaboración de un marco de evaluación de la madurez de las estrategias nacionales de ciberseguridad. La investigación documental se centra en un análisis sistemático de los documentos relevantes en creación de la capacidad y definición de estrategias de ciberseguridad, en las ENCS de los Estados Miembros presentes y en una comparación de los modelos de madurez vigentes en materia de ciberseguridad. Se ha llevado a cabo un

ejercicio de referencia sobre los modelos de madurez vigentes con la adopción de un marco de análisis que se han elaborado a los efectos de este estudio. El marco de análisis se basa en la metodología de Becker[2] para la elaboración de modelos de madurez, que establece un modelo de procedimiento genérico y consolidado que diseñe modelos de madurez y proporcione requisitos claros para la elaboración de modelos de madurez. Se siguió adaptando el marco de análisis para satisfacer las necesidades de este estudio.

2. **Recogida de los puntos de vista de los comités de expertos y de los interesados**: Basándose en los datos recogidos a través de la investigación documental y en las conclusiones preliminares relativas al análisis, esta fase consistió en identificar e invitar a determinados expertos, que contaran con experiencia previa, en la elaboración y aplicación de una ENCS o de modelos de madurez. La ENISA se puso en contacto con su Grupo de Expertos en Estrategias de Ciberseguridad Nacional y con los Oficiales de Enlace Nacionales (OEN) para seleccionar a los expertos reputados en la materia de cada Estado Miembro. Además, se entrevistó a algunos expertos que participaban en la elaboración de modelos de madurez. En total se realizaron 22 entrevistas, 19 de las cuales se llevaron a cabo con representantes de organismos de ciberseguridad pertenecientes a diferentes Estados Miembros (y países de la AELC).
3. **Análisis de las aportaciones del inventario:** Los datos que se recogieron mediante la investigación documental y las entrevistas se analizaron posteriormente para que se determinaran las buenas prácticas en el diseño de un marco de autoevaluación que midiera la madurez de las ENCS, para comprender las necesidades de los Estados Miembros y para determinar qué datos pueden recopilarse de manera viable en los diferentes países europeos[3]. Este análisis permitió afinar el modelo preliminar que se elaboró en las etapas anteriores y perfeccionar el conjunto de indicadores que se incluían en el modelo, los niveles de madurez y sus dimensiones.
4. **Finalización del modelo:** A continuación, los expertos en la materia de la ENISA revisaron una versión actualizada del marco de autoevaluación de las capacidades nacionales, que se validó posteriormente por los expertos en un taller que tuvo lugar en octubre de 2020, antes de su publicación.

1.3 PÚBLICO OBJETIVO:

El público objetivo de este informe se compone de responsables en la formulación de políticas, expertos y funcionarios gubernamentales o que participan en el diseño, la aplicación y la evaluación de una ENCS y, a un nivel más amplio, de las capacidades en ciberseguridad. Además, las conclusiones formalizadas en este documento pueden ser de utilidad para los expertos en políticas de ciberseguridad y los investigadores a nivel nacional o europeo.

[2] J. Becker, R. Knackstedt, y J. Pöppelbuß, « Developing Maturity Models for IT Management : A Procedure Model and its Application (Desarrollo de modelos de madurez para la gestión de TI: un modelo de procedimiento y su aplicación)», Business & Information Systems Engineering, vol. 1, no. 3, págs. 213 a 222, junio de 2009.
[3] A los efectos de esta investigación, los «países europeos» a los que se hace referencia en este informe incluyen los 27 Estados miembros de la UE.

2. TRAYECTORIA

2.1 TRABAJOS PRECEDENTES SOBRE LA VIDA ÚTIL DE LA ENCS

Como se establece en la Ley sobre Ciberseguridad de la UE, uno de los principales objetivos de la ENISA es el de respaldar a los Estados Miembros en la elaboración de estrategias nacionales sobre la seguridad de las redes y los sistemas de información, promover la difusión de esas estrategias y vigilar su aplicación. Como parte de su mandato, la ENISA ha elaborado varios documentos sobre este tema con el fin de fomentar el intercambio de buenas prácticas y respaldar la aplicación de las ENCS en toda la UE:

- El documento «Practical guide on the development and execution phase of NCSS, (guía práctica sobre la fase de desarrollo y ejecución de las ENCS)»,[4] publicado en 2012
- El documento «Setting the course for national efforts to strengthen security in cyberspace, (marcar el rumbo de los esfuerzos nacionales en el fortalecimiento de la seguridad en el ciberespacio)»[5], publicado en 2012
- El primer marco de la ENISA para la evaluación de una ENCS de un Estado Miembro publicado[6] en 2014.
- El «Online NCSS Interactive Map, (mapa interactivo de la ENCS en línea)»[7] publicado en 2014.
- The «NCSS Good Practice Guide, (Guía de buenas prácticas de la ENCS)»[8] publicada en 2016.
- La «National Cybersecurity Strategies Evaluation Tool, (herramienta de evaluación de estrategias nacionales de ciberseguridad»[9] publicada en 2018.
- Las «Good practices in innovation on Cybersecurity under the NCSS, (buenas prácticas de innovación en ciberseguridad en el marco de la ENCS)»,[10] publicadas en 2019.

[4] ENCS: Practical Guide on Development and Execution (ENISA, 2012), (guía práctica de desarrollo y ejecución)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] ENCS: «Setting the course for national efforts to strengthen security in cyberspace, (marcar el rumbo de los esfuerzos nacionales en el fortalecimiento de la seguridad en el ciberespacio)» (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] An evaluation framework for NCSS, (marco de evaluación para la ENCS), (ENISA, 2014).
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] National Cybersecurity Strategies - Interactive Map, (estrategias nacionales de ciberseguridad- mapa interactivo), (ENISA, 2014, actualizado en 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Este documento actualiza la guía de 2012: Guía de buenas prácticas de la ENCS: Designing and Implementing National Cybersecurity Strategies, (diseño e implementación de las estrategias nacionales de ciberseguridad), (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] *National Cybersecurity Strategies Evaluation Tool,* (herramienta de evaluación de estrategias nacionales de ciberseguridad (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

ANEXO A ofrece un breve resumen de las principales publicaciones de la ENISA sobre este tema.

Las guías y documentos que se refieren con anterioridad se estudiaron como parte de la investigación documental. Concretamente, la «herramienta de evaluación de las estrategias nacionales de ciberseguridad»[11] es un elemento fundamental del MANC. El MANC se basa en los objetivos que cubre la herramienta de evaluación en línea de la ENCS.

2.2 OBJETIVOS COMUNES QUE SE IDENTIFICAN EN LA ENCS EUROPEA

La disparidad entre los diferentes Estados Miembros hace difícil la identificación de actividades comunes o de planes de acción entre los diferentes contextos nacionales, marcos jurídicos y programas políticos. Sin embargo, la ENCS de los Estados Miembros suele tener objetivos estratégicos que se articulan en torno a los mismos temas. Así pues, basándose en el trabajo anterior de la ENISA y en el análisis de la ENCS de los Estados Miembros, se identificaron 22 objetivos estratégicos. 15 de esos objetivos estratégicos ya se habían identificado en la labor anterior de la ENISA, 2 se añadieron posteriormente a este estudio y se identificaron 5 objetivos que considerar en el futuro.

2.2.1 Objetivos estratégicos comunes cubiertos por los Estados Miembros

Basándose en el trabajo anterior de la ENISA, en concreto en la herramienta de evaluación de estrategias nacionales de ciberseguridad[12], la siguiente tabla muestra el conjunto de 15 objetivos estratégicos que normalmente cubre la ENCS de los Estados Miembros. Los objetivos dibujan el esbozo de la «filosofía nacional» general sobre el tema. Para obtener información adicional sobre los objetivos que se describen a continuación, consulte el informe de la ENISA «NCSS Good Practice Guide, (guía de buenas prácticas de la ENCS)»[13].

Cuadro 1: Objetivos estratégicos comunes que cubren los Estados Miembros en su ENCS

Identificación	Objetivos estratégicos de la ENCS	Propósitos
1	Desarrollar planes nacionales de cibercontingencia	▶ Presentar y explicar los criterios que deben usarse al definir una situación como crisis; ▶ Definir los procesos clave y las acciones para manejar la crisis; y ▶ Definir de manera clara las funciones y responsabilidades de los diferentes implicados durante una cibercrisis. ▶ Presentar y explicar los criterios para que una crisis termine y/o quien tiene la potestad de declararlo.
2	Establecer medidas de seguridad de base	▶ Armonizar las diferentes prácticas que siguen las organizaciones tanto en el sector público como privado. ▶ Crear un lenguaje común entre las autoridades públicas competentes y las organizaciones además de abrir canales de comunicación seguros;

[11] *National Cybersecurity Strategies Evaluation Tool*, (herramienta de evaluación de estrategias nacionales de ciberseguridad (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[12] *National Cybersecurity Strategies Evaluation Tool*, (herramienta de evaluación de estrategias nacionales de ciberseguridad (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Este documento actualiza la guía de 2012: Guía de buenas prácticas de la ENCS: Designing and Implementing National Cybersecurity Strategies, (diseño e implementación de las estrategias nacionales de ciberseguridad), (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Identificación	Objetivos estratégicos de la ENCS	Propósitos
		▶ Permitir que los diferentes interesados comprueben y evalúen sus capacidades en materia de ciberseguridad; ▶ Compartir información sobre buenas prácticas de ciberseguridad en todos los sectores industriales; y ▶ Promover que los interesados den prioridad a sus inversiones en seguridad.
3	Organizar ejercicios de ciberseguridad	▶ Identificar qué hay que probar (planes y procesos, personas, infraestructura, capacidades de respuesta, capacidades de cooperación, comunicación, etc.); ▶ Instaurar un equipo nacional de planificación de ciberejercicios con una potestad clara; e ▶ Incorporar ciberejercicios a la vida útil de la estrategia nacional de ciberseguridad o del plan nacional de cibercontingencia.
4	Establecer una capacidad de respuesta a incidentes	▶ Potestad: Se refiere a los poderes, funciones y responsabilidades que el gobierno respectivo debe asignar al equipo; ▶ Cartera de servicios: Cubre los servicios que un equipo proporciona a su circunscripción o que está utilizando para su propio funcionamiento interno; ▶ Capacidades operativas: Tiene relación con los requisitos técnicos y operativos que debe cumplir un equipo; y ▶ Capacidades de cooperación: Abarcan los requisitos relativos al intercambio de información con otros equipos que no estén comprendidos en las tres categorías anteriores (por ejemplo: los responsables políticos, los militares, los supervisores, los operadores (de infraestructura de información crítica) y las autoridades de vigilancia de la ley.
5	Aumentar la concienciación de los usuarios	▶ Identificar lagunas en los conocimientos con respecto a la ciberseguridad o los temas de seguridad de la información; y ▶ Cerrar las lagunas en los conocimientos mediante el aumento de la concienciación o el desarrollo/fortalecimiento de las bases del conocimiento.
6	Reforzar los programas educacionales y de formación	▶ Mejorar las capacidades operativas de la plantilla actual de seguridad de la información; ▶ Fomentar que los estudiantes se unan y se formen en el campo de la ciberseguridad; ▶ Promover y fomentar las relaciones entre los entornos académicos y la industria de la seguridad de la información; y ▶ Unificar la formación en ciberseguridad con las necesidades empresariales.
7	Fomentar la I+D	▶ Identificar las causas reales de las vulnerabilidades, en vez de reparar su impacto; ▶ Reunir a científicos de diferentes disciplinas para que den soluciones a los problemas multidimensionales y complejos como las ciberamenazas físicas; ▶ Reunir las necesidades de la industria y los hallazgos de la investigación, facilitando así la transición entre teoría y práctica; y ▶ Encontrar las vías, no solo de mantener, sino de aumentar el nivel de ciberseguridad de productos y servicios de apoyo a las infraestructuras cibernéticas vigentes.
8	Incentivar que el sector privado invierta en medidas de seguridad	▶ Identificar posibles incentivos para que las empresas privadas inviertan en medidas de seguridad; e ▶ Incentivar a las empresas para que inviertan en seguridad;
9	Proteger la infraestructura de la información crítica, los OSE y los LPD (IIC)	▶ Identificar la infraestructura de información crítica; e ▶ Identificar y mitigar los riesgos importantes para la IIC.
10	Abordar la ciberdelincuencia	▶ Elaborar leyes sobre ciberdelincuencia; e

Identificación	Objetivos estratégicos de la ENCS	Propósitos
		▶ Incrementar la efectividad de las agencias de protección de la ley.
11	Establecer mecanismos de notificación de incidentes	▶ Estudiar sobre el entorno general de la amenaza; ▶ Evaluar el impacto de los incidentes (por ejemplo: violaciones de la seguridad, fallos en la red, interrupciones del servicio); ▶ Aprender sobre las vulnerabilidades presentes y nuevas y sobre los tipos de ataques; ▶ Actualizar las medidas en materia de seguridad como corresponde; y ▶ Aplicar las disposiciones de la Directiva NIS sobre la notificación de incidentes.
12	Reforzar la privacidad y la protección de datos	▶ Contribuir a reforzar los derechos fundamentales en materia de privacidad y protección de datos.
13	Establecer una asociación público-privada (APP)	▶ Disuadir (para disuadir a los atacantes); ▶ Proteger (utilizar la investigación de nuevas amenazas a la seguridad); ▶ Detectar (utilizar el intercambio de información para hacer frente a nuevas amenazas); ▶ Responder (para proporcionar la capacidad de enfrentarse al impacto inicial de un incidente); y ▶ Recuperarse (para proporcionar la capacidad de reparación tras el impacto final de un incidente).
14	Institucionalizar la cooperación entre los organismos públicos	▶ Aumentar la cooperación entre los organismos públicos con responsabilidades y competencias relacionadas con la ciberseguridad; ▶ Evitar que se superpongan competencias y recursos entre los organismos públicos; y ▶ Mejorar e institucionalizar la cooperación entre los organismos públicos en las diferentes áreas de la ciberseguridad.
15	Comprometerse en la cooperación internacional (no solo con Estados Miembros de la UE)	▶ Beneficiarse de la creación de una base de conocimiento común entre Estados Miembros de la UE; ▶ Crear efectos sinérgicos entre las autoridades nacionales de ciberseguridad; y ▶ Habilitar e incrementar la lucha contra la delincuencia transfronteriza.

2.2.2 Objetivos estratégicos adicionales

Basándose en la investigación documental realizada y en las entrevistas dirigidas por la ENISA, se identificaron objetivos estratégicos adicionales. Los Estados Miembros están abordando cada vez más estos temas en sus ENCS o definiendo planes de acción sobre el mismo tema. También se proporcionan ejemplos de actividades realizadas por los Estados Miembros. Si un ejemplo procede de una fuente pública, se proporciona una referencia. En los casos en que los ejemplos se basan en entrevistas confidenciales con funcionarios de los Estados Miembros de la UE, no se proporcionan referencias.

Se identificaron los siguientes objetivos estratégicos adicionales:

- Mejorar la ciberseguridad de la cadena de suministros; y
- Asegurar la identidad digital y fomentar la confianza en los servicios públicos digitales.

Mejorar la ciberseguridad de la cadena de suministros

Las pequeñas y medianas empresas (PYMES) son la columna vertebral de la economía europea. Representan el 99% de todas las empresas de la UE[14] y se estima que en 2015 las PYMES habían creado alrededor del 85% de los nuevos puestos de trabajo y habían proporcionado dos tercios del empleo total del sector privado en la UE. Además, ya que las PYMES prestan servicios a las grandes empresas y colaboran cada vez más con las administraciones públicas[15], cabe señalar que en el contexto presente de interrelaciones, las PYMES constituyen el eslabón débil de los ciberataques. De hecho, las PYMES son las más expuestas a los ciberataques, pero a menudo no pueden permitirse invertir de forma adecuada en ciberseguridad[16]. Por lo tanto, la mejora de la ciberseguridad de la cadena de suministro debiera llevarse a cabo centrándose en las PYMES.

Además de este enfoque sistémico, los Estados Miembros también pueden hacer hincapié en los esfuerzos en ciberseguridad de los servicios y productos específicos de las TIC que se consideren esenciales: Las tecnologías TIC que se usan en la infraestructura crítica de la información, los mecanismos de seguridad que se aplican en el sector de las telecomunicaciones (controles a nivel de los proveedores de servicios de Internet...), los servicios de confianza que se definen en el reglamento del eIDAS y los proveedores de servicios en la nube. Por ejemplo, en su estrategia nacional de ciberseguridad para 2019-2024[17], Polonia se comprometió a elaborar un sistema nacional de evaluación y certificación de la ciberseguridad como mecanismo de garantía de la calidad en la cadena de suministro. Este sistema de certificación se unificará con el marco de certificación de la Unión Europea para los productos, servicios y procesos digitales TIC establecido por la Ley de ciberseguridad de la Unión Europea (2019/881).

Por lo tanto, es de una importancia enorme proceder a la mejora de la ciberseguridad de la cadena de suministro. Esto puede lograrse si se establecen políticas firmes que promuevan a las PYMES al proporcionarles directrices sobre los requisitos de ciberseguridad en los procedimientos de contratación de la administración pública, al fomentar la cooperación en el sector privado, al crear asociaciones público-privadas (APP), al promover mecanismos de divulgación de la vulnerabilidad coordinados(DVC)[18], al crear un plan de certificación de productos que incluya componentes de ciberseguridad en las iniciativas digitales para las PYMES y al financiar el desarrollo de aptitudes, entre otras cosas.

Asegurar la identidad digital y fomentar la confianza en los servicios públicos digitales

En febrero de 2020, la Comisión expuso su visión de la transformación digital de la UE en la comunicación «Shaping Europe's digital future», (Configurar el futuro digital de Europa)[19], con el objetivo de ofrecer tecnologías inclusivas que funcionen para las personas y respeten los valores fundamentales de la UE. Concretamente, en la comunicación se afirma que es fundamental promover la transformación digital de las administraciones públicas en toda Europa. En ese sentido, es de una gran importancia fomentar la confianza en el gobierno en relación con la identidad digital y en los servicios públicos. Esto es aún más vital si se tiene en cuenta que las transacciones y los intercambios de datos del sector público suelen ser de carácter sensible.

Muchos países han manifestado su intención de abordar este tema en su ENCS, en concreto: Dinamarca, España, Estonia, Francia, Luxemburgo, Malta, Países Bajos y Reino Unido. Entre

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16] https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Shaping Europe's digital future, (Configurar el futuro digital de Europa), COM(2020) 67 final: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

estos países, algunos también han expresado que este objetivo estratégico podría abordarse como parte de un plan más amplio:

- Estonia vincula su plan de acción sobre «la seguridad de la identidad electrónica y la capacidad de autenticación electrónica» al Programa Digital 2020 para Estonia, de carácter más amplio.
- La ENCS francesa indica que el Secretario de Estado encargado de la tecnología digital supervisa que se establezca una hoja de ruta «que proteja la vida digital, la privacidad y los datos personales de los franceses».
- La ENCS de los Países Bajos afirma que la ciberseguridad en las administraciones públicas, así como los servicios públicos que se prestan a los ciudadanos y a las empresas se examinan con mayor detalle en la Agenda Ampliada para el Gobierno Digital.
- A medida que el Gobierno del Reino Unido continúa instaurando más servicios en línea, ha designado al Servicio Digital Gubernamental (SDG) para que garantice que todos los nuevos servicios digitales que el gobierno construye o adquiere sean también «seguros por defecto», con el apoyo del Centro Nacional Británico de Ciberseguridad (CNBC).

2.2.3 Otros objetivos estratégicos que se consideran

Durante la fase de investigación documental y como parte de las entrevistas dirigidas por la ENISA se estudiaron otros objetivos estratégicos. Sin embargo, se decidió que esos objetivos no formarían parte del marco de autoevaluación. ANEXO C - Otros objetivos de estudio

proporciona definiciones para cada uno de estos objetivos que pueden utilizarse para alimentar debates futuros sobre posibles mejoras de la ENCS.

Se estudiaron los siguientes objetivos estratégicos como consideraciones futuras:

- Desarrollar estrategias de ciberseguridad específicas para cada sector.
- Luchar contra las campañas de desinformación.
- Asegurar las tecnologías de vanguardia (5G, IA, informática cuántica...);
- Garantizar la soberanía de los datos; y
- Proporcionar incentivos para el desarrollo de la industria de los ciberseguros.

2.3 LAS PRINCIPALES CONCLUSIONES DEL EJERCICIO DE REFERENCIA

La investigación documental sobre los modelos de madurez vigentes relacionados con la ciberseguridad se llevó a cabo con el objetivo de reunir información y pruebas que respaldaran el diseño del marco de autoevaluación de la capacidad nacional de la ENCS. En este contexto, se llevó a cabo un amplio examen de la bibliografía sobre los modelos vigentes que complementara las conclusiones de la investigación inicial sobre el alcance de los modelos de madurez de ciberseguridad y la ENCS que se desarrollan en los apartados 2.1 y 2.2. Este examen sistemático respalda la selección y la justificación de los niveles de madurez del marco de evaluación y la definición de las diferentes dimensiones e indicadores.

En el alcance del examen sistemático de los modelos de madurez, se examinaron y se analizaron 10 modelos que se basaban en sus características principales. El resumen general de las características fundamentales de cada modelo que se revisó en el alcance de este estudio puede consultarse en Cuadro 2: Resumen de los modelos **de** madurez analizados y se puede encontrar un análisis más detallado en ANEXO A.

Cuadro 2: Resumen de los modelos de madurez analizados

Nombre del modelo	N.º de niveles de madurez	N. º de características	Método de evaluación	Representación de los resultados
Modelo de madurez de la capacidad de ciberseguridad de las naciones (CMM)	5	5 dimensiones principales	Colaboración con una institución local para afinar el modelo antes de aplicarlo al contexto nacional	radar de 5 apartados
Modelo de madurez de las capacidades en ciberseguridad(C2M2)	4	10 dominios principales	Metodología de autoevaluación y conjunto de herramientas	Tarjeta de puntuación con gráficos circulares
Marco para la mejora de las infraestructuras críticas en ciberseguridad	n/d (4 niveles)	5 funciones básicas	Autoevaluación	n/d
Modelo catarí de madurez de la capacidad en ciberseguridad(Q-C2M2)	5	5 dominios principales	n/d	n/d
Certificación del modelo de madurez de la ciberseguridad (CMMC)	5	17 dominios principales	Evaluación por parte de auditores externos	n/d
Modelo de madurez de la ciberseguridad comunitaria (CCSMM)	5	6 dimensiones principales	Evaluación dentro de las comunidades con la aportación del estado y las fuerzas o cuerpos de seguridad federales	n/d
Modelo de madurez de seguridad de la Información para el marco de ciberseguridad del INNT(Simposio internacional sobre la gestión de la fabricación)	5	23 áreas evaluadas	n/d	n/d
Modelo de capacidad de auditoría interna (MC-AI) para el sector público	5	6 elementos	Autoevaluación	n/d
Índice de Ciberseguridad Mundial (ICM)	N/A	5 columnas	Autoevaluación	Tabla de clasificación
El Índice de Ciberpoder (ICP)	N/A	4 categorías	Proceso de análisis comparativo de la Unidad de Inteligencia de *The Economist*	Tabla de clasificación

Este examen sistemático permitió sacar conclusiones sobre las buenas prácticas adoptadas en los modelos vigentes para que se respalde la elaboración del modelo conceptual para el modelo de madurez actual. Concretamente, el ejercicio de análisis comparativo respaldó la definición de los niveles de madurez, la creación de grupos de aspectos y la selección de indicadores, así como una metodología de visualización adecuada para los resultados del modelo. Los resultados más relevantes de cada uno de estos elementos se detallan en Cuadro 3.

Cuadro 3: Principales conclusiones del ejercicio de análisis comparativo

Aspecto	Resultado clave
Niveles de madurez	▶ Por lo general, se acepta una escala de madurez de cinco niveles en los marcos de evaluación de las capacidades de ciberseguridad y se pueden proporcionar resultados de evaluación granulares (véase Tabla 6 Comparativa de los niveles de madurez para obtener un punto de vista exhaustivo sobre la definición de los niveles de madurez para cada modelo); ▶ Todos los modelos proporcionan una definición de alta calidad respecto a cada nivel de madurez que luego se adapta a los diferentes aspectos o grupos de aspectos; ▶ Al medir la madurez de las capacidades de ciberseguridad se suelen evaluar dos aspectos principales: la madurez de las estrategias y la madurez de los procesos establecidos para aplicar las estrategias.
Características	▶ El análisis comparativo de las características de los modelos de madurez existentes muestra resultados heterogéneos con un número medio de atributos por modelo de entre cuatro y cinco; ▶ Un modelo basado en unos cuatro o cinco atributos proporciona a los países el nivel adecuado de granularidad de los datos al agrupar las dimensiones relevantes y asegurar la legibilidad de los resultados (véase Cuadro 7: Comparativa de características/**dimensiones** para obtener la descripción de las características de cada modelo); ▶ El principio clave que adoptan todos los modelos cuando definen los grupos se basa en la consistencia de los elementos que se reúnen en cada grupo.
Método de evaluación	▶ Los métodos de evaluación que se usan en los diferentes modelos que se analizan varían de uno a otro; ▶ El método de evaluación más corriente se basa en la autoevaluación.
Representación de los resultados	▶ Es importante presentar los resultados a niveles diferentes de granularidad; ▶ La metodología de visualización debe explicarse por ella misma y debe ser fácil de leer.

El modelo conceptual se construyó sobre la base del ejercicio de análisis comparativo de los diferentes modelos de madurez, así como sobre el trabajo anterior de la ENISA. *Además, se decidió aprovechar la herramienta interactiva en línea de la ENISA para desarrollar los indicadores de madurez que se utilizan para cada característica.*

2.4 DESAFÍOS DE LA EVALUACIÓN DE LA ENCS

Los Estados Miembros se enfrentan a muchos desafíos a la hora de crear capacidades de ciberseguridad y, más concretamente, a la hora de garantizar que sus capacidades estén al día en relación con los últimos avances. A continuación, se presenta un resumen de los retos identificados y examinados por los Estados Miembros como parte de este estudio:

- **Dificultades de coordinación y cooperación:** Los esfuerzos al coordinar las actividades de ciberseguridad a nivel nacional para ser capaces de responder con eficacia a los asuntos de ciberseguridad pueden resultar un reto debido al alto número de interesados que intervienen.
- **Falta de recursos para realizar la evaluación:** Dependiendo del contexto local y de la estructura nacional de gobernabilidad en ciberseguridad, la evaluación de la ENCS y sus objetivos pueden necesitar a más de 15 personas trabajando durante una jornada.
- **Falta de apoyo para el desarrollo de capacidades en ciberseguridad:** Algunos Estados Miembros han expresado que para defender un presupuesto y obtener respaldo en el desarrollo de las capacidades en ciberseguridad, primero tienen que

llevar a cabo una fase de evaluación que determine las lagunas de conocimiento y las limitaciones.

- **Dificultades en atribuir los éxitos o los cambios a la estrategia:** Ya que las amenazas evolucionan a diario y la tecnología mejora, deben adaptarse los planes de acción como respuesta. Sin embargo, evaluar una ENCS y atribuir los cambios a la estrategia en si misma sigue siendo una tarea ardua. Esto a su vez dificulta la identificación de las limitaciones y deficiencias de la ENCS.
- **Dificultades en la medición de la eficacia de la ENCS:** Se pueden recoger datos que midan diferentes baremos como el progreso, la aplicación, la madurez y la eficacia. Si bien la medición de los progresos y la aplicación es relativamente sencilla en comparación con la medición de la eficacia, esta última sigue siendo más significativa al evaluar los resultados y los efectos de una ENCS. Basándose en las entrevistas realizadas por la ENISA, un gran número de Estados Miembros declaró que es importante la medición cuantitativa de la eficacia de una ENCS , pero también que representa una tarea muy exigente, casi imposible en algunos casos.
- **Dificultades para la adopción de un marco de trabajo común:** Los Estados miembros de la UE operan en contextos diferentes en cuanto a política, organizaciones, cultura, estructura de la sociedad y madurez de la ENCS. Algunos Estados Miembros entrevistados como parte de este estudio expresaron que podría resultar difícil defender y utilizar un marco de autoevaluación de «talla única».

2.5 BENEFICIOS DE UNA EVALUACIÓN DE LAS CAPACIDADES NACIONALES

Desde 2017, todos los Estados Miembros de la UE tienen una ENCS[20]. Si bien se trata de un avance positivo, también es importante que los Estados Miembros puedan evaluar adecuadamente estas ENCS de manera que aporten un valor añadido a su planificación estratégica y a su aplicación.

Uno de los objetivos del marco de evaluación de las capacidades nacionales es el de evaluar las capacidades de ciberseguridad basándose en las prioridades establecidas en las diversas ENCS. Principalmente, el marco evalúa el nivel de madurez de las capacidades de ciberseguridad de los Estados Miembros en los ámbitos definidos por los objetivos de la ENCS. Por lo tanto, los resultados del marco sirven de respaldo a los responsables de la elaboración de las políticas de los Estados Miembros para que definan la estrategia nacional en ciberseguridad al proporcionarles información sobre el estado de los países[21]. En última instancia, el MANC tiene la finalidad de ayudar a los Estados Miembros a que determinen las áreas de mejora y a que creen capacidades.

El marco tiene la finalidad de proporcionar a los Estados Miembros una autoevaluación de su nivel de madurez mediante la evaluación de sus objetivos de ENCS que les ayudará a mejorar y crear capacidades en materia de ciberseguridad tanto a nivel estratégico como operativo.

Sobre un enfoque más práctico, se identificaron y destacaron los siguientes beneficios del MECN basándose en las entrevistas que realizó la ENISA a varios organismos responsables del ámbito de la ciberseguridad en diferentes Estados Miembros:

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). The interface between evaluation and public policy, (la interfaz entre evaluación y políticas públicas). Evaluation (evaluación), 5(4), 468-486.

- Proporcionar información útil para la elaboración de una estrategia a largo plazo (por ejemplo, buenas prácticas, directrices);
- Ayudar a identificar los elementos que faltan en la ENCS;
- Ayudar a seguir creando capacidades en ciberseguridad;
- Respaldar la responsabilidad de las medidas políticas;
- Dar credibilidad ante el público en general y los asociados internacionales;
- Apoyar la divulgación y mejorar la imagen pública como organización transparente;
- Ayudar a anticipar los problemas que se avecinen;
- Ayudar a identificar los aprendizajes obtenidos y las buenas prácticas;
- Proporcionar una base de referencia sobre la capacidad de ciberseguridad en toda la UE para propiciar debates; y
- Ayudar a evaluar las capacidades nacionales en ciberseguridad.

3. METODOLOGÍA DEL MARCO DE EVALUACIÓN DE LAS CAPACIDADES NACIONALES

3.1 OBJETIVO GENERAL

El **principal objetivo** de la FNCA es medir el nivel de madurez de las capacidades en materia de ciberseguridad de los **Estados Miembros** para respaldarles en la realización de una evaluación de su capacidad nacional en ciberseguridad, aumentar la concienciación sobre el nivel de madurez del país, determinar las áreas de mejora y crear capacidades de ciberseguridad.

3.2 NIVEL DE MADUREZ:

El marco se estructura en **cinco niveles de madurez** que definen las etapas por las que pasan los Estados Miembros cuando crean las capacidades de ciberseguridad en el área que abarca cada objetivo de la ENCS. Los niveles representan niveles de madurez cada vez mayores, empezando por el primero, **Nivel 1**, en el que los Estados Miembros no tienen un planteamiento claro en la manera de definir la capacidad en ciberseguridad en las áreas que abarcan los objetivos de la ENCS y finalizando por el Nivel 5, en el que la estrategia de creación de capacidad en materia de ciberseguridad es dinámica y se adapta a la evolución del entorno. Cuadro 4 muestra la escala de niveles de madurez con una descripción de cada nivel de madurez.

Cuadro 4: Escala de madurez de cinco niveles del marco de evaluación de las capacidades nacionales de la ENISA

NiIVEL 1- INICIAL/ AD HOC	NIVEL 2- DEFINICIÓN TEMPRANA	NIVEL 3- ESTABLECIMIENTO	NIVEL 4- OPTIMIZACIÓN	NIVEL 5- ADAPTABILIDAD
El Estado Miembro no tiene un planteamiento claro al definir la creación de capacidad de ciberseguridad en las áreas que abarcan los objetivos de la ENCS. No obstante, el país podría tener algunos objetivos genéricos y haber realizado algunos estudios (técnicos, políticos, de política) para mejorar las capacidades nacionales.	Se ha definido el planteamiento nacional para el fomento de la capacidad en el área que abarcan los objetivos de la ENCS. Los planes de acción o las actividades para alcanzar los resultados están en marcha pero en una fase inicial. Además, es posible que se hayan identificado y/o comprometido los interesados que participen.	El plan de acción para la creación de la capacidad en el área que abarcan los objetivos de la ENCS de ha definido de manera clara y cuenta con el respaldo de los interesados que participen. Las prácticas y actividades se aplican y se ejecutan de manera uniforme a nivel nacional. Las actividades se definen y se documentan con una asignación de recursos y de gestión claras y un número de plazos.	El plan de acción se evalúa periódicamente: se le asigna un orden de prioridad, se optimiza y es sostenible. Se mide periódicamente el rendimiento de las actividades de creación de capacidad en ciberseguridad. Se identifican los factores de éxito, los retos y las lagunas de conocimiento en la ejecución de las actividades.	La estrategia de creación de la capacidad en ciberseguridad es dinámica y adaptable. La atención constante a la evolución del medio ambiente (avances tecnológicos, conflictos mundiales, nuevas amenazas...) fomenta la toma de decisiones rápida y la capacidad de realizar mejoras con celeridad.

3.3 GRUPOS Y ESTRUCTURA GENERAL DEL MARCO DE AUTOEVALUACIÓN

El marco de autoevaluación se compone por **cuatro grupos**: I) Gobernabilidad de ciberseguridad y normas , II) Creación de capacidad y concienciación, III) Jurídico y normativo y IV) Cooperación. Cada uno de esos grupos abarca un área temática fundamental para la creación de capacidad en ciberseguridad de un país y contiene un conjunto de objetivos diversos que los Estados Miembros podrían incluir en su ENCS. En concreto:

- **(I) Gobernabilidad de ciberseguridad y normas**: este grupo mide la capacidad de los Estados Miembros para que establezcan la gobernanza, las normas y las buenas prácticas apropiadas en el ámbito de la ciberseguridad. Este nivel tiene en cuenta diferentes aspectos de la ciberdefensa y la resiliencia, a la vez que respalda el desarrollo de la industria nacional de la ciberseguridad y fomenta la confianza en los gobiernos;
- **(II) Creación de capacidades y concienciación:** este grupo evalúa la capacidad de los Estados Miembros para que aumenten la conciencia sobre los riesgos y amenazas a la ciberseguridad y sobre la forma de hacerles frente. Además, este apartado mide la capacidad del país para crear constantemente capacidades en materia de ciberseguridad y aumentar el nivel general de conocimientos y aptitudes en este ámbito. Se aborda el desarrollo del mercado de la ciberseguridad y los avances en la investigación y el desarrollo de la ciberseguridad. En este grupo se reúnen todos los objetivos que componen los cimientos para fomentar la creación de capacidad;
- **(III) Jurídico y normativo:** este grupo mide la capacidad de los Estados Miembros para establecer los instrumentos jurídicos y reglamentarios necesarios que hagan frente y contrarresten el aumento de la ciberdelincuencia y de los ciberincidentes relacionados, así como la protección de la infraestructura de información crítica.

Además, en este nivel se evalúa también la capacidad de los Estados Miembros de crear un marco jurídico que proteja a los ciudadanos y las empresas como, por ejemplo, en el caso de equilibrar la seguridad con la privacidad; y

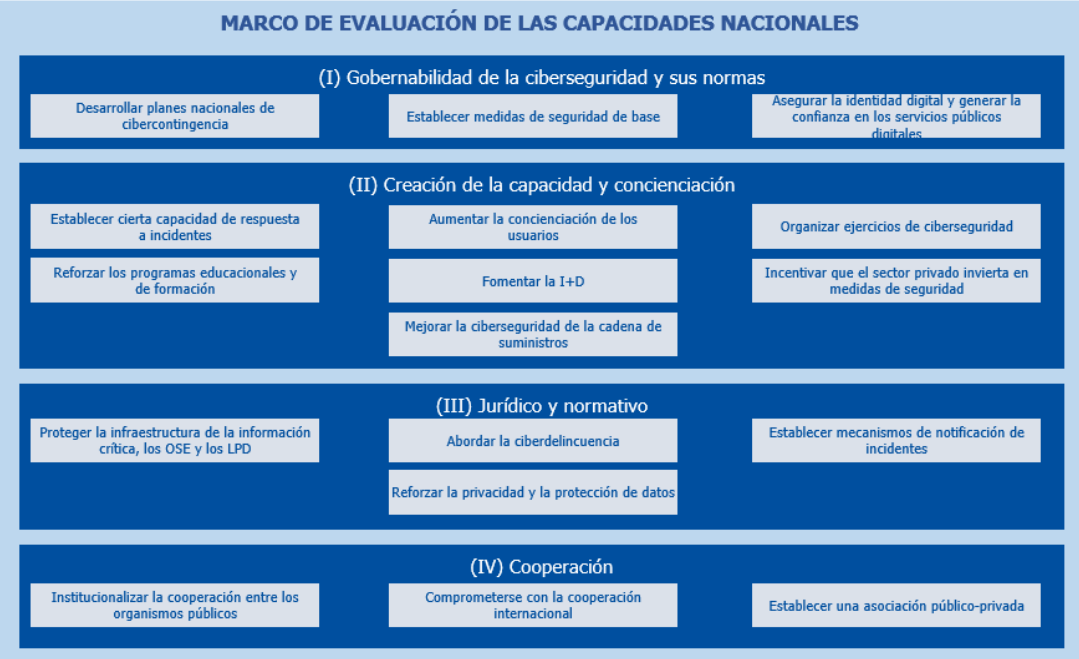
- **(IV) Cooperación:** este grupo evalúa la cooperación y el intercambio de información entre los diferentes grupos de interesados a nivel nacional e internacional al ser un instrumento importante para comprender mejor y dar respuesta a un entorno de amenazas en evolución continua.

Los objetivos que se han incluido en el modelo son los que normalmente adoptan los Estados Miembros y se han seleccionado entre los objetivos enumerados en el apartado 2.2. En concreto, el modelo evalúa los siguientes objetivos:

- 1. Desarrollar planes nacionales de cibercontingencia (I)
- 2. Establecer medidas de seguridad de base (*I*)
- 3. Asegurar la identidad digital y fomentar la confianza en los servicios públicos digitales (I)
- 4. Establecer una capacidad de respuesta a incidentes(II)
- 5. Aumentar la concienciación de los usuarios(II)
- 6. Organizar ejercicios de ciberseguridad(II)
- 7. Reforzar los programas educacionales y de formación(II)
- 8. Fomentar la I+D
- 9. Incentivar que el sector privado invierta en medidas de seguridad(II)
- 10. Mejorar la ciberseguridad de la cadena de suministros(II)
- 11. Proteger la infraestructura de la información crítica, los OSE y los LPD (IIC)
- 12. Abordar la ciberdelincuencia(III)
- 13. Establecer mecanismos de notificación de incidentes(III)
- 14. Reforzar la privacidad y la protección de datos(III)
- 15. Institucionalizar la cooperación entre los organismos públicos(IV)
- 16. Comprometerse con la cooperación internacional(IV)
- 17. Establecer una asociación público-privada(IV)

Los cuatro grupos y los objetivos subyacentes en el modelo se combinan para obtener una visión holística de la madurez de las capacidades de ciberseguridad de los Estados Miembros. Figura 1 presenta la estructura general del marco de autoevaluación y muestra cómo estos elementos (es decir, los objetivos, los grupos y el marco de autoevaluación) se vinculan a la evaluación del desempeño de un país.

Figura 1: Estructura del marco de autoevaluación



Para cada objetivo que se incluye en el marco de autoevaluación, hay una serie de indicadores distribuidos entre los cinco niveles de madurez.. Cada indicador se basa en una pregunta dicotómica (sí/no). El indicador puede ser un requisito o un no requisito.

3.4 MECANISMO DE PUNTUACIÓN

El mecanismo de puntuación del marco de autoevaluación tiene en cuenta los elementos anteriores y los principios que se enumeran en el apartado 3.5. De hecho, el modelo proporciona una puntuación basada en el valor de dos parámetros, el **nivel de madurez** y la **tasa de cobertura**. Cada uno de estos parámetros puede calcularse en diferentes niveles: i) por objetivo, ii) por grupo de objetivos o iii) general.

Puntuaciones a nivel de objetivo

La **puntuación del nivel de madurez** ofrece una visión general del nivel de madurez al mostrar qué capacidades y prácticas se han puesto en marcha. La puntuación del nivel de madurez se calcula como el nivel más alto para el que el encuestado cumplió con todos los requisitos (es decir, respuesta «SÍ» a todas las preguntas formuladas), además de haber cumplido todos los requisitos de los niveles de madurez anteriores.

La **tasa de cobertura** muestra el radio de cobertura de todos los indicadores para los que la respuesta es positiva, independientemente de su nivel. Es un valor complementario que tiene en cuenta todos los indicadores que miden un objetivo. La tasa de cobertura se calcula como la proporción entre el número total de preguntas dentro del objetivo y el número de preguntas para las que la respuesta es positiva

Es importante aclarar que para el resto del documento, la palabra **puntuación** se utiliza para referirse tanto a los valores del nivel de madurez como a la tasa de cobertura.

Figura 2 : El mecanismo de puntuación por objetivo proporciona una visualización del mecanismo de evaluación que se describe en el apartado 3.1 que se desarrollará más adelante.

Figura 2: Mecanismo de puntuación por objetivo

Figura 2 muestra un ejemplo de cómo se calcula el nivel de madurez por objetivo. Cabe señalar que el encuestado cumplió todos los requisitos de los tres primeros niveles de madurez y sólo cumplió parcialmente los del nivel 4. Por lo tanto, la puntuación indica que el ***nivel de madurez del encuestado es el Nivel 3 para el objetivo «organizar el ejercicio de ciberseguridad»****.*

Sin embargo, en el ejemplo representado en Figura 2, el nivel de madurez del objetivo no es capaz de captar la información proporcionada por los indicadores que tienen una puntuación positiva y que están por encima del nivel 3 de madurez. En ese caso, la tasa de cobertura puede proporcionar una visión general de todos los elementos que el encuestado implementó para lograr ese objetivo, a pesar de su nivel real de madurez. En este caso, la proporción entre el número total de preguntas dentro del objetivo y el número de preguntas para las que la respuesta es positiva es igual a 19/27, es decir, ***el valor de la tasa de cobertura es del 70%.***

Además, para adaptarse a las especificidades de los Estados Miembros y permitir al mismo tiempo una visión general coherente, la puntuación se calcula a partir de dos muestras diferentes a nivel de grupo y a nivel general:

- **Puntuaciones generales:** una muestra completa que abarca todos los objetivos incluidos en el grupo o dentro del marco general (del 1 al 17);
- **Puntuaciones específicas:** una muestra específica que abarca únicamente los objetivos seleccionados por el Estado Miembro (que suelen corresponderse con los objetivos presentes en la ENCS del país concreto) dentro del grupo o en el marco general.

Puntuaciones a nivel del grupo

El **nivel general de madurez de cada grupo** se calcula como la media aritmética del nivel de madurez de todos los objetivos de ese grupo.

El **nivel de madurez específico de cada grupo** se calcula como la media aritmética del nivel de madurez de los objetivos de ese grupo, que el Estado Miembro ha decidido evaluar (que suele corresponder a los objetivos actuales en la ENCS del país concreto).

Por ejemplo, *Figura 1* muestra que el grupo (I) Gobernabilidad y normas de ciberseguridad se compone de tres objetivos. *Suponiendo que el encuestado opta por evaluar sólo los dos primeros objetivos, pero no el tercero, y suponiendo que los dos primeros objetivos presentan respectivamente un nivel de madurez de 2 y 4, entonces el nivel de madurez del grupo que considera todos los objetivos es de nivel 2 (nivel de madurez genérico de la agrupación (I) = (2+4)/3), mientras que el nivel de madurez del grupo que considera solo los objetivos específicos seleccionados por el encuestador es de nivel 3 (nivel de madurez específico de la agrupación (I) = (2+4)/2).*

La **tasa de cobertura general de cada grupo** se calcula como la proporción entre el número total de preguntas dentro del agregado de defectos y el número de preguntas para las que la respuesta es positiva

La **tasa de cobertura específica de cada grupo** se calcula como la proporción entre el número total de preguntas del grupo correspondientes a los objetivos que el Estado Miembro ha decidido evaluar (que suelen corresponder a los objetivos presentes en la ENCS del país concreto) y el número de preguntas para las que la respuesta es positiva.

Puntuaciones a nivel total

El **nivel total general de madurez de un país** se calcula como la media aritmética del nivel de madurez de todos los objetivos del marco, del 1 al 17.

El **nivel total específico de madurez de un país** se calcula como la media aritmética del nivel de madurez de los objetivos dentro del marco que el Estado Miembro ha decidido evaluar (que normalmente corresponde a los objetivos presentes en la ENCS del país concreto).

La tasa de cobertura total general de un país se calcula como la proporción entre el número total de preguntas dentro de todos los objetivos incluidos en el marco (del 1 al 17) y el número de preguntas para las que la respuesta es positiva.

La **tasa de cobertura general específica de un país** se calcula como la proporción entre el número total de preguntas dentro de los objetivos incluidos en el marco que el Estado Miembro haya decidido evaluar (que suelen corresponderse con los objetivos presentes en la ENCS del país concreto) y el número de preguntas para las que la respuesta es positiva.

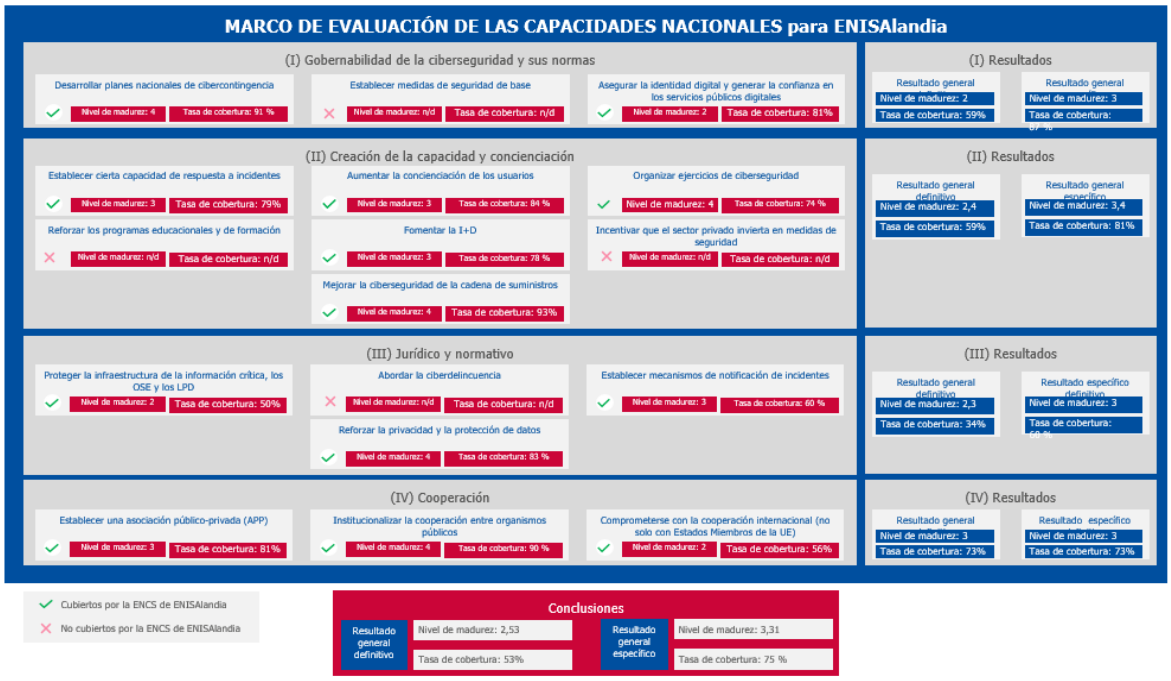
Para cada indicador, los encuestados pueden seleccionar una tercera opción «no sabe/no aplica» en su respuesta. En este caso, el indicador se excluye del cálculo total de los resultados.

Los niveles de madurez a nivel de grupo y a nivel general se calculan con una media aritmética que muestre el progreso entre dos evaluaciones. De hecho, la alternativa que consiste en calcular el grupo y los niveles de madurez como el nivel de madurez del objetivo menos maduro -aunque pertinente desde el punto de vista de la madurez- no puede sumar en los progresos que se hayan hecho en las áreas que cubren otros objetivos.

Dado que el nivel de grupo y el nivel general están consolidados a efectos de presentación de informes, se ha optado por utilizar la media aritmética. Para mayor exactitud, se ruega utilizar las puntuaciones a nivel de objetivo a efectos de la presentación de informes.

En la figura 3 que figura a continuación se resumen los mecanismos de puntuación en los diferentes niveles del modelo (objetivo, grupo, total).

Figura 3: Mecanismo total de puntuación



3.5 REQUISITOS DEL MARCO DE AUTOEVALUACIÓN

El marco de evaluación de la capacidad nacional que se presenta en esta sección se basa en las necesidades que destacan los Estados Miembros y se construye en torno a un conjunto de requisitos que se enumeran a continuación:

- El Estado Miembro implanta el MACN de manera voluntaria como marco de autoevaluación;
- El MANC tiene como objetivo medir la capacidad de los Estados Miembros en materia de ciberseguridad en relación con los 17 objetivos. Sin embargo, el Estado Miembro puede elegir los objetivos que desee evaluar y evaluar únicamente un subconjunto de los 17 objetivos;
- El marco de autoevaluación tiene como objetivo medir el nivel de madurez de las capacidades en ciberseguridad del Estado Miembro;
- Los resultados de la evaluación no se publican, a menos que el Estado Miembro decida hacerlo por iniciativa propia;
- El Estado Miembro puede mostrar los resultados de la evaluación al presentar el nivel de madurez de las capacidades en ciberseguridad del país, de un grupo de objetivos o incluso de un único objetivo;
- Todos los objetivos que se evalúan son igual de relevantes dentro del marco de evaluación, por lo que tienen la misma importancia. Lo mismo cabe decir de los indicadores implantados en él; y
- El Estado Miembro puede hacer un seguimiento de sus avances en el tiempo.

El marco de autoevaluación tiene por finalidad respaldar a los Estados Miembros en la creación de capacidades en ciberseguridad, por lo que también incluye un conjunto de recomendaciones o directrices que orienten a los países europeos en la mejora de su nivel de madurez.

Nota: esas recomendaciones o directrices son genéricas; se basan en las publicaciones de la ENISA y en lo aprendido en otros países, así como en el resultado de la autoevaluación.

4. INDICADORES MANC

4.1 INDICADORES DEL MARCO

En este apartado se presentan los indicadores del marco de evaluación de las capacidades nacionales de la ENISA. Las siguientes secciones se organizan en grupos.

Para cada grupo hay una tabla que muestra el conjunto completo de indicadores en forma de preguntas representativas de un determinado nivel de madurez. El cuestionario es el principal instrumento para hacer la autoevaluación. Por cada objetivo, hay dos conjuntos de indicadores que deben tenerse en cuenta:

- Un conjunto de preguntas genéricas de madurez estratégica(9 preguntas genéricas), marcadas de la «a» a la «c» para cada nivel de madurez que se repiten para cada objetivo; y
- Un conjunto de preguntas sobre la capacidad en materia de ciberseguridad (319 preguntas sobre la capacidad de ciberseguridad), numeradas del «1» al «10» para cada nivel de madurez que son específicas del área que cubre el objetivo.

Cada pregunta se presenta con una etiqueta (0-1) que indica si la pregunta es un indicador de requisito (1) o un indicador de no requisito (0) para el nivel de madurez.

Cada pregunta se identifica con un número de identificación compuesto por:

- El número objetivo;
- El nivel de madurez; y
- El número de pregunta.

Por ejemplo, la pregunta ID 1.2.4 es la cuarta pregunta del nivel de madurez 2 del objetivo estratégico (I) «Elaborar planes nacionales de cibercontingencia».

Cabe señalar que a lo largo del cuestionario, el alcance de las preguntas es a nivel nacional, a menos que se indique lo contrario. En todas las preguntas, el pronombre «usted» se refiere al Estado Miembro de manera genérica y no a la persona u organismo gubernamental que realiza la evaluación.

La definición de cada objetivo se encuentra en el capítulo 2.2 - Objetivos comunes que se identifican en la ENCS europea

4.1.1 Grupo nº. 1: Gobernabilidad y normas de ciberseguridad

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
1 – Desarrollar planes nacionales de cibercontingencia	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Ha empezado a trabajar en la creación de planes nacionales de cibercontingencia? Por ejemplo: estableciendo los objetivos generales, el alcance y/o los principios de los planes de contingencia...	1	¿Tiene una doctrina/estrategia nacional que incluya la ciberseguridad como factor de crisis (es decir, un plan, una política, etc.)?	1	¿Tiene un plan de gestión de cibercrisis a nivel nacional?	1	¿Está satisfecho con el número o el porcentaje de sectores críticos que incluye el plan nacional de cibercontingencia?	1	¿Tiene en marcha un proceso de aprendizaje después de los ciberejercicios o de las crisis reales a nivel nacional?	1
	2	¿Se entiende, por lo general, que los ciberincidentes constituyen un factor de crisis que podría amenazar la seguridad nacional?	0	¿Tiene un centro para adquirir información e informar a los responsables de la toma de decisiones? Es decir, cualquier método, plataforma o lugar que garantice que todos los involucrados en dar respuesta a la crisis puedan acceder a la misma información a tiempo real sobre la cibercrisis.	1	¿Tiene procedimientos específicos para las cibercrisis a nivel nacional?	1	¿Organiza actividades (por ejemplo, ejercicios) relacionadas con la planificación nacional de cibercontingencias con la frecuencia suficiente?	1	¿Tiene un proceso para probar el plan nacional de manera periódica?	1
	3	¿Se han realizado estudios (técnicos, operacionales, políticos) en el ámbito de la planificación de cibercontingencias?	0	¿Se dedican los recursos correspondientes a la supervisión de la elaboración y ejecución de planes nacionales de cibercontingencia?	1	¿Tiene un equipo de comunicaciones entrenado especialmente para responder a las cibercrisis e informar al público?	1	¿Tiene suficientes personas dedicadas a la planificación de la crisis, a observar los aprendizajes obtenidos y a implementar el cambio?	1	¿Tiene herramientas y plataformas apropiadas para concienciar de la situación?	1
	4	-		¿Tiene una metodología de evaluación de la ciberamenaza a nivel nacional que incluya procedimientos que evalúen el impacto?	0	¿Involucra a todos los interesados nacionales relevantes (seguridad nacional, defensa, protección civil, cumplimiento de la ley, ministerios, autoridades, etc.)?	1	¿Cuenta con suficientes personas capacitadas para responder a las cibercrisis a nivel nacional?	1	¿Sigue un modelo de madurez específico que supervise y mejore el plan de cibercontingencia?	0
	5	-		-		¿Tiene instalaciones adecuadas para la gestión de crisis y salas de situación?	1	-		¿Dispone de recursos especializados tanto en la anticipación de amenazas como en la ciberseguridad para hacer frente a futuras crisis o a los retos del futuro?	0

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
	6	-		-		¿Se compromete usted con los interesados internacionales de la UE si es necesario?	0	-		-	
	7	-		-		¿Participa usted con los interesados internacionales de países no pertenecientes a la UE si es necesario?	0	-		-	
2 – Establecer medidas de seguridad de base	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Ha realizado un estudio para identificar los requisitos y las lagunas de conocimiento de las organizaciones públicas que se base en normas reconocidas internacionalmente? Por ejemplo, ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	¿Las medidas de seguridad se elaboran de conformidad con las normas internacionales/nacionales?	1	¿Son obligatorias las medidas de seguridad de base?	1	¿Existe un proceso que actualice con frecuencia las medidas de seguridad de base?	1	¿Dispone de un proceso para endurecer las TIC cuando los incidentes no se aborden con las medidas?	1
	2	¿Ha realizado un estudio para identificar los requisitos y las lagunas de conocimiento de las organizaciones públicas que se base en normas reconocidas internacionalmente? Por ejemplo, ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	¿Consulta al sector privado y a otros interesados al definir las medidas de seguridad de referencia?	1	¿Implementa medidas de seguridad horizontales para los sectores críticos?	1	¿Hay en marcha un mecanismo de monitorización que examine la adopción de las medidas de seguridad básicas?	1	¿Existe un mecanismo de vigilancia que examine la adopción de medidas de seguridad de referencia?	1
	3	-		-		¿Implementa medidas de seguridad específicas para los sectores críticos?	1	¿Existe una autoridad nacional que compruebe si se aplican o no las medidas de seguridad básicas?	1	¿Tiene o promueve un proceso de divulgación de la vulnerabilidad (PDV) coordinado a nivel nacional?	1

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
	4	-				¿Las medidas de seguridad de referencia están en consonancia con los planes de certificación relevantes?	1	¿Ha puesto en marcha un proceso que identifique a las organizaciones que no cumplen con las normas en un período de tiempo concreto?	1	-	
	5	-		-		¿Existe un proceso de autoevaluación de riesgos para las medidas de seguridad de referencia?	1	¿Existe un proceso de auditoría que garantice que las medidas de seguridad se aplican correctamente?	1	-	
2 – Establecer medidas de seguridad de base	6	-		-		¿Revisa usted las medidas de seguridad de base obligatorias en el proceso de contratación de los organismos gubernamentales?	0	¿Define o fomenta activamente la adopción de normas de seguridad para el desarrollo de productos críticos de TI/OT (equipos médicos, vehículos conectados y autónomos, radio profesional, equipos de industria pesada...)?	0	-	
3 – Asegurar la identidad digital y fomentar la confianza en los servicios públicos digitales	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Ha realizado estudios o análisis de las deficiencias que determinen las necesidades que garanticen los servicios públicos digitales a los ciudadanos y a las empresas?	1	¿Realiza análisis de riesgos que determinen el perfil de riesgo de los activos o de los servicios antes de trasladarlos a la nube o para emprender algún proyecto de transformación digital?	1	¿Promueve usted las metodologías de «privacidad por diseño» en todos los proyectos de e-Gobierno?	1	¿Recopila indicadores sobre incidentes de ciberseguridad relacionados con la violación de servicios digitales públicos ?	1	¿Participa usted en grupos de trabajo europeos para el mantenimiento de las normas y/o diseño de nuevos requisitos para los servicios de confianza electrónicos (firmas electrónicas, sellos electrónicos, servicios de entrega registrados electrónicamente, sellado de tiempo, autenticación de sitios web)? Por ejemplo, ETSI/CEN/CENELEC, ISO, IETF, NIST, UIT...	1

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
3 – Asegurar la identidad digital y fomentar la confianza en los servicios públicos digitales	2	-		¿Tiene una estrategia para crear o promover planes nacionales de identificación electrónica que sean seguros para los ciudadanos y las empresas?	1	¿Incluye usted a los interesados privados en el diseño y la prestación de servicios públicos digitales seguros?	1	¿Ha puesto en práctica el reconocimiento mutuo de los medios de identificación electrónica con otros Estados Miembros?	1	¿Participa activamente en exámenes de homólogos como parte de los planes de notificación electrónica a la Comisión Europea?	1
	3	-		¿Dispone de una estrategia que cree o promueva servicios electrónicos seguros y de confianza nacionales (firmas electrónicas, sellos electrónicos, servicios de entrega registrados electrónicamente, sellado de tiempos, autenticación de sitios web) para los ciudadanos y las empresas?	1	¿Implementa una base mínima de seguridad para todos los servicios digitales públicos ?	1	-		-	
	4	-		¿Tiene una estrategia para la nube gubernamental (una estrategia de informática en la nube dirigida al gobierno y a los organismos públicos como ministerios, agencias gubernamentales y administraciones públicas...) que tenga en cuenta las implicaciones en cuanto a la seguridad?	0	¿Hay algún sistema de identificación electrónica a disposición de los ciudadanos y las empresas con un nivel de garantía sustancial o elevado, tal como se define en el anexo del Reglamento eIDAS (UE) Nº 910/2014?	1	-		-	
	5	-		-		¿Dispone usted de servicios públicos digitales que requieren sistemas de identificación electrónica con un nivel de garantía sustancial o elevado, tal como se define en el anexo del Reglamento eIDAS (UE) Nº 910/2014?	1	-		-	
	6	-		-		¿Dispone de proveedores de servicios de confianza para los ciudadanos y las empresas (firmas electrónicas, sellos electrónicos, servicios de entrega registrados electrónicamente, sellos de tiempo, autenticación de sitios web)?	1	-		-	

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
	7	-		-		¿Fomenta la adopción de medidas de seguridad de referencia para todos los modelos de despliegue de nubes (por ejemplo, privado, público, híbrido. IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Grupo nº. 2: Creación de la capacidad y concienciación

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
4 – Establecer una capacidad de respuesta a incidentes	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Dispone de capacidades informales de respuesta a incidentes gestionadas dentro o entre los sectores público y privado?	1	¿Tiene al menos un CSIRT nacional oficial?	1	¿Tiene capacidad de respuesta a incidentes para los sectores mencionados en el anexo II de la Directiva NIS?	1	¿Ha definido y promovido prácticas normalizadas para los procedimientos de respuesta a incidentes y los esquemas de clasificación de incidentes?	1	¿Tiene algún mecanismo para la detección temprana, identificación, prevención, respuesta y mitigación de las vulnerabilidades del día cero?	1
	2	-		¿Tiene(n) su(s) CSIRT nacional(es) un ámbito de intervención claramente definido? Por ejemplo, dependiendo del sector al que se dirija, los tipos de incidentes, los impactos.	1	¿Existe en su país un mecanismo de cooperación del CSIRT para responder a los incidentes?	1	¿Evalúa su capacidad de respuesta a los incidentes para asegurarse de que dispone de los recursos y aptitudes adecuados para llevar a cabo las tareas establecidas en el punto (2) del Anexo I de la Directiva NIS?	1	-	
	3	-		¿Tiene(n) su(s) CSIRT nacional(es) relaciones definidas claramente con otros interesados nacionales en relación con el panorama de la ciberseguridad nacional y las prácticas de respuesta a los incidentes (por ejemplo, AAL, militares, PSN, ENSC)?	0	¿Tiene(n) su(s) CSIRT nacional(es) una capacidad de respuesta a incidentes de acuerdo con el Anexo I de la Directiva NIS? es decir, disponibilidad, seguridad física, continuidad de las actividades, cooperación internacional, vigilancia de incidentes, capacidad de alerta temprana y alertas, respuesta a incidentes, análisis de riesgos y conocimiento de la situación, cooperación con el sector privado, prácticas estándar...	1	-		-	
	4	-				¿Existe un mecanismo de cooperación con otros países vecinos en relación con los incidentes?	1	-		-	

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
4 – Establecer una capacidad de respuesta a incidentes	5	-		-		¿Ha definido formalmente políticas y procedimientos claros para el manejo de incidentes?	1	-		-	
	6	-		-		¿Participan sus CSIRT nacionales en ejercicios de ciberseguridad tanto a nivel nacional como internacional?	1	-		-	
	7	-		-		¿Su(s) CSIRT nacional(es) está(n) afiliado(s) al FIRST (Foro de Respuesta a Incidentes y Equipos de Seguridad)?	0	-		-	
5 – Aumentar la concienciación de los usuarios	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Existe un reconocimiento mínimo por parte del gobierno, el sector privado o los usuarios en general, de que es necesario aumentar la conciencia sobre las cuestiones de ciberseguridad y privacidad?	1	¿Ha identificado un público objetivo específico para sensibilizar a los usuarios? Por ejemplo, usuarios generales, jóvenes, usuarios comerciales (que aún se pueden desglosar más: PYMES, OSE, PSD, etc.)	1	¿Ha desarrollado planes de comunicación/estrategias para las campañas?	1	¿Dispone de mediciones que evalúen su campaña durante la etapa de planificación?	1	¿Ha puesto en marcha mecanismos que garanticen que las campañas de concienciación sigan siendo relevantes en lo que respecta a los avances tecnológicos, los cambios en el panorama de las amenazas, las reglamentaciones jurídicas y las directivas de seguridad nacional?	1
	2	¿Los organismos públicos están llevando a cabo campañas de concienciación sobre ciber seguridad dentro de su organización de forma ad hoc? por ejemplo, tras un incidente de ciberseguridad.	0	¿Diseña un plan de proyecto que conciencie sobre cuestiones de seguridad de la información y la privacidad?	1	¿Tiene un proceso para crear contenido a nivel gubernamental?	1	¿Evalúa sus campañas después de la ejecución?	1	¿Realiza evaluaciones o estudios periódicos que midan los cambios de actitud o de comportamiento en ciberseguridad y privacidad en los sectores público y privado?	1

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
5 – Aumentar la concienciación de los usuarios	3	¿Los organismos públicos están realizando campañas de sensibilización sobre ciberseguridad dirigidas al público en general de manera ad hoc? Por ejemplo, tras un incidente de ciberseguridad.	0	¿Tiene recursos disponibles y fácilmente identificables (por ejemplo, un único portal en línea, herramientas para la concienciación) para los usuarios que deseen informarse sobre cuestiones de ciberseguridad y privacidad?	1	¿Dispone de algún mecanismo para identificar las áreas objetivo de concienciación (por ejemplo, el paisaje de amenazas de la ENISA, los paisajes nacionales, los paisajes internacionales, la información de los centros nacionales de ciberdelitos, etc.)?	1	¿Dispone de algún mecanismo que identifique los medios o canales de comunicación más relevantes en función del público al que se dirigen para aumentar la difusión y el compromiso? Por ejemplo, diferentes tipos de medios digitales, folletos, correos electrónicos, material didáctico, carteles en zonas concurridas, televisión, radio...	1	¿Consulta a los expertos en comportamientos para que adapten su campaña al público objetivo?	1
	4	-		-		¿Reúne a los interesados con expertos y equipos de comunicación para crear contenidos?	1			-	
	5	-		-		¿Involucra y adquiere compromisos con el sector privado en sus esfuerzos de concienciación que promuevan y difundan los mensajes a un público más amplio?	1	-		-	
	6	-		-		¿Prepara usted iniciativas de concienciación específicas para los ejecutivos de los sectores público, privado, académico o de la sociedad civil?	1	-		-	
	7	-		-		¿Participa en las campañas del Mes de la Ciberseguridad Europea de la ENISA (MCSE)?	0	-		-	
6 – Organizar ejercicios de ciberseguridad	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
6 – Organizar ejercicios de ciberseguridad	1	¿Realiza ejercicios de crisis en otros sectores (distintos a la ciberseguridad) a nivel nacional o paneuropeo?	1	¿Dispone de un programa de ejercicios de ciberseguridad a nivel nacional?	1	¿Involucra a todas las autoridades relacionadas de la administración pública? (incluso en el supuesto de un sector específico)	1	¿Redacta informes de acción/de evaluación?	1	¿Dispone de una capacidad de análisis del aprendizaje obtenido en materia cibernética (procesos de información, análisis, mitigación)?	1
	2	¿Dispone de una asignación de recursos para el diseño y la planificación de ejercicios de gestión de crisis?	1	¿Realiza o da prioridad a los ejercicios de gestión de cibercrisis en funciones vitales de la sociedad e infraestructuras críticas?	1	¿Involucra al sector privado en la planificación y ejecución de los ejercicios?	1	¿Prueba los planes a nivel nacional y los procedimientos?	1	¿Dispone de un proceso establecido del aprendizaje obtenido?	1
	3	-		¿Ha reconocido un organismo de coordinación que supervise el diseño y la planificación de los ejercicios de ciberseguridad (organismo público, consultoría...)?	0	¿Organiza ejercicios específicos del sector a nivel nacional y/o internacional?	1	¿Participa en ejercicios de ciberseguridad a nivel paneuropeo?	1	¿Adapta los supuestos de los ejercicios en función de los últimos acontecimientos (avances tecnológicos, conflictos mundiales, panorama de amenazas...)?	1
	4	-		-		¿Organiza ejercicios en todos los sectores críticos que se indican en el anexo II de la Directiva SRI?	1	-		¿Unifica sus procedimientos de gestión de crisis con los de otros Estados Miembros para que se garantice una gestión eficaz de crisis paneuropea ?	1
	5	-		-		¿Organiza ejercicios de ciberseguridad intersectoriales y/o transectoriales?	1	-		¿Dispone de un mecanismo que adapte rápidamente la estrategia, los planes y los procedimientos a partir de los aprendizajes obtenidos durante los ejercicios?	0
	6	-		-		¿Organiza ejercicios de ciberseguridad específicos para varios niveles? (nivel técnico y operativo, nivel de procedimiento, nivel de decisión, nivel político...)	0	-		-	
7 – Reforzar los programas educacionales y de formación	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
	1	¿Considera usted la posibilidad de desarrollar programas educacionales y de formación en ciberseguridad?	1	¿Programa cursos dedicados a la ciberseguridad?	1	¿Abarca su país la cultura de la ciberseguridad en la etapa de educación infantil del currículo educativo de los estudiantes? Por ejemplo, ¿propicia la ciberseguridad en la escuela primaria y secundaria?	1	¿Insta a que el personal de los sectores público y privado tenga acreditación o titulación?	1	¿Dispone de mecanismos que garanticen que la formación y los programas educativos estén al día en lo que respecta a los avances tecnológicos actuales y emergentes, los cambios en el supuesto de las amenazas, las normativas legales y las directrices de seguridad nacional?	1
	2	-		¿Ofrecen las universidades de su país doctorados en ciberseguridad como una disciplina independiente y no como una asignatura perteneciente al grado en informática?	1	¿Dispone de laboratorios nacionales de investigación e instituciones educativas especializadas en ciberseguridad?	1	¿Su país ha desarrollado programas de formación o de mentores en ciberseguridad que apoyen a las empresas nacionales de reciente creación y a las PYMES?	1	¿Crea centros académicos de excelencia en ciberseguridad para que actúen como centros de investigación y educación?	1
	3	-		¿Considera formar a los educadores, independientemente de su campo, en temas de seguridad y privacidad de la información? Por ejemplo, seguridad en línea, protección de datos personales, ciberacoso.	1	¿Alienta/funda cursos de ciberseguridad y planes de formación para empleados de agencias de empleo de los Estados Miembros?	1	¿Promueve activamente la incorporación de cursos de seguridad de la información en la enseñanza superior no solo para los estudiantes de informática sino también para cualquier otra especialidad profesional? Por ejemplo, cursos adaptados a las necesidades de esa profesión.	1	¿Participan las instituciones académicas en los principales debates en el área de la educación e investigación en ciberseguridad a nivel internacional?	0
	4	-		-		¿Dispone de cursos de ciberseguridad y/o de un currículum especializado para los niveles 5 a 8 del MEC (Marco Europeo de Calificaciones)?	1	¿Evalúa periódicamente las lagunas de formación (escasez de trabajadores de ciberseguridad) en el área de la seguridad de la información?	1	-	
	5	-		-		¿Alienta y/o apoya iniciativas que incluyan cursos de seguridad en Internet en la educación primaria y secundaria?	1	¿Fomenta usted la creación de redes y el intercambio de información entre instituciones académicas, tanto a nivel nacional como internacional?	1		

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
7 - Reforzar los programas educacionales y de formación	6	-		-		¿Financia u ofrece gratuitamente cursos básicos de ciberseguridad a los ciudadanos?	0	¿Involucra al sector privado de alguna forma en las iniciativas de educación en materia de ciberseguridad? Por ejemplo, diseño e impartición de cursos, pasantías, prácticas laborales...	1	-	
	7	-		-		¿Organiza eventos anuales sobre seguridad de la información (por ejemplo, concursos de hacking o hackathons)?	0	¿Implementa mecanismos de financiación para fomentar la formación universitaria en ciberseguridad? Por ejemplo, becas, prácticas o aprendizajes garantizados, trabajos garantizados en industrias específicas o funciones en el sector público.	0	-	
8 – Fomentar la I+D	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Ha realizado estudios o análisis que identifiquen las prioridades de I+D en ciberseguridad?	1	¿Dispone de un proceso que defina las prioridades de I+D (por ejemplo, los temas emergentes que disuadan, protejan, detecten y se adapten a los nuevos tipos de ciberataques)?	1	¿Existe un plan para vincular las iniciativas de I+D con la economía real?	1	¿Están las iniciativas de I+D en materia de ciberseguridad en consonancia con los objetivos estratégicos relevantes como por ejemplo, DSM, H2020, Europa digital, estrategia de ciberseguridad de la UE?	1	¿Sigue la cooperación, a nivel nacional, con alguna iniciativa internacional de I+D relacionada con la ciberseguridad?	1
	2	-		¿Participa el sector privado en el establecimiento de las prioridades de I+D?	1	¿Existen proyectos nacionales relacionados con la ciberseguridad?	1	¿Existe un plan de evaluación de las iniciativas de I+D?	1	¿Están las prioridades de I+D en consonancia con las normativas actuales o futuras (a nivel nacional)?	1

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
8 – Fomentar la I+D	3	-		¿Participa el sector privado en el establecimiento de las prioridades de I+D?	1	¿Cuenta con ecosistemas locales/regionales de puesta en marcha y otros canales de creación de redes (por ejemplo, parques tecnológicos, grupos de innovación, eventos/plataformas de creación de redes) que fomenten la innovación (incluso para las empresas emergentes de ciberseguridad)?	1	¿Existen acuerdos de cooperación con universidades y otros centros de investigación?	1	¿Participa usted en los principales debates acerca de uno o varios temas punteros de I+ D a nivel internacional?	0
	4	-		¿Existen iniciativas nacionales de I+ D relacionadas con la ciberseguridad?	0	¿Hay inversión en programas de I+D de ciberseguridad en el mundo académico y en el sector privado?	1	¿Existe un órgano institucional reconocido que supervise las actividades de I+ D en ciberseguridad?	0	-	
	5	-		-		¿Dispone de cátedras de investigación industrial en las universidades que unan los temas de investigación con las necesidades del mercado?	1	-		-	
	6	-		-		¿Dispone de programas de financiación de I+D dedicados a la ciberseguridad?	0	-		-	
9– Incentivar que el sector privado invierta en medidas de seguridad	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Existe una política industrial o una voluntad política que fomenten el desarrollo de la industria de la ciberseguridad?	1	¿Participa el sector privado en el diseño de los incentivos?	1	¿Existen incentivos económicos/regulatorios o de otro tipo para promover las inversiones en ciberseguridad?	1	¿Hay algún agente privado que reaccione a los incentivos invirtiendo en medidas de seguridad? Por ejemplo, inversores especializados en ciberseguridad e inversores no especializados	1	¿Centra los incentivos en temas de ciberseguridad en función de los últimos avances en materia de amenazas?	1

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
9– Incentivar que el sector privado invierta en medidas de seguridad	2	-		¿Ha identificado temas específicos de ciberseguridad que haya que desarrollar? Por ejemplo, criptografía, privacidad, nueva forma de autenticación, IA para la ciberseguridad...	0	¿Proprociona un respaldo a las empresas emergentes de ciberseguridad y a las PYMES (por ejemplo, incentivos fiscales)?	1	¿Proporciona incentivos para que el sector privado se centre en la seguridad de las tecnologías de vanguardia? Por ejemplo, 5G, inteligencia artificial, IoT, informática cuántica...	1	-	
	3	-		-		¿Proporciona incentivos fiscales u otro incentivo financiero a los inversores del sector privado en las empresas de ciberseguridad?	1	-		-	
	4	-		-		¿Facilita el acceso de las empresas de ciberseguridad y las PYMES al proceso de contratación pública?	0	-		-	
	5	-		-		¿Dispone de un presupuesto para ofrecer incentivos al sector privado?	0	-		-	
10 – Mejorar la ciberseguridad de la cadena de suministros	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Ha realizado un estudio sobre las buenas prácticas de seguridad para la gestión de la cadena de suministros que se usa en las contrataciones en diversos segmentos industriales y/o del sector público?	1	¿Cuenta con un proceso para identificar los eslabones débiles de la ciberseguridad en la cadena de suministro de los sectores críticos (tal como se identifica en el anexo II de la Directiva NIS (2016/1148))?	1	¿Usa un plan de certificación de seguridad (nacional o internacional) para los servicios y productos con bases TIC? por ejemplo, el GAF-SI ARM (Grupo de Altos Funcionarios para la Seguridad de los Sistemas de Información), el Acuerdo de Reconocimiento Mutuo en Europa, el ARCC (Acuerdo de Reconocimiento de Criterios Comunes), las iniciativas nacionales, las iniciativas del sector, ...	1	¿Cuenta con un proceso que actualice las evaluaciones de ciberseguridad de la cadena de suministro de los servicios y productos de las TIC en sectores críticos (como se señala en el Anexo II de la Directiva NIS (2016/1148))?	1	¿Dispone de sondas de detección en elementos claves de la cadena de suministro que detecten indicios de compromiso? Por ejemplo, controles de seguridad a nivel de proveedores de servicios de internet, sondas de seguridad en los principales componentes de la infraestructura...	1

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
10 – Mejorar la ciberseguridad de la cadena de suministros	2	-		¿Aplica usted normas en las políticas de contratación de las administraciones públicas que garanticen que los proveedores de productos o servicios de TIC cumplan los requisitos básicos de seguridad de la información? Por ejemplo, ISO/CEI 27001 y 27002, ISO/CEI 27036...	1	¿Promueve activamente la seguridad y la privacidad al diseñar buenas prácticas en el desarrollo de los productos y servicios TIC? por ejemplo, asegurar la vida útil en el desarrollo del software, vida útil de IoT.	1	¿Cuenta con un proceso que identifique los eslabones débiles de la ciberseguridad en la cadena de suministro de los sectores críticos (tal como se identifica en el Anexo II de la Directiva NIS (2016/1148))?	1	-	
	3	-		-		¿Desarrolla y proporciona un catálogo centralizado con información amplia sobre las normas de seguridad y privacidad de la información actuales que sea trasladable y aplicable a PYMES?	1	¿Dispone de mecanismos que aseguren que los productos y servicios TIC que son críticos para los OSE sean ciberresilientes (por ejemplo: tengan la capacidad de mantener la disponibilidad y la seguridad contra un ciberincidente)? Por ejemplo, a través de pruebas, evaluaciones frecuentes, detección de elementos comprometidos...	1	-	
	4	-				¿Participa activamente en el diseño de un marco de certificación de la UE para los productos, servicios y procesos digitales de las TIC, tal como se establece en la Ley de Ciberseguridad de la UE (Reglamento (UE) 2019/881)?; por ejemplo, la participación en el Grupo Europeo de Certificación de la Ciberseguridad (GECC), que promueva normas y procedimientos técnicos para la seguridad de los productos/servicios de las TIC	0	¿Promueve usted el desarrollo de planes de certificación dirigidos a las PYME para impulsar la adopción de normas de seguridad de la información y la privacidad?	0	-	
	5	-		-		¿Ofrece algún tipo de incentivos a las PYMES para que adopten normas de seguridad y privacidad?	0	¿Dispone de medidas que animen a las grandes empresas a aumentar la ciberseguridad de las pequeñas empresas en sus cadenas de suministro? Por ejemplo, un centro de ciberseguridad, campañas de formación y concienciación...	0	-	

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
	6	-		-		¿Anima a los proveedores de software a que respalden a las PYMES al garantizar configuraciones predeterminadas seguras en los productos para entidades pequeñas?	0	-		-	

4.1.3 Grupo nº. 3: Jurídico y normativo

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
11 – Proteger la infraestructura de la información crítica, los OSE y los LPD	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Se entiende de manera general que los operarios de IIC contribuyen a la seguridad nacional?	1	¿Dispone de metodología que identifique los servicios esenciales?	1	¿Ha implementado la Directiva NIS (2016/1148)?	1	¿Dispone de un procedimiento de actualización del registro de riesgos?	1	¿Elabora y actualiza informes de entorno de amenazas?	1
	2	-		¿ Dispone de metodología que identifique las ICC?	1	¿Ha aplicado la Directiva CE (2008/114) relativa a la identificación y designación de infraestructuras críticas europeas y a la evaluación de la necesidad de mejorar su protección?	1	¿Dispone de otros mecanismos que cuantifiquen que las medidas técnicas y organizativas aplicadas por los OSE son adecuadas para que se gestionen los riesgos que se plantean en cuanto a la seguridad de las redes y los sistemas de información?; por ejemplo, auditorías periódicas de ciberseguridad, marco nacional para la implementación de medidas estándar, herramientas técnicas que proporcione el Gobierno como sondas de detección o revisión de la configuración específica del sistema...	1	En función de los últimos avances en el entorno de las amenazas, ¿podrá embarcarse en un nuevo sector de su plan de acción PIIC?	1
	3	-		¿Dispone de metodología que identifique a los OSE?	1	¿Dispone de un registro nacional de identificación de OSE por sector crítico?	1	¿ Revisa y por lo tanto actualiza la lista de OSE identificados al menos cada dos años?	1	En función de los últimos avances en el entorno de las amenazas, ¿podrá adaptar los nuevos requisitos en su plan de acción PIIC?	1

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
11 – Proteger la infraestructura de la información crítica, los OSE y los LPD	4	-		¿Dispone de una metodología que identifique a los proveedores de servicios digitales?	1	¿Dispone de un registro nacional de proveedores de servicios digitales que estén identificados?	1	¿Dispone de otros mecanismos que cuantifiquen que las medidas técnicas y organizativas que aplican los proveedores de servicios digitales son adecuadas para gestionar los riesgos que plantea la seguridad de las redes y los sistemas de información? Por ejemplo, auditorías periódicas de ciberseguridad, marco nacional para la aplicación de medidas estándar, herramientas técnicas que proporciona el gobierno como sondas de detección o revisión de la configuración específica del sistema...	1	-	
	5	-		¿Dispone de una o más autoridades nacionales que se encargan de la supervisión de la protección de la infraestructura de información crítica y de la seguridad de la red y los sistemas de información? Por ejemplo, según lo dispuesto en la Directiva NIS (2016/1148)	1	¿Tiene un registro nacional de riesgos para los riesgos identificados o conocidos?	1	¿ Revisa y por lo tanto actualiza la lista de proveedores de servicios digitales identificados al menos cada dos años?	1	-	
	6	-		¿Desarrolla planes de protección específicos para cada sector? Por ejemplo, incluyendo medidas de ciberseguridad de base (obligatorias o directrices)	0	¿Dispone de una metodología para mapear las dependencias de IIC?	1	¿Usa un plan de certificación de seguridad (nacional o internacional) que ayude a la OSE y a los proveedores de servicios digitales a identificar productos de TIC seguros? por ejemplo, el SOG-IS MRA , las iniciativas nacionales...	1	-	
	7	-		-		¿Utiliza prácticas de gestión de riesgos que identifiquen, cuantifiquen y gestionen los riesgos relacionados con las IIC a nivel nacional?	1	¿Utiliza un esquema de certificación de seguridad o un procedimiento de calificación que evalúe a los proveedores de servicios que trabajan con los OSE? Por ejemplo, proveedores de servicios en el campo de la detección de incidentes, respuesta a incidentes, auditoría de ciberseguridad, servicios en la nube, tarjetas inteligentes...	1	-	

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
11 – Proteger la infraestructura de la información crítica, los OSE y los LPD	8	-		-		¿Se compromete con un proceso de consulta que identifique las dependencias transfronterizas?	1	¿Dispone de mecanismos que midan el nivel de cumplimiento de los proveedores de servicios digitales y de los OSE con respecto a las medidas básicas de ciberseguridad?	0	-	
	9					¿Tiene un único punto de contacto encargado de coordinar las cuestiones relacionadas con la seguridad de las redes y los sistemas de información a nivel nacional y la cooperación transfronteriza a nivel de la Unión?	1	¿Tiene alguna disposición que asegure la continuidad de los servicios proporcionados por las infraestructuras de información críticas? Por ejemplo, anticipación de crisis, procedimientos para reconstruir los sistemas de información críticos, continuidad del negocio sin TI, procedimientos de sistema de recuperación de interfaces por aire...	0		
	10					¿Define usted medidas básicas de ciberseguridad (obligatorias o directrices) para los proveedores de servicios digitales y todos los sectores identificados en el Anexo II de la Directiva NIS (2016/1148)?	1				
	11	-		-		¿Proporciona herramientas o metodologías que detecten ciberincidentes?	1	-		-	
12 – Abordar la ciberdelincuencia	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
12 – Abordar la ciberdelincuencia	1	¿Ha realizado un estudio que determine los requisitos de las fuerzas del orden (base jurídica, recursos, aptitudes...) para hacer frente con eficacia a la ciberdelincuencia?	1	¿Su marco jurídico nacional cumple en su totalidad con el marco jurídico pertinente de la UE, incluida la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información? Por ejemplo, el acceso ilegal a los sistemas de información, la interferencia ilegal en los sistemas, la interferencia ilegal de datos, la interceptación ilegal, los instrumentos utilizados para cometer delitos...	1	¿Dispone de unidades en las oficinas de la fiscalía que se dediquen a gestionar la ciberdelincuencia ?	1	¿Recoge estadísticas de acuerdo con las disposiciones del artículo 14 (1) de la Directiva 2013/40/UE (directiva relativa a los ataques contra los sistemas de información)?	1	¿Dispone de formación interinstitucional o de talleres de formación para las AAL, los jueces, los fiscales y los CSIRT nacionales/gubernamentales a nivel nacional y/o multilateral?	1
	2	¿Ha realizado un estudio que identifique los requisitos de los fiscales y jueces (base legal, recursos, habilidades...) para abordar eficazmente la ciberdelincuencia?	1	¿Dispone de alguna medida legal sobre la sustracción en línea de identidad y la sustracción de datos personales?	1	¿Dispone de un presupuesto dedicado a las unidades de ciberdelincuencia?	1	¿Recoge estadísticas por separado sobre el ciberdelito? Por ejemplo, estadísticas operativas, estadísticas sobre tendencias en ciberdelincuencia, estadísticas sobre los procesos de la ciberdelincuencia y los perjuicios...	1	¿Participa en acciones coordinadas a nivel internacional con la finalidad de desestabilizar las actividades delictivas? Por ejemplo, infiltración en foros de *hacking* criminal, grupos organizados de ciberdelincuencia, mercados en redes oscuras y retirada de redes de *bots*...	1
	3	¿Su país ha firmado el Convenio de Budapest del Consejo de Europa sobre la Ciberdelincuencia?	1	¿Dispone de alguna medida legal que se ocupe de las infracciones de la propiedad intelectual y de los derechos de autor en línea?	1	¿Ha establecido un órgano/entidad central que coordine las actividades en el área de la lucha contra la ciberdelincuencia?	1	¿Evalúa la idoneidad de la formación que se imparte al personal de las AAL, del poder judicial y de los CSIRT nacionales para que se haga frente a la ciberdelincuencia?	1	¿Existe una clara segregación de funciones entre los CSIRT, las AAL y el poder judicial (fiscales y jueces) cuando cooperan para hacer frente a la ciberdelincuencia?	1
	4			¿Dispone de alguna medida legal que se ocupe del acoso en línea o el ciberacoso?	1	¿Ha establecido mecanismos de cooperación entre las instituciones nacionales pertinentes que participan en la lucha contra la ciberdelincuencia incluidos los CSIRT nacionales encargados del cumplimiento de la ley?	1	¿Realiza evaluaciones periódicas para asegurarse de que dispone de recursos suficientes (humanos, presupuesto y herramientas) dedicados a las unidades de ciberdelincuencia dentro de las AAL?	1	¿Su marco reglamentario facilita la cooperación entre los CSIRT/AL y el Poder Judicial (fiscales y jueces)?	1
	5			¿Dispone de alguna medida legal sobre el fraude informático? Por ejemplo, que cumplan las medidas del Convenio de Budapest del Consejo de Europa sobre la Ciberdelincuencia	1	¿Colabora y comparte información con otros Estados Miembros en el área de la lucha contra la ciberdelincuencia?	1	¿Realiza evaluaciones periódicas para asegurarse de que dispone de recursos suficientes (humanos, presupuesto y herramientas) dedicados a las unidades de ciberdelincuencia dentro de las unidades de vigilancia de la ley?	1	¿ Participa en la elaboración y el mantenimiento de herramientas estandarizadas y metodologías, formularios y procedimientos que se compartan con los interesados de la UE (AAL, CSIRT, ENISA, Europol EC3, ...)?	1

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
12 – Abordar la ciberdelincuencia	6	-		¿Dispone de alguna medida legal que aborde la protección infantil en línea? Por ejemplo: el cumplimiento con las medidas de la Directiva 2011/93/UE y el Convenio de Budapest del Consejo de Europa sobre la Ciberdelincuencia...	1	¿ Colabora y comparte información con las agencias de la UE (por ejemplo, Europol EC3, Eurojust, la ENISA) en la lucha contra la ciberdelincuencia?	1	¿Dispone de juzgados de instrucción o juzgados especializados que encausen ciberdelitos?	1	¿Dispone de mecanismos avanzados para evitar que particulares se vean atraídos/ involucrados en ciberdelincuencia?	0
	7	-		¿Ha identificado un punto de contacto operativo nacional para el intercambio de información que responda a las solicitudes de información urgentes de otros Estados Miembros en relación con los delitos establecidos en la Directiva 2013/40/UE (Directiva relativa a los ataques contra los sistemas de información)?	1	¿Tiene las herramientas apropiadas que hagan frente a la ciberdelincuencia? Por ejemplo, taxonomía y clasificación de la ciberdelincuencia, herramientas para recopilar pruebas electrónicas, herramientas forenses informáticas, plataformas de intercambio de confianza...	1	¿Dispone de algún mecanismo dedicado a prestar apoyo y asistencia a las víctimas de ciberdelitos (usuarios en general, PYMES, grandes empresas)?	1	¿Su país usa el EU *Blueprint* y/o el Protocolo de Respuesta de Emergencia de las Fuerzas de Seguridad (PRE FS UE) para dar una respuesta eficaz a los ciberincidentes a gran escala?	0
	8			¿Su organismo de vigilancia de la ley incluye una unidad dedicada a los ciberdelitos?	1	¿ Dispone de procedimientos operativos estandarizados para manejar las e-pruebas?	1	¿Ha establecido un marco interinstitucional y mecanismos de cooperación entre todos los interesados relevantes(por ejemplo, la Dirección de Asuntos Jurídicos, el CSIRT nacional, las sedes judiciales), incluido el sector privado (por ejemplo, los operadores de servicios esenciales, los proveedores de servicios) cuando proceda para responder a los ciberataques?	1	-	
	9			¿Ha designado, de acuerdo al artículo 35 de la Convención de Budapest, un contacto permanente las 24h del día?	1	¿ Su país participa en ofertas formativas respaldadas/ofertadas por las agencias de la EU (por ejemplo, Europol, Eurojust, OLAF, Cepol, la ENISA)?	0	¿Su marco reglamentario facilita la cooperación entre los CSIRTy AL?	1	-	
	10	-		¿Ha designado un contacto nacional que esté operativo las 24h del día para el protocolo de respuesta a las emergencias de la ley de refuerzo de la EU (EU LE ERP) que responda a los principales ciberataques?	1	¿Su país está considerando la posibilidad de adoptar el segundo protocolo adicional del Convenio de Budapest del Consejo de Europa sobre Ciberdelincuencia?	0	¿Dispone de mecanismos (por ejemplo, herramientas, procedimientos) que faciliten el intercambio de información y la cooperación entre el CSIRT/AL y posiblemente el poder judicial (fiscales y jueces) en el área de la lucha contra la ciberdelincuencia?	1	-	

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
	11			¿Proporciona con frecuencia formación especializada a los interesados que participan en la lucha contra los ciberdelitos (organismos de cumplimiento de la ley, poder judicial, CSIRT)? Por ejemplo, sesiones de formación sobre la presentación y el enjuiciamiento de ciberdelitos , formación sobre la recopilación de pruebas electrónicas y la garantía de la integridad a lo largo de la cadena de custodia digital e informática forense, entre otras.	1						
	12			¿Su país ha ratificado o se ha adherido a la Convención de Budapest del Consejo de Europa sobre la Ciberdelincuencia?	1			-	-	-	
	13	-		¿Ha firmado y ratificado su país el Protocolo Adicional (tipificación como delito de los actos de carácter racista y xenófobo cometidos mediante sistemas informáticos) del Convenio de Budapest del Consejo de Europa sobre la Ciberdelincuencia?	0	-	-	-		-	
13 – Establecer mecanismos de notificación de incidentes	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Dispone de mecanismos informales de intercambio de información sobre incidentes de ciberseguridad entre organizaciones privadas y autoridades nacionales?	1	¿Tiene un sistema de notificación de incidentes para todos los sectores en virtud del anexo II de la Directiva NIS?	1	¿Tiene un sistema de notificación obligatoria de incidentes que esté funcionando en la práctica?	1	¿Tiene un procedimiento armonizado para los planes de notificación de incidentes sectoriales?	1	¿Crea usted un informe anual de incidentes?	1

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
13 – Establecer mecanismos de notificación de incidentes	2	-		¿Ha aplicado los requisitos de notificación para los proveedores de servicios de telecomunicaciones en cumplimiento del artículo 40 de la Directiva (UE 2018/1972)? La Directiva exige que los Estados Miembros velen por que los proveedores de redes públicas o de servicios de comunicaciones electrónicas que estén disponibles al público notifiquen a la autoridad competente, sin demora injustificada, un incidente de seguridad que haya tenido repercusiones importantes en la explotación de las redes o servicios.	1	¿Existe un mecanismo de coordinación/cooperación para las obligaciones de notificación de incidentes en relación con la RNBP, la NISD, el artículo 40 (ex art. 13a) y el eIDAS?	1	¿Tiene un sistema de notificación de incidentes para otros sectores distintos a los de la Directiva NIS?	1	¿Existen informes sobre el panorama de la ciberseguridad u otros tipos de análisis preparados por la entidad que recibe los informes de incidentes?	1
	3	-		¿Ha aplicado los requisitos de notificación para los proveedores de servicios de confianza en cumplimiento del artículo 19 del Reglamento eIDAS (Reglamento (UE) N.º 910/2014)? El artículo (19) exige, entre otros requisitos, que los proveedores de servicios de confianza notifiquen al órgano supervisor los incidentes/incumplimientos significativos.	1	¿Dispone de los instrumentos adecuados que garanticen la confidencialidad e integridad de la información que se comparte a través de los diversos canales de información?	1	¿Mide usted la eficacia de los procedimientos de notificación de incidentes? Por ejemplo, indicadores sobre los incidentes que se han notificado a través de los canales adecuados, el momento de la notificación del incidente...	1	-	
	4	-		¿Ha aplicado los requisitos de notificación para los proveedores de servicios digitales de conformidad con el artículo 16 de la Directiva NIS? El artículo (16) exige que los proveedores de servicios digitales notifiquen a la autoridad competente o al CSIRT nacional, sin demora injustificada, cualquier incidente que tenga un impacto sustancial en la prestación de un servicio que ofrezcan dentro de la Unión., como se menciona en el Anexo III.	1	¿Tiene una plataforma/herramienta para facilitar el proceso de presentación de informes?	0	¿Tiene una taxonomía común a nivel nacional para la clasificación de incidentes y causas principales?	0	-	

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
14 – Reforzar la privacidad y la protección de datos	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Ha realizado estudios o análisis que identifiquen las áreas de mejora que mejor protejan los derechos de la privacidad de los ciudadanos?	1	¿Se involucra la autoridad nacional de protección de datos en las áreas relacionadas con la ciberseguridad (por ejemplo, la redacción de nuevas leyes y reglamentos de ciberseguridad, la definición de medidas mínimas de seguridad)?	1	¿Promueve usted a propósito buenas prácticas en medidas de seguridad y protección de datos para el sector público y/o privado?	1	¿Realiza evaluaciones periódicas para asegurarse de que dispone de recursos suficientes (humanos, presupuesto e instrumentos) dedicados a la autoridad de protección de datos?	1	¿Dispone de algún mecanismo de supervisión de los últimos avances tecnológicos para que adapte las directrices y las disposiciones/obligaciones jurídicas relevantes?	1
	2	¿Ha elaborado una base jurídica a nivel nacional para hacer cumplir el Reglamento General de Protección de Datos (Reglamento UE Nº 2016/679)? Por ejemplo, mantener o introducir disposiciones o limitaciones más específicas en las normas del Reglamento.	0	-		¿Lanza programas de concienciación y de formación sobre este tema?	1	¿Anima a las organizaciones y empresas para que obtengan el certificado de cumplimiento de la norma ISO/IEC 27701:2019 del Sistema de Gestión de Información de Privacidad (SGIP)?	1	¿Promueve o participa activamente en iniciativas de I+D sobre tecnologías de mejora de la privacidad (TMP)?	0
	3	-		-		¿Coordina los procedimientos de reporte de incidentes con la LPD?	1	-		-	
	4	-		-		¿Promueve y respalda el desarrollo de normas técnicas sobre seguridad de la información y privacidad? ¿Están creadas a medida de las pequeñas y medianas empresas (PYMES)?	0	-		-	

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
	5	-		-		¿Proporciona directrices prácticas y ampliables que respalden a los diversos de controladores de datos en el cumplimiento de los requisitos y de obligaciones legales de privacidad y protección de datos?	0	-		-	

4.1.4 Grupo nº. 4: Cooperación

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
15 – Establecer una asociación público-privada (APP)	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						
	1	¿Se entiende en general que las asociaciones público-privadas contribuyen a elevar el nivel de ciberseguridad en el país a través de diferentes medios? Por ejemplo, compartiendo intereses en el crecimiento de la industria de la ciberseguridad, cooperando en la creación de un marco normativo relevante en de ciberseguridad, fomentando la I+D...	1	¿Tiene un plan de acción nacional para establecer las APP?	1	¿Ha establecido asociaciones nacionales entre el sector público y el privado?	1	¿Ha establecido asociaciones público-privadas intersectoriales?	1	En función de los últimos avances tecnológicos y normativos, ¿podrá adaptar o crear las APP?	1
	2	-		¿Establece una base legal o contractual (leyes específicas, acuerdos de confidencialidad, propiedad intelectual) en el ámbito de actuación de las APP?	1	¿Ha establecido asociaciones público-privadas específicas para cada sector?	1	En las APP constituidas, ¿se centra también en la cooperación entre organismos público-público y entidades privadas-privadas?	1		
	3	-		-		¿ Proporciona financiación para que se constituyan las APP?	1	¿Promociona las APP entre las pequeñas y medianas empresas (PYMES)?	1	-	

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
15 – Establecer una asociación público-privada (APP)	4	-		-		¿Las instituciones públicas lideran las APP en general? (es decir, hay un único punto de contacto del sector público que gestiona y coordina la APP. Los organismos públicos acuerdan de antemano lo que quieren lograr, hay directrices claras de las administraciones públicas sobre sus necesidades y limitaciones al sector privado...)	1	¿Mide usted los resultados de las APP?	1	-	
	5	-		-		¿ Es usted miembro de la Organización Europea de Ciberseguridad (ECSO) , asociación contractual público - privada?	0	-		-	
	6	-		-		¿ Tiene una o varias APP que trabajan en actividades CSIRT?	0	-		-	
	7					¿Tiene una o varias APP que trabajan en temas de infraestructuras de protección de información crítica?	0				
	8	-		-		¿Tiene una o varias APPs que trabajan en aumentar la concienciación en ciberseguridad y desarrollo de aptitudes?	0	-		-	
16 – Institucionalizar la cooperación entre los organismos públicos	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participen en la consecución del objetivo de forma no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
	1	¿Tiene canales de cooperación informales entre organismos públicos?	1	¿Tiene un plan de cooperación nacional centrado en la ciberseguridad? Por ejemplo, juntas consultivas, grupos directivos, foros, consejos, cibercentros o grupos de reunión para expertos.	1	¿Participan las autoridades públicas en el plan de cooperación?	1	¿Garantiza que existan canales de cooperación dedicados a la ciberseguridad al menos entre los siguientes organismos públicos: servicios de inteligencia, fuerzas del orden nacionales, autoridades fiscales, agentes gubernamentales, CSIRT nacionales y el ejército?	1	¿Se proporciona a los organismos públicos un mínimo de información unificada sobre las últimas novedades del entorno de las amenazas y el conocimiento de la situación de la ciberseguridad?	1
	2	-		-		¿Ha establecido plataformas de cooperación para el intercambio de información?	1	¿Mide usted los éxitos y los límites de los distintos planes de cooperación al fomentar una cooperación eficaz?	1	-	
16 – Institucionalizar la cooperación entre los organismos públicos	3	-		-		¿Ha definido el alcance de las plataformas de cooperación (por ejemplo las tareas y responsabilidades, número de áreas temáticas)?	1	-		-	
	4	-		-		¿Organiza reuniones anuales?	1	-		-	
	5	-		-		¿Dispone de mecanismos de cooperación entre las autoridades competentes de las distintas regiones geográficas? Por ejemplo, una red de corresponsales de seguridad por región, un oficial de ciberseguridad en las cámaras de comercio regionales...	1	-		-	
17 – Comprometerse con la cooperación internacional (no solo con Estados Miembros de la UE)	a	¿Cubre el objetivo en su ENCS actual o piensa que lo cubrirá en la siguiente edición?	1	¿Existen prácticas informales o actividades que participan en el logro del objetivo de manera no coordinada?	1	¿Dispone de un plan de acción que esté definido formalmente y documentado?	1	¿Revisa su plan de acción en relación con el objetivo para probar su rendimiento?	1	¿Dispone de mecanismos que garanticen que el plan de acción se adapte de forma dinámica a la evolución del medio ambiente?	1
	b			¿Ha definido los resultados previstos, los principios guía o las actividades clave de su plan de acción?	1	¿Tiene un plan de acción con una asignación clara de recursos y gobernabilidad?	1	¿Revisa su plan de acción en relación con el objetivo para asegurarse de que se le asigna la prioridad correcta y se optimiza?	1		
	c			Si es relevante, ¿se ha aplicado su plan de acción y ya es eficaz en un alcance limitado?	0						

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
17 – Comprometerse con la cooperación internacional (no solo con Estados Miembros de la UE)	1	¿ Dispone de una estrategia de compromiso internacional?	1	¿Tiene acuerdos de cooperación con otros países (bilaterales, multilaterales) o con asociados de otros países? Por ejemplo, intercambio de información, creación de capacidad, asistencia...	1	¿Intercambian información a nivel estratégico? Por ejemplo, política de alto nivel, percepción de riesgos...	1	¿Participan los organismos públicos de ciberseguridad de su país en planes de cooperación internacional?	1	¿Dirige usted los debates sobre uno o varios temas en el marco de los acuerdos multilaterales?	1
	2	¿Tiene canales informales de cooperación con otros países?	1	¿Dispone de un punto de contacto único que pueda ejercer una función de enlace que garantice la cooperación transfronteriza con las autoridades de los Estados Miembros (grupo de cooperación, red de CSIRT...)?	1	¿Intercambian información a nivel táctico? Por ejemplo, el boletín de agentes de amenazas, ISAC (Comunidades que comparten datos de análisis inteligentes), técnicas, tácticas y procedimientos..	1	¿Evalúa periódicamente los resultados de las iniciativas de cooperación internacional?	1	¿Dirige usted los debates sobre uno o varios temas en el marco de los tratados o convenciones internacionales?	1
	3	¿Han expresado los dirigentes públicos su intención de participar en la cooperación internacional en el área de la ciberseguridad?	1	¿Dispone de personal dedicado a la cooperación internacional?	1	¿Intercambian información a nivel operativo? Por ejemplo, información de coordinación operativa, incidentes en curso, indicadores de compromiso...	1	-		¿Dirige los debates o las negociaciones en uno o varios temas dentro de los grupos de expertos internacionales? Por ejemplo, la Comisión Mundial sobre la Estabilidad del Ciberespacio (GCSC), el grupo de cooperación de la ENISA NIS, el Grupo de Expertos Gubernamentales de la ONU sobre Seguridad de la Información...	1
	4	-		-		¿ Se compromete con los ejercicios internacionales de ciberseguridad?	1	-		-	
	5	-		-		¿ Se compromete con las iniciativas de creación de capacidad internacionales? por ejemplo, formaciones, desarrollo de aptitudes, realización de procedimientos habituales...	0	-		-	
	6	-		-		¿Ha establecido acuerdos de asistencia mutua con otros países? Por ejemplo, actividades de las AAL, procedimientos legales, reciprocidad de las capacidades de respuesta a incidentes, reparto de activos de ciberseguridad...	0	-		-	

Objetivo de la ENCS	#	Nivel 1	R	Nivel 2	R	Nivel 3	R	Nivel 4	R	Nivel 5	R
	7	-		-		¿Ha firmado o ratificado tratados o convenios internacionales en ciberseguridad? Por ejemplo, el Código Internacional de Conducta para la Seguridad de la Información, el Convenio sobre la Ciberdelincuencia.	0	-		-	

4.2 GUÍAS DE UTILIZACIÓN DEL MARCO

Este apartado tiene el objetivo de proporcionar a los Estados Miembros algunas directrices y recomendaciones para aplicar el marco y rellenar el cuestionario. Las recomendaciones que se enumeran a continuación se derivan principalmente de la información recogida en las entrevistas con los representantes de los Estados Miembros:

- **Prever actividades de coordinación para reunir y consolidar datos.** La mayoría de los Estados Miembros reconocen que la realización de ese ejercicio de autoevaluación debería llevarle 15 días a una persona. A fin de realizar la autoevaluación, habrá que solicitar la participación de una gran cantidad de partes interesadas. Por lo tanto, se recomienda asignar tiempo a la fase de preparación para identificar a todos los interesados relevantes de los órganos gubernamentales, los organismos públicos y el sector privado.
- **Identificar un órgano central encargado de completar la autoevaluación a nivel nacional.** Dado que para reunir el material para todos los indicadores del MANC podrían participar muchos interesados, se recomienda que un órgano u organismo central se encargue de completar la autoevaluación sirviendo como enlace y coordinador de todos los interesados relevantes.
- **Usar el ejercicio de evaluación como una forma de compartir y comunicar en asuntos de ciberseguridad.** El aprendizaje obtenido por los Estados Miembros demostró que los debates (ya sea en forma de entrevistas individuales o de talleres colectivos) son una buena oportunidad para fomentar el diálogo sobre temas de ciberseguridad y para compartir opiniones comunes y áreas de mejora. Además de enfocar los principales logros, el intercambio de resultados también puede ayudar a promover los temas de ciberseguridad.
- **Use la ENCS como ámbito de actuación para seleccionar los objetivos de evaluación.** Los 17 objetivos que componen las ENCS se crearon al basarse sobre los objetivos que normalmente se cubrían en los ENCS de los Estados Miembros. Los objetivos que cubre en parte por la ENCS deberían utilizarse como medio para delimitar el alcance de la evaluación. Sin embargo, las ENCS no deberían limitar la evaluación. Dado que las ENCS se centran de forma natural en las prioridades, se omiten intencionadamente ciertas áreas de las ENCS. Sin embargo, ello no implica que no exista una capacidad determinada. Por ejemplo, en el caso de que se omita un objetivo específico en la ENCS pero el país disponga de capacidades de ciberseguridad relacionadas con ese objetivo, puede realizarse la evaluación de ese objetivo.
- **Cuando el ámbito de la ENCS evolucione, asegúrese de que la interpretación de la puntuación siga siendo coherente con la evolución de la ENCS.** La vida útil del ENCS es un proceso de varios años. La ENCS de algunos Estados Miembros suele reforzarse con una hoja de ruta de 3 a 5 años y presenta cambios en el alcance entre dos ediciones sucesivas de la ENCS. Desde ese punto de vista, hay que tener especial cuidado al presentar los resultados de la autoevaluación entre dos ediciones de la ENCS: los cambios de alcance podrían, de hecho, afectar a la puntuación de madurez definitiva. Se recomienda comparar las puntuaciones en el ámbito completo de los objetivos estratégicos de un año a otro (es decir, la puntuación general definitiva).

Recordatorio sobre el mecanismo de puntuación - ejemplo sobre la tasa de cobertura.
El mecanismo de puntuación incluye dos niveles:
(i) Una **tasa de cobertura general total** basada en la lista completa de objetivos estratégicos presentes en el marco de autoevaluación; y
(ii) una **tasa de cobertura general específica** basada en los objetivos estratégicos seleccionados por el Estado Miembro (que suelen corresponderse con los objetivos presentes en la ENCS del país concreto).

Por su diseño (véase el apartado 3.1 sobre el mecanismo de puntuación), la tasa de cobertura general específica será igual o superior a la tasa de cobertura general total, ya que esta última puede incluir objetivos que no estén cubiertos por el Estado Miembro, lo que reduce la tasa de cobertura general total. Cuando un Estado Miembro añada un nuevo objetivo, la tasa de cobertura total aumentará (es decir, se cubrirán más indicadores de madurez), mientras que la madurez específica total puede disminuir (en caso de que el objetivo recién añadido se encuentre en una fase inicial y, por tanto, tenga un bajo nivel de madurez).

- **Al rellenar el cuestionario de autoevaluación, tenga en cuenta que el objetivo principal es respaldar a los Estados Miembros en la creación de capacidad en ciberseguridad.** Por consiguiente, al rellenar la autoevaluación, aunque en algunas situaciones pueda resultar difícil responder a la pregunta de manera concluyente, se recomienda elegir la respuesta que sea más aceptada en general. Si, por ejemplo, la respuesta a una pregunta es «SÍ» en un ámbito determinado pero es «NO» en otro ámbito, los Estados Miembros deben tener presente que una respuesta de «NO» necesita tomar acción: ya sea un plan de reparación o un plan para actuar en un área de mejora que deba considerarse en próximas revisiones.

5. PRÓXIMOS PASOS

5.1 MEJORAS FUTURAS

Durante las entrevistas con los representantes de los Estados Miembros y durante la fase de investigación documental, también se señalaron como posibles próximas revisiones las siguientes recomendaciones de mejora del actual Marco de Autoevaluación de las Capacidades Nacionales:

- **Desarrollar el sistema de puntuación para permitir una mayor precisión.** Por ejemplo, se podría introducir un porcentaje de cobertura en lugar de la respuesta binaria «SÍ/NO» para calcular mejor la complejidad de la consolidación de las capacidades a nivel nacional. Como primer paso, se eligió un enfoque sencillo con respuestas «SÍ/NO».
- **Introducir medidas cuantitativas que calculen la eficacia de la ENCS de los Estados Miembros.** De hecho, el Marco de Evaluación de las Capacidades Nacionales se centra en la evaluación del nivel de madurez de las capacidades de ciberseguridad de los Estados Miembros. Esto podría complementarse con parámetros que midan la eficacia de las actividades y los planes de acción aplicados por los Estados Miembros para crear esas capacidades. No parecía fiable que se establecieran esos parámetros de eficacia en la etapa actual, dado que hay: poca retroinformación que procede del campo, dificultad para encontrar indicadores significativos que vinculen los resultados con la aplicación de la ENCS y dificultad para establecer indicadores fiables que, por lo tanto, puedan agruparse Sin embargo, este sigue siendo un tema de trabajo para el futuro.
- **Cambio de un ejercicio de autoevaluación a un enfoque de evaluación.** Una posible evolución futura del marco puede que fuera el cambio a un enfoque de evaluación que evalúe la madurez de las capacidades de ciberseguridad de los Estados Miembros de una forma más coherente. El hecho de que un tercero realice la evaluación puede que permita, de hecho, reducir al mínimo los márgenes de error posibles.

ANEXO A – RESUMEN DE LOS RESULTADOS DE LA INVESTIGACIÓN DOCUMENTAL

En el anexo A figura un resumen de la labor anterior de la ENISA sobre la ENCS y un examen de los modelos de madurez relevantes que están disponibles al público sobre la capacidad de la ciberseguridad. Para la selección y el examen de los modelos se tienen en cuenta los siguientes supuestos:

- No todos los modelos se basan en una metodología de investigación rigurosa;
- La estructura y los resultados de los modelos no siempre se explican a fondo, con vínculos claros entre los distintos elementos que caracterizan a cada modelo;
- Algunos modelos no ofrecen detalles sobre el proceso de desarrollo, la estructura y la metodología de evaluación;
- Otros modelos e instrumentos que encontramos no ofrecen detalles sobre la estructura y el contenido y, por lo tanto, no se enumeran; y
- La selección de los modelos para el examen se basa en la cobertura geográfica. El enfoque principal se centra en los modelos de madurez de la capacidad de ciberseguridad creados para evaluar el desempeño de los países europeos. Sin embargo, es importante ampliar la cobertura geográfica para analizar las buenas prácticas al crear modelos de madurez en todo el mundo.

Este examen sistemático de los modelos relevantes de madurez sobre la capacidad de ciberseguridad ,que están disponibles para el público, se llevó a cabo utilizando un marco de análisis personalizado que se basa en la metodología definida por Becker para la elaboración de modelos de madurez.[22] Se analizaron los siguientes elementos para cada modelo de madurez vigente:

- **Nombre del modelo de madurez:** Nombre del modelo de madurez y de las principales referencias;
- **Fuente institucional:** La institución, tanto si es pública como privada, que se encarga del diseño del modelo;
- **Propósito general y objetivo:** El alcance general del modelo y el/los objetivo(s) previsto(s);
- **Número y definición de los niveles:** El número de niveles de madurez del modelo así como su descripción general;
- **Número y nombre de los atributos:** El número y el nombre de los atributos que utiliza el modelo de madurez. El análisis de los atributos tiene un triple objetivo:
  - Desglosar el modelo de madurez en secciones de comprensión fácil;
  - Agregar varios atributos en grupos de atributos que cumplan el mismo objetivo; y
  - Proporcionar diferentes puntos de vista sobre el tema del nivel de madurez.

[22] J. Becker, R. Knackstedt, y J. Pöppelbuß, « Developing Maturity Models for IT Management : A Procedure Model and its Application (Desarrollo de modelos de madurez para la gestión de TI: un modelo de procedimiento y su aplicación)», Business & Information Systems Engineering, vol. 1, no. 3, págs. 213 a 222, junio de 2009.

- **Método de evaluación** El método de evaluación del modelo de madurez;
- **Representación de resultados:** Definir el método de visualización de los resultados del modelo de madurez. La lógica de este paso es que los modelos de madurez tienden a fallar si son demasiado complejos y, por lo tanto, el modo de representación debe satisfacer las necesidades prácticas.

Trabajos anteriores sobre ENCS

La ENISA publicó en 2012 dos documentos sobre el tema de las ENCS como parte de sus primeros esfuerzos. En primer lugar, la «*Practical guide on the development and execution phase of NCSS,* (guía práctica sobre la fase de desarrollo y ejecución de las ENCS)[23] » proponía un conjunto de medidas concretas para la aplicación eficiente de una ENCS y representa la vida útil de la ENCS en cuatro fases: elaboración de estrategias, ejecución de estrategias, evaluación de estrategias y mantenimiento de estrategias. En segundo lugar, en un documento titulado «*Setting the course for national efforts to strengthen security in cyberspace* (marcar el rumbo de los esfuerzos nacionales para fortalecer la seguridad en el ciberespacio)»[24] se esbozaba la situación de las estrategias de ciberseguridad dentro y fuera de la UE en 2012 y se proponía que los Estados Miembros determinaran los temas comunes y las diferencias entre sus ENCS.

En 2014, se publicó el primer marco de la ENISA que evaluaba evaluar la ENCS de un Estado Miembro[25]. Este marco contiene recomendaciones y buenas prácticas, así como un conjunto de herramientas para crear la capacidad que evalúa una ENCS (por ejemplo, objetivos identificados, datos de entrada y de salida, indicadores de rendimiento clave...). Esas herramientas se adaptan a las diversas necesidades de los países con distintos niveles de madurez en su planificación estratégica. Ese mismo año, la ENISA publicó el «*Online NCSS Interactive Map* , (mapa interactivo en línea de la ENCS)»[26], que permite a los usuarios consultar rápidamente las ENCS de todos los Estados Miembros y de los países de la AELC, incluidos sus objetivos estratégicos y modelos de aplicación. El mapa, que se elaboró primero como depósito de la ENCS (2014), se actualizó con ejemplos de implementación en 2018 y, desde 2019, actúa como centro de información que centraliza los datos facilitados por los Estados Miembros sobre sus esfuerzos por mejorar la ciberseguridad nacional.

«La Guía de buenas prácticas de ENCS»[27] , publicada en 2016, identifica 15 objetivos estratégicos: Esta guía también analiza el estado de implementación de la ENCS de cada Estado Miembro e identifica varias lagunas y retos en relación a dicha implementación.

[23] ENCS: Practical Guide on Development and Execution (ENISA, 2012), (Guía práctica de desarrollo y ejecución)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] ENCS: «Setting the course for national efforts to strengthen security in cyberspace, (marcar el rumbo de los esfuerzos nacionales en el fortalecimiento de la seguridad en el ciberespacio)» (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] An evaluation framework for NCSS, (marco de evaluación para la ENCS), (ENISA, 2014).
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] National Cybersecurity Strategies - Interactive Map, (estrategias nacionales de ciberseguridad- mapa interactivo), (ENISA, 2014, actualizado en 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Este documento actualiza la guía de 2012: Guía de buenas prácticas de la ENCS: Designing and Implementing National Cybersecurity Strategies, (diseño e implementación de las estrategias nacionales de ciberseguridad), (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

A continuación, en 2018, la ENISA publicó la «Herramienta de evaluación de las estrategias nacionales de ciberseguridad»[28]: un instrumento interactivo de autoevaluación que ayude a los Estados Miembros a evaluar sus prioridades y objetivos estratégicos relacionados con su ENCS. Mediante un conjunto de preguntas sencillas, esta herramienta proporciona a los Estados Miembros recomendaciones específicas para aplicar cada objetivo. Por último, en el documento publicado en 2019 «buenas prácticas de innovación en materia de ciberseguridad en el marco de la ENCS»[29] se presenta el tema de la innovación en materia de ciberseguridad en el marco de la ENCS. En el documento se exponen los retos y las buenas prácticas en los diferentes campos de la innovación, tal como las perciben los expertos en la materia, para ayudar a redactar los futuros objetivos estratégicos de innovación.

A.1 Modelo de madurez de la capacidad de ciberseguridad de las naciones(CMM)

El Modelo de madurez de la capacidad de ciberseguridad de las naciones (CMM) se ha desarrollado por el Centro de Capacidad de Ciberseguridad Mundial (Centro de Capacidad), que forma parte de la Escuela Martin de la Universidad de Oxford. El objetivo del Centro de Capacidad es aumentar la escala y la eficacia de la creación de capacidad en ciberseguridad, tanto en el Reino Unido como a nivel internacional, mediante la utilización del Modelo de Madurez de la Capacidad en Ciberseguridad (MMC). El CMM se dirige directamente a los países que quieran aumentar su capacidad nacional en ciberseguridad. El MMC, que se utilizó por primera vez en 2014, se revisó en 2016 tras usarse en el examen de 11 capacidades nacionales en ciberseguridad.

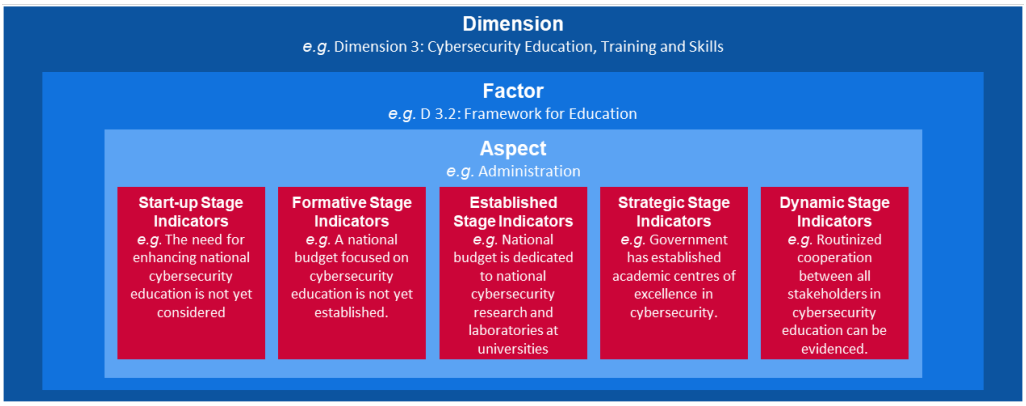
Características/Dimensiones

El CMM considera que la capacidad de ciberseguridad se compone de **cinco dimensiones** que representan los grupos de capacidad de ciberseguridad. Cada grupo representa un «prisma » de investigación diferente a través del que se estudia y se comprende la capacidad. Dentro de las cinco dimensiones, los **factores** describen lo qué es tener la capacidad de ciberseguridad. Estos detalles son elementos que contribuyen a la mejora en la madurez de la capacidad de ciberseguridad dentro de cada dimensión. Cada factor se representa por varios **aspectos** que lo componen. Los aspectos representan un método organizativo que divide los indicadores en pequeños grupos que son más fáciles de comprender. Después, cada aspecto se evalúa mediante **indicadores** que describen los pasos, las acciones o los elementos constitutivos que son indicativos de una etapa específica de madurez (definida en la siguiente sección) dentro de un aspecto, un factor y una dimensión distintos.

Los términos que se mencionan antes pueden superponerse, como se muestra en la figura siguiente.

[28] *National Cybersecurity Strategies Evaluation Tool,* (herramienta de evaluación de estrategias nacionales de ciberseguridad (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

Figura 4: Ejemplo de indicadoresMMC



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Dimensión, por ejemplo: dimensión 3: Educación en ciberseguridad, formación y habilidades
Factor e.g. D 3.2: Framework for Education	Factor, por ejemplo D 3.2: Marco para la educación
Aspect e.g. Administration	Aspecto, por ejemplo administración
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Indicadores del grado de puesta en marcha, por ejemplo la razón para mejorar la educación nacional en materia de ciberseguridad aún no se considera
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Indicadores de la etapa de formación, por ejemplo un presupuesto nacional centrado en la educación sobre ciberseguridad no está establecido todavía
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Indicadores de la etapa de establecimiento, por ejemplo, el presupuesto nacional se dedica a la investigación en ciberseguridad y los laboratorios de las universidades
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Indicadores de la etapa estratégica, por ejemplo el Gobierno ha instaurado un centro académico de excelencia para la educación en ciberseguridad.
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Indicadores de la etapa dinámica, por ejemplo, rutina en cooperación entre todas las partes interesadas

A continuación se detallan las cinco dimensiones:

i Elaboración de una política y estrategia de ciberseguridad (6 factores);
ii Fomento de una cultura responsable de ciberseguridad en la sociedad (5 factores);
iii Desarrollo de conocimientos sobre ciberseguridad (3 factores);
iv Creación de marcos jurídicos y reglamentarios eficaces (3 factores); y
v Control de los riesgos a través de normas, organizaciones y tecnologías (7 factores).

Niveles de madurez

El MMC usa **5 niveles de madurez** que determinan el grado de progreso de un país en relación con un determinado factor/aspecto en la capacidad de ciberseguridad. Estos niveles sirven como una captura de imagen de la capacidad de ciberseguridad presente:

- Puesta en marcha: En esta etapa, o bien no existe una madurez en materia de ciberseguridad, o bien es de naturaleza muy embrionaria. Es posible que haya

debates iniciales sobre la creación de capacidad en ciberseguridad, pero no se han tomado medidas concretas. En esta etapa no se observan pruebas;

- **Formativa:** Algunas características de los aspectos han comenzado a crecer y a formularse, pero pueden ser ad hoc, desorganizadas, mal definidas, o simplemente «nuevas». Sin embargo, pueden demostrarse claramente las pruebas de esta actividad;
- **Establecida:** Los elementos del aspecto están funcionando y en su sitio. No obstante, no se ha estudiado bien la asignación relativa de los recursos. Se han negociado pocas decisiones sobre la inversión «relativa» de los elementos varios del aspecto. Sin embargo, el aspecto es funcional y está definido;
- **Estratégica:** Se han tomado decisiones sobre qué partes del aspecto son importantes y cuáles son menos importantes para la organización o país concreto. La etapa estratégica muestra el hecho de que se han tomado estas decisiones condicionadas a las circunstancias particulares del país u organización; y
- **Dinámica:** En esta etapa existen mecanismos claros en su sitio que modifican la estrategia en función de las circunstancias imperantes, como la tecnología del entorno de la amenaza, el conflicto mundial o un cambio significativo en un área de interés (por ejemplo, la ciberdelincuencia o la privacidad). Las organizaciones dinámicas han desarrollado métodos que cambian las estrategias a pasos agigantados. Son características de esta etapa la rápida toma de decisiones, la reasignación de recursos y la atención constante al cambio del entorno.

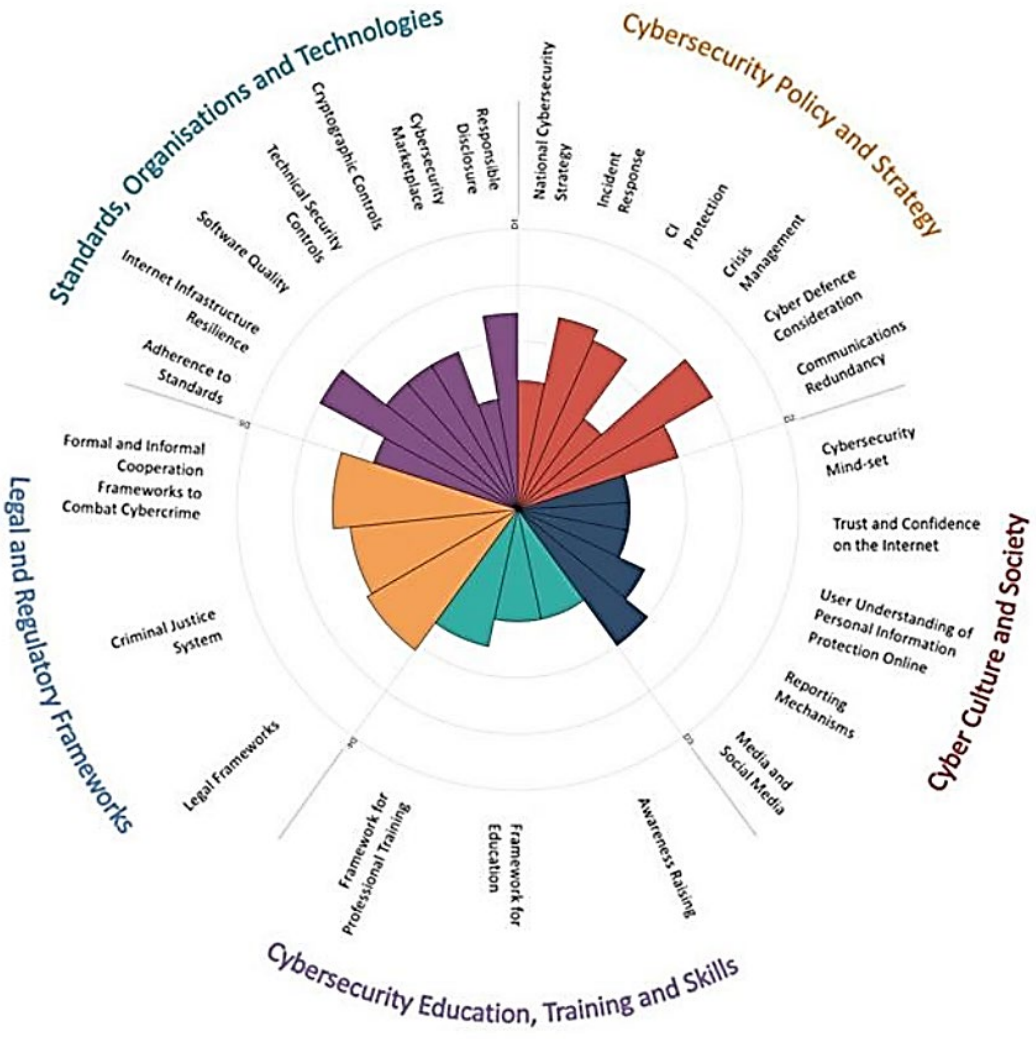
Método de evaluación

Como el centro de capacidad no tiene un conocimiento profundo y exhaustivo de cada contexto nacional en el que se usa el modelo, éste trabaja junto con organizaciones internacionales, ministerios anfitriones u organizaciones del país respectivo para examinar la madurez de la capacidad de ciberseguridad. Para evaluar el nivel de madurez de las cinco dimensiones que comprende el MMC, el centro de capacidad y la organización anfitriona se reúnen durante 2 o 3 días con los interesados nacionales de relevancia de los sectores públicos y privados para que dirijan grupos de enfoque sobre las dimensiones del MMC. Los grupos de interesados diferentes debaten cada dimensión al menos un par de veces. Esto constituye el conjunto preliminar de datos para la evaluación posterior.

Modo o representación de los resultados

El MCC proporciona una visión general del nivel de madurez de cada país a través de un radar compuesto por cinco secciones, una para cada dimensión. Cada dimensión representa una quinta parte del gráfico, con las cinco etapas de madurez de cada factor que van desde el centro del gráfico hacia afuera. Como se muestra a continuación, la «puesta en marcha» está más cerca del centro del gráfico y la «dinámica» está en el perímetro.

Figura 5 CMM: Resumen de resultados



Standards, Organisations and Technologies	Normas, entidades y tecnología
Legal Regulatory Frameworks	Marco jurídico y normativo
Cybersecurity Education, Training and Skills	Educación en ciberseguridad, formación y habilidades
Cybersecurity Policy and Strategy	Política de ciberseguridad y estrategia
Cyber Culture and Society	Cibercultura y sociedad
Responsible Disclosure	Divulgación responsable
Cybersecurity market place	Mercado mundial de ciberseguridad
Cryptographic Controls	Controles criptográficos
Technical Security Controls	Controles técnicos de seguridad
Software Quality	Calidad de *software*
Internet Infrastructure Resilience	Resiliencia de infraestructura de internet
Adherence to Standards	Adhesión a las normas
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Marcos de cooperación formales e informales para luchar contra la ciberdelincuencia
Criminal Justice System	Sistema judicial penal
Legal Frameworks	Marco jurídico
Framework for Professional Training	Marco para la formación profesional
Framework for Education	Marco para la educación
Awareness Raising	Concienciación
Media and Social Medai	Medios de comunicación y redes sociales
Reporting Mechanisms	Mecanismos de información
User Understanding of Personal Information Protection Online	Entendimiento de los usuarios sobre la protección en línea de la información personal
Trust and Confidence on the Internet	Fiabilidad y confianza en internet
Cybersecurity Mind-set	Mentalidad cibersegura
Communications Redundancy	Redundancia de comunicaciones
Cyber Defence Consideration	Consideración de la ciberdefensa
Crisis Management	Gestión de crisis
CI Protection	Protección de la ciberinformación

Incident Response	Respuesta a incidentes
National Cybersecurity Strategy	Estrategias nacionales de ciberseguridad

Centro de Capacidad de Ciberseguridad Mundial de la Escuela *Martin*, 2017, Universidad de Oxford.

A.2 Modelo de madurez de las capacidades en ciberseguridad(C2M2)

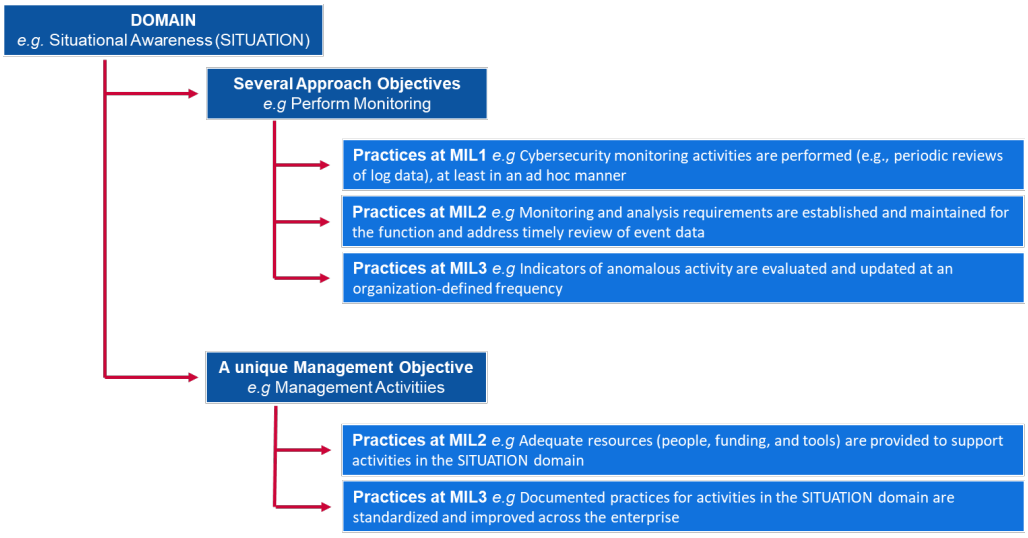
El Modelo de madurez de la capacidad de ciberseguridad (C2M2) se ha desarrollado por el departamento de Energía de EEUU en colaboración con expertos de los sectores privado y público. El objetivo del Centro de Capacidad es el de ayudar a las organizaciones de todos los sectores, tipos y tamaños a que evalúen y progresen en sus programas de ciberseguridad y que refuercen su resiliencia operativa. El C2M2 se concentra en la implementación y la gestión de prácticas de seguridad asociadas con los activos de la información, la tecnología de la información (IT) y la tecnología de operaciones (TO) y los entornos en los que actúan. El C2M2 define los modelos de madurez como: «un conjunto de características, atributos, indicadores o patrones que representan la capacidad y progreso en una disciplina concreta». El C2M2, que se utilizó por primera vez en 2014, se revisó en 2019.

Características/Dimensiones

El C2M2 considera **diez dominios** que representan un grupo lógico de prácticas de ciberseguridad. Cada conjunto de prácticas representa las actividades que una organización lleva a cabo cuando establece y madura la capacidad en el dominio. Cada dominio se asocia entonces con un **único objetivo de gestión** y **varios objetivos de aproximación**. Dentro de los objetivos de aproximación y gestión se detallan **varias prácticas** que describen las actividades institucionalizadas.

La relación entre estas nociones se resume a continuación:

Figura 6: Ejemplo de indicadores MMC



Domain eg Situational Awareness (SITUATION)	**Dominio,** por ejemplo, consciencia situacional (SITUACIÓN);
Several Approaches Objectives e.g. Perform Monitoring	**Varios objetivos de aproximación**, por ejemplo, realizar el seguimiento
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Prácticas en NIM1,** por ejemplo, las actividades de seguimiento de ciberseguridad se ejecutan (por ejemplo revisiones periódicas de datos de registro), al menos de manera ad hoc
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Prácticas en NIM2**, por ejemplo, se establecen y mantienen los requisitos de seguimiento y análisis para la función y se aborda la revisión oportuna de los datos de los acontecimientos
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Prácticas en NIM3**, por ejemplo, los indicadores de actividad anómala se evalúan y actualizan según una frecuencia definida por la institución
A unique Management Objectve e.g. Management Activities	Un objetivo de gestión único, por ejemplo, actividades de gestión

Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Prácticas en NIM2,** por ejemplo, se dota de los recursos apropiados (personal, fondos y herramientas) que respaldan las actividades en el dominio situación
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Prácticas en NIM3,** por ejemplo, las prácticas documentadas para las actividades en el dominio situación se estandarizan y se mejoran en toda la empresa

Los diez dominios se detallan a continuación:

i Gestión de riesgo (RIESGO);
ii Gestión de activos, cambios y configuración (ACTIVO);
iii Gestión de identidad y acceso (ACCESO);
iv Gestión de amenazas y vulnerabilidad (AMENAZA);
v Consciencia situacional (SITUACIÓN);
vi Respuesta a eventos e incidentes (RESPUESTA);
vii Gestión de la cadena de suministros y dependencias externas (DEPENDENCIAS);
viii Gestión de la plantilla (PLANTILLA);
ix Arquitectura de ciberseguridad (ARQUITECTURA); y
x Gestión del programa de ciberseguridad (PROGRAMA).

Niveles de madurez

El C2M2 usa **4 niveles de madurez** (denominados Niveles Indicadores de Madurez- NIM) que determinan una progresión dual de madurez: una progresión de aproximación y de gestión. El rango de los NIM va de NIM0 a NIM3 y están destinados para aplicarse independientemente para cada dominio.

- **NIM0:** No se realizan prácticas.
- **NIM1:** Las prácticas iniciales se realizan, pero puede que sean ad hoc.
- **NIM2:** Características de la gestión:
  - Las prácticas se documentan;
  - Se proporcionan recursos adecuados para respaldar el proceso;
  - El personal que realiza las prácticas tiene las aptitudes y los conocimientos adecuados; y
  - Se asignan la responsabilidad y la autoridad para llevar a cabo las prácticas.

  Característica de aproximación:
  - Las prácticas son más completas o avanzadas que en la NIM1.
- **NIM3:** Características de la gestión:
  - Las actividades se guían a través de políticas (u otras directivas organizativas);
  - Se establecen y se supervisan objetivos de rendimiento para las actividades del dominio a fin de hacer un seguimiento de los logros; y
  - Las prácticas documentadas para las actividades de dominio se normalizan y mejoran en toda la empresa.

  Característica de aproximación:
  - Las prácticas son más completas o avanzadas que en la NIM2.

Método de evaluación

El C2M2 se diseña para que una organización lo use con una **metodología de autoevaluación** y unas herramientas (disponibles bajo petición) que midan y mejoren su programa de ciberseguridad. Una autoevaluación puede completarse en un día usando las herramientas, pero dichas herramientas podrían adaptarse para un esfuerzo de evaluación más riguroso Además, el C2M2 puede usarse de guía para desarrollar un programa de ciberseguridad nuevo.

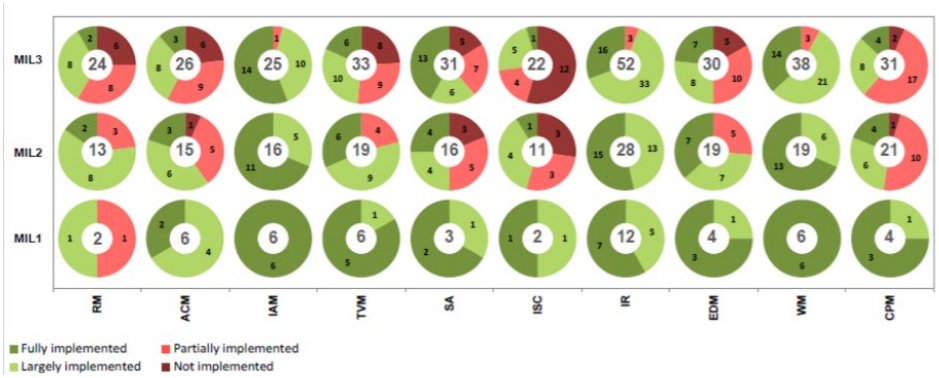
El contenido del modelo se representa con un nivel alto de abstracción de manera que las organizaciones de varios tipos, estructuras, tamaños e industrias puedan interpretarlas. El uso amplio del modelo por parte de un sector puede respaldar el análisis comparativo de las capacidades del sector en ciberseguridad.

Modo o representación de los resultados

EL C2M2 produce un informe de evaluación de resultados que se genera por los datos de la encuesta. El informe presenta resultados en dos vertientes: el punto de vista del objetivo, que muestra las respuestas a las preguntas prácticas por cada dominio y sus objetivos y el punto de vista del dominio, que muestra las respuestas de todos los dominios y los NIM. Ambas opiniones se basan en un sistema de representación que se caracteriza con gráficos circulares de tarta (o «de rosquilla») uno por respuesta y con un mecanismo de puntuación con los colores del semáforo. Como se muestra en Figura 7, los sectores rojos del gráfico de rosquilla muestran un recuento del número de preguntas de la encuesta respondidas con un «no implementado», (rojo oscuro) o «implementado parcialmente», (rojo claro). Los sectores verdes muestran el número de preguntas respondidas con respuesta «implementado en gran parte», (verde claro) o «implementado por completo», (verde oscuro).

Figura 7 a continuación es un ejemplo de tarjeta de puntuación al terminar de una evaluación de madurez. En el eje X se encuentran los 10 dominios de C2M2, y en el eje Y, los niveles de madurez (NIM). Si se observa el gráfico y se considera el dominio de la gestión de riesgos (GR), es posible que se observen tres gráficos de tarta, uno por cada nivel de madurez NIM1, NIM2 y NIM3. En el caso del dominio de la GR, el gráfico destaca que hay dos elementos que hay que evaluar para que alcancen el primer nivel de madurez, el NIM1. En este caso, una puntuación «implementado en gran parte» y otra, «implementado parcialmente». Para el segundo nivel de madurez, NIM2, el modelo prevé 13 puntos de evaluación. Dos de esos 13 elementos pertenecen al primer nivel, NIM1, y 11 al segundo nivel, NIM2. Lo mismo se aplica para el tercer nivel, NIM3.

Figura 7: Ejemplo de vista del dominio C2M2



Fully implemented	Implementado por completo
Largely implemented	Implementado en gran parte
Partially implemented	Implementado parcialmente
Not implemented	No implementado
MIL1	NIM1:
MIL2	NIM2:
MIL3	NIM3:
RM	RM
ACM	ACM
IAM	GIA
TVM	TVM
SA	AE
ISC	ISC
IR	IR
EDM	EDM
WM	WM
CPM	CPM

Fuente: Departamento de Energía de EEUU, Oficina de suministro eléctrico y fiabilidad energética

A.3 Marco para la mejora de las infraestructuras críticas en ciberseguridad

El marco para la mejora de las infraestructuras críticas en ciberseguridad fue desarrollado por el Instituto Nacional de Normas y Tecnología (INNT). Se centra en la guía de las actividades de ciberseguridad y la gestión de los riesgos de una organización. Se dirige a todo tipo de organizaciones, independientemente de su tamaño, del grado de riesgo de ciberseguridad o de la sofisticación de la ciberseguridad. Al tratarse de un marco y no de un modelo, se construye de forma diferente a los modelos analizados antes.

El marco consta de tres partes: el núcleo del marco, los niveles de implementación y los perfiles del marco:

- El **núcleo del marco** es un conjunto de actividades de ciberseguridad, resultados deseados y referencias aplicables que son comunes a todos los sectores de las infraestructuras esenciales. Son similares a los atributos o dimensiones que se encuentran en los modelos de madurez de la capacidad de ciberseguridad.
- **Los niveles de implementación del marco** («niveles») proporcionan un contexto sobre la forma en que una organización considera el riesgo de ciberseguridad y los procesos establecidos para gestionar ese riesgo. Los niveles (que van desde el parcial (Nivel 1) hasta el adaptativo (Nivel 4)) describen un grado cada vez mayor de rigor y sofisticación en las prácticas de gestión de riesgos de ciberseguridad. Los niveles no representan niveles de madurez, sino que se destinan a respaldar la toma de decisiones organizativa sobre cómo gestionar el riesgo de ciberseguridad y qué dimensiones de la organización son de mayor prioridad y pueden recibir recursos suplementarios.
- **Un perfil del marco** («perfil») representa los resultados basados en las necesidades comerciales que una organización selecciona desde las categorías y subcategorías del marco. El perfil se caracteriza con respecto a la unificación de las normas, directrices y prácticas con el núcleo del marco en un entorno de aplicación determinado. Los perfiles se usan para identificar oportunidades de mejora en la postura de la ciberseguridad al comparar un perfil «actual» (el estado «tal cual») con un perfil «objetivo» (el estado «futuro »).

Núcleo del marco

El núcleo del marco consta de cinco **funciónes**. Cuando se consideran en conjunto, estas funciones proporcionan una visión estratégica de alto nivel de la vida útil de la gestión del riesgo de ciberseguridad de una organización. Entonces, el núcleo del marco identifica las **categorías** y **subcategorías** clave subyacentes para cada función y las compara con referencias informativas de ejemplo como las normas, directrices y prácticas vigentes para cada subcategoría.

Las funciones y categorías se detallan a continuación:

Identificar:

i **Identificar:** Desarrollar un entendimiento organizativo sobre cómo gestionar los riesgos de seguridad para los sistemas, las personas, los activos, los datos y las capacidades.
   - Subcategorías: Gestión de activos, entorno empresarial; gobernabilidad; gestión de riesgos; y estrategia de gestión de riesgos

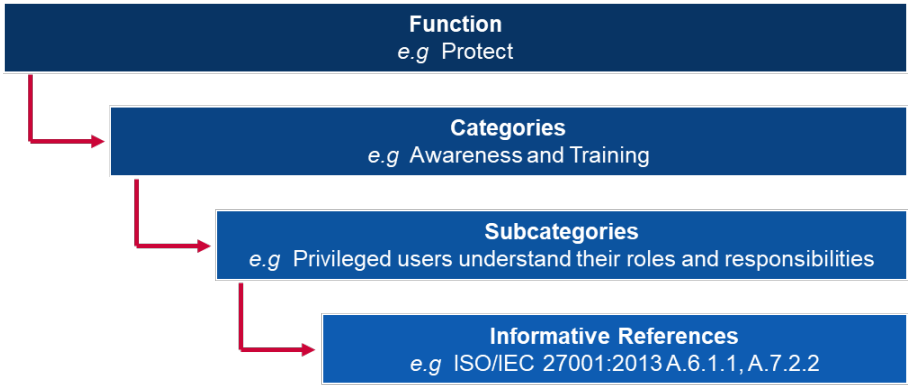
ii **Proteger:** Desarrollar e implementar salvaguardias apropiadas que aseguren la ejecución de los servicios críticos.
   - Subcategorías: Gestión de identidad y control de accesos; conciencia y formación; seguridad de datos; procesos de protección de información y procedimientos; mantenimiento; y tecnología protectora

iii **Detectar:** Desarrollar e implementar actividades adecuadas que identifiquen si se produce un acontecimiento de ciberseguridad.
   - Subcategorías: Anomalías y acontecimientos; seguimiento continuo de seguridad; y procesos de detección.

iv **Responder:** Desarrollar e implementar actividades adecuadas que tomen medidas en cuanto se detecte un incidente de ciberseguridad.
- Subcategorías: Plan de respuesta; comunicaciones; análisis; mitigación; y mejoras.

v **Recuperar:** Desarrollar e implementar actividades adecuadas que mantengan los planes para la resiliencia y que restauren cualesquiera capacidades o servicios que se hayan deteriorado por un incidente de ciberseguridad.
- **Subcategorías:** Planes de recuperación; mejoras; y comunicaciones

Figura 8: Ejemplo del marco para la mejora de las infraestructuras críticas en ciberseguridad



Function e.g Project
Categories e.g Awarness and Training
Subcategories e.g Privileged useres understand their roles and responsibilities
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Función, por ejemplo: proyecto
Categorías, por ejemplo: concienciación y formación
Subcategorías, por ejemplo: los usuarios privilegiados entienden sus funciones y responsabilidades
Referencias a título informativo, por ejemplo: ISO/IEC 27001:2013 A.6.1.1, A.7.2.2

Niveles

El marco de mejora de infraestructura crítica de ciberseguridad se basa en **4 niveles**, cada uno de los cuales se define a lo largo de 3 ejes: Proceso de gestión de riesgos, programa de gestión de riesgos integrados y participación externa. Los niveles no pueden considerarse como niveles de madurez sino como un marco que proporcione a las organizaciones una contextualización de sus opiniones sobre riesgos de ciberseguridad y los procesos en marcha que gestionen esos riesgos.

- **Nivel 1: Parcial**
  - **Proceso de gestión de riesgos**: las prácticas de gestión de riesgos de ciberseguridad de la organización no están formalizadas y el riesgo se gestiona de forma ad hoc y a veces reactiva;
  - **Programa integrado de gestión de riesgos:** hay una conciencia limitada del riesgo de ciberseguridad a nivel de la organización. La organización implementa la gestión de riesgos de ciberseguridad de forma irregular, caso por caso, y puede que no disponga de procesos que permitan compartir la información sobre la ciberseguridad dentro de la organización;
  - **Participación externa:** la organización no entiende su función en el ecosistema más amplio con respecto a sus dependencias o a sus dependientes. En general, la organización no es consciente de los riesgos de la cadena de cibersuministro de los productos y servicios que proporciona y que usa;
- **Nivel 2: Informado de los riesgos**
  - **Proceso de gestión de riesgos:** las prácticas de gestión de riesgos se aprueban por la administración pero no pueden establecerse como política para toda la organización;
  - **Programa integrado de gestión de riesgos:** existe una conciencia del riesgo de ciberseguridad a nivel de la organización, pero no se ha establecido un enfoque

de gestión del riesgo de ciberseguridad a nivel de toda la organización. La evaluación del ciberriesgo de los activos externos y de la organización se produce pero no suele repetirse o ser recurrente;
- **Participación externa:** la organización no entiende su función en el ecosistema más amplio con respecto a sus dependencias o a sus dependientes,. Además, la organización es consciente de los riesgos de la cadena de cibersuministro asociados a los productos y servicios que proporciona y utiliza, pero no actúa de manera coherente o formal ante esos riesgos;

- **Nivel 3: Repetible**
  - **Proceso de gestión de riesgos:** las prácticas de gestión de riesgos de la organización se aprueban oficialmente y se expresan como políticas. Las prácticas de ciberseguridad de la organización se actualizan periódicamente basándose sobre la aplicación de los procesos de gestión de riesgos a los cambios en los requisitos de las empresas/misiones y a la evolución del entorno de las amenazas y la tecnología;
  - **Programa integrado de gestión de riesgos:** existe un enfoque a nivel de toda la organización que gestiona el riesgo de ciberseguridad. Las políticas, los procesos y los procedimientos informados sobre los riesgos se definen, se aplican según lo previsto y se revisan. Los altos ejecutivos garantizan que se considera la ciberseguridad en todas las líneas de operación de la organización;
  - **Participación externa**: la organización entiende su papel, sus dependencias y sus dependientes en el ecosistema más amplio y puede que contribuya a la comprensión más amplia de los riesgos por parte de la comunidad. La organización es consciente de los riesgos de la cadena de cibersuministro asociados a los productos y servicios que proporciona y que utiliza;
- **Nivel 4: Adaptativo**
  - **Proceso de gestión de riesgos:** la organización adapta sus prácticas de ciberseguridad que se basan en actividades de ciberseguridad anteriores y actuales, incluyendo los aprendizajes adquiridos y los indicadores de predicción;
  - **Programa integrado de gestión de riesgos:** existe un enfoque de toda la organización para la gestión de los riesgos de ciberseguridad que utiliza políticas, procesos y procedimientos basados en el riesgo para hacer frente a los posibles incidentes de ciberseguridad; y
  - **Participación externa:** la organización entiende su papel, sus dependencias y sus dependientes en el ecosistema más amplio y contribuye a la comprensión más amplia de los riesgos por parte de la comunidad.

Método de evaluación

El marco para la mejora de la ciberseguridad de las infraestructuras críticas se destina a que las organizaciones autoevalúen sus riesgos para que su enfoque de ciberseguridad y sus inversiones sean más racionales, eficaces y valiosas. Para examinar la eficacia de las inversiones, una organización debe tener en primer lugar una clara comprensión de sus objetivos organizativos, de la relación entre dichos objetivos y de los resultados de respaldo a la ciberseguridad. Los resultados en ciberseguridad del marco básico respaldan la autoevaluación de la eficacia de las inversiones y de las actividades de ciberseguridad.

A.4 Modelo catarí de madurez de la capacidad en ciberseguridad(Q-C2M2)

El Modelo de Madurez de la Capacidad de Ciberseguridad Catarí (Q-C2M2) fue desarrollado en 2018 por la Facultad de Derecho de la Universidad de Catar. El Q-C2M2 se basa en varios modelos vigentes para construir una metodología de evaluación integral que mejore el marco de ciberseguridad catarí.

Características/Dimensiones

El Q-C2M2 adopta el enfoque del marco del Instituto Nacional de Normas y Tecnología (INNT) que usa cinco funciones básicas como principales dominios del modelo. Las cinco funciones básicas se aplican en el contexto catarí porque son comunes a todos los sectores de infraestructura crítica, un elemento importante del marco de ciberseguridad catarí. La Q-C2M2

se basa en **cinco dominios**, cada uno de los cuales se divide a su vez en varios **subdominios** que cubren toda la gama de madurez de capacidad de ciberseguridad.

Los cinco dominios se detallan a continuación:

i El **«dominio entendimiento»** incluye cuatro subdominios: Cibergobernabilidad, activos, riesgos y formación;
ii Los subdominios bajo el **«dominio seguridad»** incluyen seguridad de datos, seguridad de tecnología, seguridad de control de accesos, seguridad de comunicaciones y seguridad de personal;
iii El **«dominio exposición»** incluye los subdominios de monitoreo, gestión de incidentes, detección, análisis y exposición;
iv El **«dominio respuesta»** incluye la planificación de respuesta, mitigación y comunicación de respuesta; y
v El **«dominio sostenibilidad»** incluye la planificación de la recuperación, la gestión de la continuidad, la mejora y las dependencias externas.

Niveles de madurez

El Q-C2M2 utiliza **5 niveles de madurez** que miden la madurez de la capacidad de una entidad del estado o de una organización no estatal a nivel de la función central. Estos niveles tienen como finalidad evaluar la madurez en los cinco dominios que se detallan en el apartado anterior.

- **Inicial:** Emplea prácticas ad hoc de ciberseguridad y procesos bajo algunos de los dominios;
- **Implementado:** Se adoptan políticas que implementan todas las actividades de ciberseguridad bajo los dominios con el fin de completar la implementación en un momento determinado;
- **En desarrollo:** Implementar políticas y prácticas que desarrollen y mejoren las actividades de ciberseguridad bajo los dominios con el fin de sugerir nuevas actividades que implementar;
- **Adaptativo:** Vuelve y revisa las actividades de ciberseguridad y adopta las prácticas basadas en los indicadores predictivos que se derivan de experiencias previas y mediciones; y
- **Ágil:** Continúa practicando la etapa de adaptación con un énfasis añadido en la agilidad y en la velocidad cuando implementa actividades en los dominios.

Método de evaluación

El Q-C2M2 se encuentra en una fase inicial de investigación y aún no está construido para su implementación. Se trata de un marco que podría utilizarse para desplegar un modelo de evaluación detallado para las instituciones cataríes en el futuro.

A.5 Certificación del modelo de madurez de la ciberseguridad (CMMC)

Certificación del modelo de madurez de la ciberseguridad (CMMC)

El modelo de Certificación de Madurez de la Ciberseguridad (CMMC) fue desarrollado por el Departamento de Defensa de los Estados Unidos en colaboración con la Universidad *Carnegie Mellon* y el Laboratorio de Física Aplicada de la Universidad *Johns Hopkins*. El objetivo principal del DdD al diseñar este modelo es proteger la información del sector de la Base Industrial de Defensa (DIB). La información a la que apunta el CMMC se clasifica como «información de contratos federales», información proporcionada o generada por el Gobierno en virtud de contratos no destinados a la divulgación pública, o «información no clasificada controlada», información que requiere la salvaguardia o los controles de divulgación de conformidad con las leyes, los reglamentos y las políticas de todo el Gobierno. El CMMC mide la madurez de la ciberseguridad y proporciona las buenas prácticas junto con un elemento de

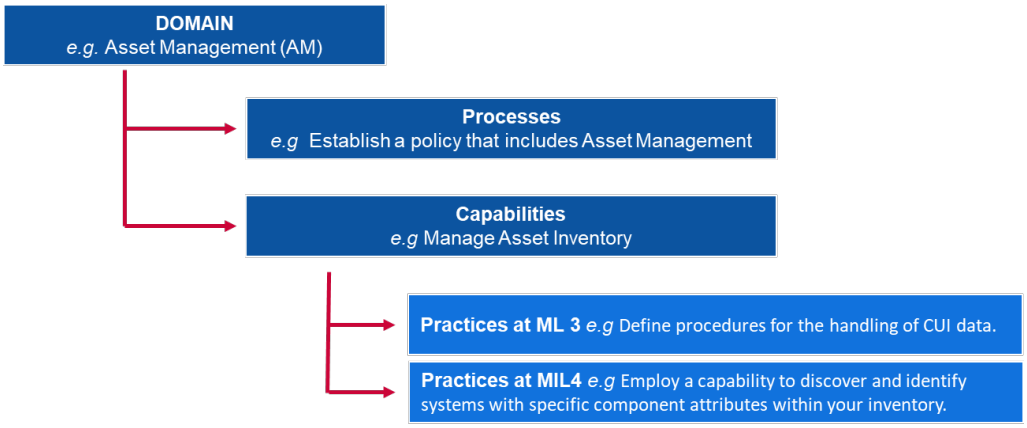
certificación que garantice la aplicación de las prácticas asociadas a cada nivel de madurez. La última versión del CMMC se publicó en 2020.

Características/Dimensiones

El CMMC considera **diecisiete dominios** que representan grupos de procesos y capacidades de ciberseguridad. Cada dominio se desglosa después en múltiples **procesos** que son similares en todos los dominios; y de una a muchas **capacidades** que abarcan más de cinco niveles de madurez. Las capacidades (o capacidad) se detallan después en **prácticas** para cada nivel de madurez relevante.

La relación entre estas nociones es la siguiente:

Figura 9: Ejemplo de indicadoresCMMC



DOMAIN e.g. Asset Management (AM)
Processes
e.g Establish a policy that includes Asset Management
Capabilities
e.g Manage Asset Inventory
Practices at ML 3 e.g Define procedures for the handling of CUI data

Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory

DOMINIO, por ejemplo, gestión de activos (GA)
Procesos, por ejemplo, establecer una política que incluya gestión de activos
Capacidades, por ejemplo gestionar el inventario de activos

Prácticas en NIM3, por ejemplo, definir los procedimientos para manejar los datos de INC
Prácticas en NIM4, por ejemplo, emplear una capacidad que descubra e identifique sistemas con características de componentes específicos dentro del inventario

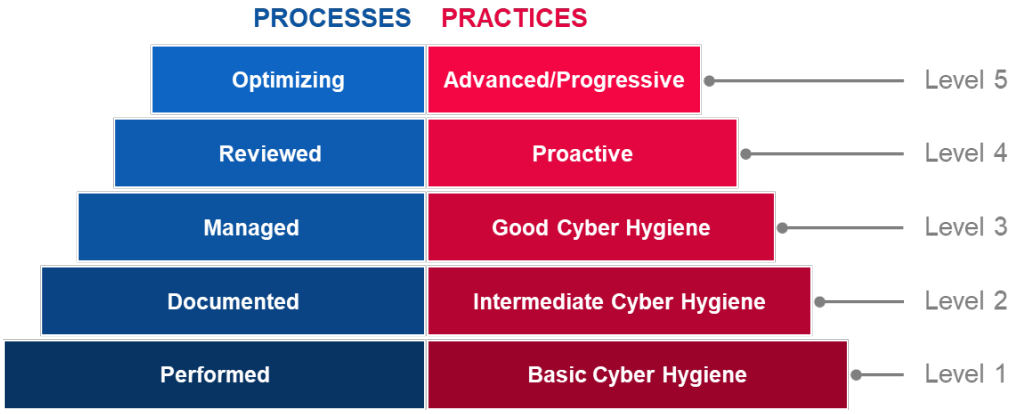
A continuación se detallan los 17 dominios:

i Control de accesos (CA);
ii Gestión de Activos (GA);
iii Auditoría y responsabilidad (AU);
iv Concienciación y formación (CF);
v Gestión de la configuración (GC);
vi Identificación y autenticación (IA);
vii Respuesta a incidentes (RI);
viii Mantenimiento (MA);
ix Protección de los medios de comunicación (PM);
x Seguridad del personal (SP);
xi Protección física (PF);
xii Recuperación (RE);
xiii Gestión de riesgos (GR);
xiv Evaluación de seguridad (ES);
xv Consciencia situacional (CS);
xvi Protección de los sistemas y las comunicaciones (PS); y
xvii Integridad de los sistemas y la información (IS).

Niveles de madurez

El CMMC utiliza **5 niveles de madurez** que se definen basándose en procesos y prácticas. Para alcanzar un cierto nivel de madurez en el CMMC, una organización debe cumplir los requisitos previos de los procesos y de las prácticas en ese mismo nivel. Esto también implica el cumplimiento de los requisitos previos de todos los niveles inferiores a ese.

Figura 10: Niveles de madurez de CMMC



PROCESSES	PROCESOS
Optimizing	Optimizado
Reviewed	Revisado
Managed	Gestionado
Performed	Realizados
Documented	Documentado
PRACTICES	PRÁCTICAS
Advanced/Progressive	Avanzadas/ en progreso
Proactive	Proactivo
Good Cyber Hygiene	Ciberhigiene correcta
Intermediate Cyber Hygiene	Ciberhigiene intermedia
Basic Cyber Hygiene	Ciberhigiene básica
Level 5	Nivel 5
Level 4	Nivel 4
Level 3	Nivel 3
Level 2	Nivel 2
Level 1	Nivel 1

- **Nivel 1**
  - **Procesos – realizados**: dado que posiblemente la organización sólo pueda realizar estas prácticas con carácter ad hoc y podría basarse o no en la documentación. La madurez de los procesos no se evalúa para el Nivel 1;
  - **Prácticas – ciberhigiene básica:** el nivel 1 se centra en la protección de la ICF (información de contratos federales) que consiste únicamente en prácticas que se corresponden con los requisitos básicos de salvaguardia;
- **Nivel 2**
  - **Procesos – documentados:** el nivel 2 requiere que una organización establezca y documente prácticas y políticas que guíen la implementación de sus esfuerzos de CMMC. La documentación de las prácticas permite a los individuos realizarlas de modo repetible. Las organizaciones desarrollan capacidades maduras al documentar sus procesos y luego practicarlos tal como están documentados;:
  - **Práctica – ciberhigiene intermedia:**el nivel 2 sirve como una transición del nivel 1 al nivel 3 y consiste en un subconjunto de los requisitos de seguridad especificados en la NIST SP 800-171 así como las prácticas de otras normas y referencias;
- **Nivel 3**
  - **Procesos – gestionados:** el nivel 3 requiere que una organización establezca, mantenga y dote de recursos un plan que demuestre la gestión de las actividades

para que implemente la práctica. El plan puede que incluya información sobre las misiones, los objetivos, los planes de proyecto, los recursos, la formación necesaria y la participación de los interesados relevantes;
    - **Prácticas – correcta ciberhigiene:** el nivel 3 se centra en la protección de INC y abarca todos los requisitos de seguridad especificados en la NIST SP 800-171, así como las prácticas añadidas de otras normas y referencias que mitiguen las amenazas;
- **Nivel 4**
    - **Procesos – revisados**: El nivel 4 requiere que una organización examine y mida las prácticas de eficacia. Además de medir las prácticas de eficacia, las organizaciones de este nivel pueden adoptar medidas correctivas cuando sea necesario e informar a los directivos de nivel superior sobre la situación o los problemas de manera recurrente;
    - **Prácticas – proactivas:** el nivel 4 se centra en la protección de la INC (información no clasificada controlada) y abarca un subconjunto de los requisitos de seguridad reforzada. Estas prácticas mejoran las capacidades de detección y respuesta de una organización para que aborde y se adapte a las tácticas, técnicas y procedimientos que cambian;
- **Nivel 5**
    - **Procesos – optimización:** el nivel 5 requiere que una organización estandarice y optimice la implementación de procesos en toda la organización; y
    - **Prácticas – avanzadas/ proactivas:** el nivel 5 se centra en la protección del CUI. Las prácticas añadidas aumentan la profundidad y la sofisticación de las capacidades de ciberseguridad.

Método de evaluación

El CMMC es un modelo relativamente joven, terminado en el primer trimestre de 2020. Hasta ahora, ninguna organización lo ha usado. Sin embargo, los contratistas del DdD esperan contactar con examinadores externos titulados de terceros para que realicen auditorías. El DdD espera que sus contratistas implementen las buenas prácticas que fomenten la ciberseguridad y la protección de la información sensible.

A.6 Modelo de madurez de la ciberseguridad comunitaria (CCSMM)

El Modelo de Madurez de la Ciberseguridad Comunitaria (MMCSC) ha sido desarrollado por el Centro de Garantía de la Infraestructura y Seguridad de la Universidad de Texas. El objetivo del MMCSC es definir mejor los métodos que determinen la situación actual de una comunidad en su ciberpreparación y proporcionar una hoja de ruta para que las comunidades sigan con sus esfuerzos de preparación. Las comunidades a las que se dirige el MMCSC son principalmente gobiernos locales o estatales. El CCSMM se diseñó en 2007.

Características/Dimensiones

Los niveles de madurez se definen siguiendo **6 dimensiones** principales que cubren los diferentes aspectos de la ciberseguridad dentro de las comunidades y organizaciones. Estas dimensiones se definen claramente en cada nivel de madurez (detallado en el Figura 11: Resumen de las **dimensiones** del MMCSC). Las 6 dimensiones son:

i Amenazas tratadas;
ii Mediciones;
iii Intercambio de información;
iv Tecnología
v Formación; y
vi Testeo.

Niveles de madurez

El MMCSC depende de **5 niveles de madurez** basados en los principales tipos de amenazas y actividades que se tratan en el nivel:

- **Nivel 1: Consciencia de la seguridad**

  El tema principal de las actividades a este nivel es concienciar a personas y organizaciones de las amenazas, los problemas y las cuestiones relacionadas con la ciberseguridad;

- **Nivel 2: Desarrollo del proceso**

  Nivel diseñado para ayudar a las comunidades a que establezcan y mejoren los procesos de seguridad necesarios para abordar con eficacia los problemas de ciberseguridad;

- **Nivel 3: Información habilitada**

  Diseñado para mejorar los mecanismos de intercambio de información dentro de la comunidad, que permita a la misma establecer con eficacia analogías entre informaciones aparentemente dispares.

- **Nivel 4: Desarrollo de Tácticas**

  Los elementos de este nivel están diseñados para desarrollar métodos mejores y más proactivos que detecten y respondan a los ataques. En este nivel, la mayoría de los métodos de prevención debieran estar en funcionamiento.

- **Nivel 5: Capacidad operativa de seguridad completa**

  Este nivel representa aquellos elementos que debieran estar en vigor para que cualquier organización se considere plenamente preparada desde el punto de vista operativo para hacer frente a cualquier tipo de ciberamenaza.

Figura 11: Resumen de las dimensiones del MMCSC por nivel

	Level 1 Security Aware	**Level 2** Process Development	**Level 3** Information Enabled	**Level 4** Tactics Development	**Level 5** Full Security Operational Capability
Threats Addressed	Unstructured	Unstructured	Structured	Structured	Highly Structured
Metrics	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens
Information Sharing	Information Sharing Committee	Community Security Web Site	Information Correlation Center	State/Fed Correlation	Complete Info Vision
Technology	Rosters, GETS, Access Controls, Encryption	Secure Web Site Firewalls, Backups	Event Correlation SW IDS/IPS	24/7 manned operations	Automated Operations
Training	1-day Community Seminar	Conducting a CCSE	Vulnerability Assessments	Operational Security	Multi-Discipline Red Teaming
Test	Dark Screen - EOC	Community Dark Screen	Operational Dark Screen	Limited Black Demon	Black Demon

Level 1
Security Aware
Level 2
Process Development

Nivel 1. Consciencia de la seguridad

Nivel 2. Desarrollo del proceso

Level 3 Information Enabled	Nivel 3. Información habilitada
Level 4 Tactics Development	Nivel 4. Desarrollo de tácticas
Level 5 Full Security Operational Capability	Nivel 5. Capacidad operativa de seguridad completa
Threats Addressed	Amenazas tratadas
Metrics	Mediciones
Information sharing	Intercambio de información
Technology	Tecnología
Training	Formación
Test	Testeo
Unstructured	Desestructurado
Governement	Gobierno
Industry	Industria
Citizens	Ciudadanos
Information Sharing Committee	Comité de intercambio de información
Rosters, GETS, Assess Controls, Encryption	Listas, GETS, controles de evaluación, encriptación
1-dat Community Seminar	Seminario comunitario de 1 día de duración
Dark Screen – EOC	*Dark Screen – EOC*
Unstructured	Desestructurado
Governement	Gobierno
Industry	Industria
Citizens	Ciudadanos
Community Security Web site	Sitio web *Community Security*
Secure Web Site Firewalls, Backups	Cortafuegos para sitios web seguros, copias de seguridad
Conudcting a CCSE	Conectar un CCSE
Community Dark Screen	Pantalla oscura comunitaria
Structured	Estructurado
Governement Industry Citizens	Gobierno, Industria, Ciudadanos
Information Correlation Center	Centro de Correlación de Información
Event Correlation SW IDS/IPS	Acontecimiento de correlación SW, JDS/JPS
Vulnerability Assessment	Evaluación de la vulnerabilidad
Operational Dark Screen	Pantalla oscura operativa
Structured	Estructurado
Governement	Gobierno
Industry	Industria
Citizens	Ciudadanos
State/Fed Correlation	Correlación estatal/federal
24/7 manned operations	Operaciones con personal 24 horas al día
Operational Security	Seguridad operativa
Limited Black Demon	*Black demon* limitado
Highly Structured	Altamente estructurada
Complete Info	Infovisió
Vision	completa
Automated	Operaciones
Operations	automatizadas
Multi-Discipline	Red
Red	Teaming
Teaming	multidiciplinar
Black Demon	Black Demon

Método de evaluación

El MMCSC como metodología de evaluación está destinado a que las comunidades lo usen con la aportación de las agencias estatales y federales de vigilancia de la ley. Su objetivo es ayudar a que la comunidad defina qué es lo más importante, cuáles son los objetivos más probables y qué es necesario proteger (y en qué medida). Teniendo en cuenta estos objetivos, pueden elaborarse planes que lleven cada aspecto de la comunidad a su nivel necesario de madurez en ciberseguridad. La inteligencia específica que el MMCSC genera ayuda a que se definan los objetivos de varios ejercicios y testeos y que pueden usarse al medir la eficacia de los programas establecidos.

A.7 Modelo de madurez de seguridad de la Información para el marco de ciberseguridad del INNT (MMSI)

El Modelo de Madurez de la Seguridad de la Información (MMSI) se ha desarrollado en la Facultad de Ciencias Informáticas e Ingeniería de la Universidad Rey Fahd del Petróleo y los Minerales de Arabia Saudita. En él se propone un nuevo modelo de madurez de la capacidad

para medir la aplicación de las medidas de ciberseguridad. El objetivo del MMSI es permitir a las organizaciones que midan el progreso de su implementación a lo largo del tiempo al usar de forma habitual la misma herramienta de medición que garantice que se mantiene la posición de seguridad esperada. El ISMM se desarrolló en 2017.

Características/Dimensiones

EL MMSI se basa en las actuales áreas de evaluación del marco del INNT y añade una dimensión sobre la evaluación del cumplimiento. Esto lleva el modelo hacia **23 áreas de evaluación** que cubren la posición de seguridad de una organización. Las 23 áreas que se evalúan son:

i Gestión de activos;
ii Entorno empresarial
iii Gobernabilidad;
iv Evaluación de riesgos;
v Estrategia de gestión de riesgos;
vi Evaluación del cumplimiento;
vii Control de acceso;
viii Sensibilización y formación;
ix Seguridad de los datos;
x Procesos de protección de la información y procedimientos;
xi Mantenimiento;
xii Tecnología de protección;
xiii Anomalías y acontecimientos;
xiv Monitoreo continuo de la seguridad;
xv Procesos de detección;
xvi Planificación de la respuesta;
xvii Comunicaciones de respuesta;
xviii Análisis de respuesta;
xix Mitigación de respuesta;
xx Mejoras de respuesta;
xxi Planificación de recuperación;
xxii Mejoras en la recuperación; y
xxiii Comunicaciones de recuperación.

Niveles de madurez

El MMSI se basa en **5 niveles de madurez**, que, lamentablemente, no se detallan en la documentación disponible.

- **Nivel 1:** Proceso realizado;
- **Nivel 2:** Proceso gestionado;
- **Nivel 3:** Proceso establecido;
- **Nivel 4:** Proceso predecible; y
- **Nivel 5:** Proceso optimizado;

Método de evaluación

El MMSI no propone ninguna metodología específica que lleve a cabo la evaluación para las organizaciones.

A.8 Modelo de capacidad de auditoría interna (MC-AI) para el sector público

El Modelo de Capacidad de Auditoría Interna (MC-AI) se elaboró por la Fundación de Investigación del Instituto de Auditores Internos con la intención de fomentar la capacidad y la promoción mediante la autoevaluación en el sector público. Dirigido a los profesionales de la auditoría, el MC-AI ofrece una visión general del propio modelo junto con una guía de aplicación que ayude a usar el modelo como herramienta de autoevaluación.

A pesar de que el MC-AI se centra en la capacidad de auditoría interna más que en la creación de capacidad en ciberseguridad, el modelo se construye como un instrumento de autoevaluación de la madurez de las entidades del sector público que puede aplicarse a nivel mundial para mejorar los procesos y la eficacia. Como el ámbito no se centra en la ciberseguridad no se analizarán sus características. El IA-CM se concluyó en 2009.

Niveles de madurez

El Modelo de Capacidad de Auditoría Interna (MC-AI) incluye **5 niveles de madurez**, cada uno de los cuales describe las características y capacidades de una actividad de auditoría interna a ese nivel. Los niveles de capacidad del modelo proporcionan una hoja de ruta para una mejora continua.

- **Nivel 1: Inicial**

  Sin capacidades sostenibles y repetibles, que dependan de los esfuerzos individuales
  - Ad hoc o desestructurado.
  - Auditorías únicas aisladas o revisiones de documentos y transacciones para comprobar su exactitud y cumplimiento.
  - Los resultados dependen de la capacidad de la persona concreta en el puesto.
  - No se han establecido prácticas profesionales distintas de las proporcionadas por las asociaciones profesionales.
  - Aprobación de la financiación por parte de la administración, según sea necesario.
  - Ausencia de infraestructura.
  - Los auditores puede que formen parte de una unidad organizativa mayor.
  - No se desarrolla la capacidad institucional.

- **Nivel 2: Infraestructura**

  Prácticas y procedimientos sostenibles y repetibles
  - La pregunta clave o el reto para el Nivel 2 es cómo establecer y mantener la repetibilidad de los procesos y, por tanto, una capacidad de repetición.
  - Se establecen relaciones de notificación de auditoría interna, infraestructuras de gestión y administrativas y prácticas profesionales y procesos (asesoramiento de auditoría interna, procesos y procedimientos).
  - La planificación de la auditoría se basa principalmente en las prioridades de la dirección.
  - Dependencia permanente basada esencialmente en las aptitudes y competencias de personas concretas.
  - Cumplimiento parcial de las normas.

- **Nivel 3: Integrado**

  Prácticas profesionales y de gestión y que se aplican de manera homogénea.
  - Las políticas de auditoría interna, los procesos y los procedimientos se definen, documentan e integran entre sí y con la infraestructura de la organización.
  - La gestión de la auditoría interna y las prácticas profesionales están bien establecidas y se aplican de manera homogénea en toda la actividad de auditoría interna.
  - La auditoría interna está empezando a adaptarse a las actividades de la organización y a los riesgos a los que ésta se enfrenta.

- La auditoría interna evoluciona desde la dirección de la auditoría interna tradicional a la integración como colaborador y la prestación de asesoramiento sobre el rendimiento y la gestión de riesgos.
- Se centra en la creación de equipos y la capacidad de la actividad de auditoría interna y su independencia y objetividad.
- En general, se ajusta a las normas.

▶ **Nivel 4: Gestionado**

Integra la información de toda la organización para que mejore la gobernabilidad y la gestión de los riesgos.

- La auditoría interna y las expectativas de los interesados están en consonancia.
- Se han establecido medidas de rendimiento que cuantifiquen y supervisen los procesos y resultados de la auditoría interna.
- Se reconoce que la auditoría interna aporta contribuciones importantes a la organización.
- La auditoría interna funciona como parte integrante de la gobernabilidad y la gestión de riesgos de la organización.
- La auditoría interna es una unidad de negocio bien gestionada.
- Los riesgos se miden y gestionan cuantitativamente.
- Se dispone de las aptitudes y competencias necesarias con capacidad de renovación e intercambio de conocimientos (dentro de la auditoría interna y en toda la organización).

▶ **Nivel 5: Optimización**

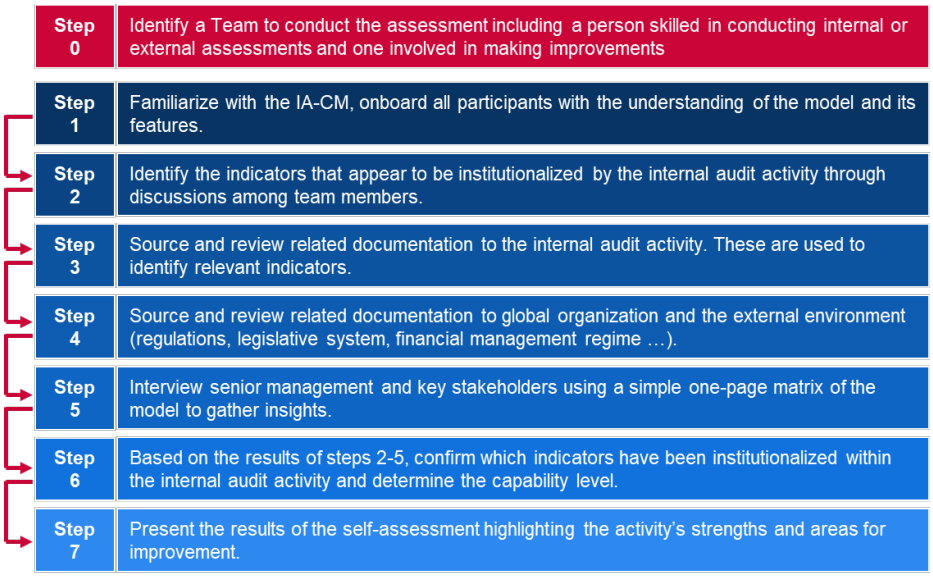
Aprender de dentro y fuera de la organización para obtener una mejora continua.

- La auditoría interna es una institución de aprendizaje con continuos procesos de mejora e innovación.
- La auditoría interna utiliza información de dentro y fuera de la organización para contribuir al logro de los objetivos estratégicos.
- Desempeño de categoría mundial / recomendado/ de buenas prácticas.
- La auditoría interna es una parte crítica de la estructura de gobierno de la organización.
- Competencias profesionales y especializadas de alto nivel.
- Las medidas de desempeño individual, unitario y de la organización están plenamente integradas para
- mejorar el rendimiento de la unidad.

Método de evaluación

El Modelo de Capacidad de Auditoría Interna se construye claramente para la autoevaluación. Proporciona los pasos detallados que hay que seguir para usar el MC-AI y un paquete de diapositivas de muestra para personalizar. Antes de iniciar la autoevaluación, se debe identificar un equipo específico que incluya, como mínimo, una persona con formación para realizar evaluaciones internas o externas de las auditorías internas y una persona que participe en la realización de mejoras en este área.

Figura 12: Pasos para la evaluación del MC-AI



Step 0	Paso 0
Step 1	Paso 1
Step 2	Paso 2
Step 3	Paso 3
Step 4	Paso 4
Step 5	Paso 5
Step 6	Paso 6
Step 7	Paso 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Identificar un equipo que lleve a cabo la evaluación, que incluya a un experto en la realización de evaluaciones internas o externas y a otra implicada en la realización de mejoras.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Familiarizarse con el MC-AI, invitar a que todos los participantes entiendan el modelo y sus características.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Identificar a través del debate entre los miembros del equipo a los indicadores que parecen institucionalizarse en la auditoría interna .
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Buscar y revisar la documentación relacionada con la actividad de auditoría interna. Estos se utilizan para identificar los indicadores relevantes.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Buscar y revisar la documentación relacionada con la institución general y el entorno externo (normativas, sistema legislativo, régimen de gestión financiera...).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Entrevistar a la gerencia y a las principales partes interesadas utilizando una sencilla matriz de una página del modelo para recabar la información.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Basándose en los resultados de los pasos 2-5, confirmar qué indicadores se han institucionalizado en la actividad de auditoría interna y determinar el nivel de capacidad.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Presentar los resultados de la autoevaluación destacando los puntos fuertes de la actividad y las áreas de mejora.

A.9 Índice de Ciberseguridad Mundial (ICM)

El índice de ciberseguridad mundial (ICM) es una iniciativa de la Unión Internacional de Telecomunicaciones (UIT) que tiene como finalidad examinar el compromiso y la situación en materia de ciberseguridad en todas las regiones de la UIT: África, América, Países árabes, Asia-pacífico, Países de la CEI y Europa, y pone de relieve a los países con un alto grado de compromiso y prácticas recomendables. El objetivo de la Iniciativa Mundial sobre la Ciberdelincuencia es ayudar a los países a que identifiquen las áreas de mejora en ciberseguridad, así como motivarles a que adopten las medidas de mejora en su clasificación, contribuyendo así a elevar el nivel general de la ciberseguridad en todo el mundo.

Dado que el IMC es un índice y no un modelo de madurez, no utiliza niveles de madurez sino más bien una puntuación para clasificar y comparar el compromiso de las naciones y regiones en ciberseguridad a nivel mundial.

Características/Dimensiones

El índice de ciberseguridad mundial (ICM) se basa en los cinco pilares de la Agenda de Ciberseguridad Mundial (ACM). Estos pilares forman los cinco subíndices del ICS y cada uno de ellos incluye un conjunto de indicadores. Los cinco pilares e indicadores son los siguientes:

i **Jurídico:** medidas basadas en la existencia de instituciones y marcos jurídicos que se ocupan de la ciberseguridad y de la ciberdelincuencia.
- Legislación sobre el ciberdelincuencia;
- Normativa de la ciberseguridad;
- Contener/reducir la legislación sobre el correo basura.

ii **Técnico:** Medidas basadas en la existencia de instituciones y marcos técnicos que se ocupan de la ciberseguridad.
- CERT/CIRT/CSRIT;
- Marco de implementación de normas;
- Órgano de normalización;
- Mecanismos y capacidades técnicas que se usan para hacer frente al correo basura;
- Utilización de la nube para usos relativos a la ciberseguridad; y
- Mecanismos en línea para la protección de la infancia.

iii **Organizativo:** Medidas basadas en la existencia de instituciones de coordinación de políticas y estrategias para el desarrollo de la ciberseguridad a nivel nacional.
- Estrategia nacional de ciberseguridad;
- Organismo responsable; y
- Ciberseguridad.

iv **Creación de capacidad:** Medidas basadas en la existencia de programas de investigación y desarrollo, educación y formación, profesionales titulados y organismos del sector público que fomenten la creación de capacidad.
- Campañas de concienciación públicas;
- Marco para la certificación y acreditación de los profesionales de la ciberseguridad;
- Cursos de formación profesional en ciberseguridad;
- Programas educativos o currículos académicos en ciberseguridad;
- Programas de I+D en ciberseguridad; y
- Mecanismos de incentivo.

v Cooperación: Medidas basadas en la existencia de asociaciones, marcos de cooperación y redes de intercambio de información.
- Acuerdos bilaterales;
- Acuerdos multilaterales;
- Participación en foros internacionales /asociaciones;
- Asociaciones público-privadas;
- Asociaciones interinstitucionales e intrainstitucionales; y
- Buenas prácticas

Método de evaluación

El ICM es una herramienta de autoevaluación construida desde una encuesta[30] de preguntas binarias, precodificadas y abiertas. El uso de respuestas binarias elimina la evaluación basada en opiniones y cualquier posible margen de error hacia ciertos tipos de respuestas. Las respuestas precodificadas ahorran tiempo y permiten un análisis más preciso de los datos. Además, una simple escala dicotómica permite una evaluación más rápida y compleja, ya que no requiere respuestas largas, lo que acelera y agiliza el proceso de respuesta y la evaluación posterior. El encuestado solo debiera confirmar la presencia o la ausencia de ciertas soluciones de ciberseguridad identificadas anteriormente. Un mecanismo de encuesta en línea, que se utiliza para reunir respuestas y cargar material relevante, permite que un grupo de expertos extraiga buenas prácticas y un conjunto de evaluaciones cualitativas temáticas.

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf

El proceso general del ICS se lleva a cabo de la siguiente manera:

- Se envía una carta de invitación a todos los participantes, en la que se les informa de la iniciativa y se solicita un centro de coordinación que se encargue de reunir todos los datos relevantes y de rellenar el cuestionario del ICM en línea. Durante la encuesta en línea, la UIT invita oficialmente al coordinador que se seleccione para que responda al cuestionario;
- Recopilación de datos primarios (para los países que no respondan al cuestionario):
  - La UIT elabora un proyecto inicial de respuesta al cuestionario utilizando datos de dominio público e investigación en línea;
  - El borrador de cuestionario se envía a los coordinadores para que lo examinen;
  - Los coordinadores mejoran la precisión y luego devuelven el borrador de cuestionario;
  - El borrador de cuestionario corregido se envía a cada coordinador para que le den su visto bueno; y
  - El cuestionario validado se usa para el análisis, la puntuación y la clasificación.
- Recopilación de datos primarios (para los países que respondan al cuestionario):
  - La UIT identifica las respuestas que falten, los documentos de respaldo, los enlaces, etc.;
  - El coordinador mejora la exactitud de las respuestas donde sea necesario;
  - El borrador de cuestionario corregido se envía a cada coordinador para que le den su visto bueno; y
  - El cuestionario validado se usa para el análisis, la puntuación y la clasificación.

A.10 El Índice de Ciberpoder (ICP)

El índice de ciberpoder (IPC) fue creado por el programa de investigación de la Unidad de Inteligencia de The Economist, patrocinado por Booz Allen Hamilton en 2011. El IPC es un «modelo cuantitativo y cualitativo dinámico, [...] que mide los atributos específicos del ciberentorno a través de cuatro impulsores del ciberpoder: marco jurídico y normativo; contexto económico y social; infraestructura tecnológica; y aplicación de la industria, que examina el progreso digital a través de las industrias clave»[31]. El objetivo del índice de ciberpoder es establecer una referencia en la capacidad de los países del G-20 para resistir los ciberataques y desplegar la infraestructura digital necesaria para conseguir una economía próspera y segura. El punto de referencia que proporciona el IPC se centra en 19 países del G-20 (excluida la UE). El índice proporciona entonces una clasificación de países para cada indicador.

Características/Dimensiones

El índice de ciberpoder (ICP) se basa en cuatro impulsores. Cada categoría se mide a través de múltiples indicadores que otorgan una puntuación específica a cada país. Las categorías y las columnas son las siguientes:

i **Marco jurídico y normativo**
  - Compromiso de los gobiernos con el ciberdesarrollo
  - Políticas de ciberprotección
  - Cibercensura (o falta de ella)
  - Eficacia política
  - Delitos contra la propiedad intelectual

ii **Contexto político y social:**
  - Niveles de educación
  - Habilidades técnicas
  - Apertura del comercio
  - Grado de innovación en el entorno empresarial

iii **Infraestructura tecnológica**
  - Acceso a la tecnología de la información y de las comunicaciones

[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

- Calidad de la tecnología de la información y de las comunicaciones
- Asequibilidad de la tecnología de la información y de las comunicaciones
- Gasto en tecnología de la información
- Número de servidores seguros

iv **Aplicación en la industria**

- Redes inteligentes
- e-salud
- Comercio electrónico
- Transporte inteligente
- Gobierno electrónico

Método de evaluación

El IPC es un modelo de puntuación cuantitativo y cualitativo. La evaluación se realizó por la Unidad de Inteligencia de *The Economist*, que usó indicadores cuantitativos de las fuentes estadísticas disponibles e hizo estimaciones cuando faltaban datos. Las principales fuentes utilizadas son la Unidad de Inteligencia de *The Economist;* la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO); la Unión Internacional de Telecomunicaciones (UIT); y el Banco Mundial.

A.11 El Índice de CiberPoder (ICP)

En este apartado se resumen las principales conclusiones del análisis de los modelos de madurez existentes. Cuadro 5: Resumen de los modelos de madurez analizados ofrece un resumen de las principales características de cada modelo según el modelo de Becker modificado. Tabla 6 Comparativa de los niveles de madurez las definiciones de alto nivel de los niveles de madurez de los modelos que se han analizado. Cuadro 7 proporciona un resumen de las dimensiones o atributos utilizados en cada modelo.

Cuadro 5: Resumen de los modelos de madurez analizados

Nombre del modelo	Fuente de la institución	Finalidad	Objetivo	N.º de niveles	N.º de características	Método de evaluación	Representación de los resultados
Modelo de madurez de la capacidad de ciberseguridad de las naciones(CMM)	Centro de Capacidad de Ciberseguridad Mundial Universidad de Oxford	Aumenta la escala y efectividad de la creación de la capacidad de ciberseguridad internacionalmente	Países	5	5 dimensiones principales	Colaboración con una institución local para afinar el modelo antes de aplicarlo al contexto nacional	radar de 5 apartados
Modelo de madurez de las capacidades en ciberseguridad(C2M2)	Departamento de Energía de EEUU (DdE)	Ayudar a que las instituciones evalúen y hagan mejoras en sus programas de ciberseguridad y refuercen su resiliencia operativa	Instituciones de todos los sectores, tipos y tamaños	4	10 dominios principales	Metodología de autoevaluación y conjunto de herramientas	Tarjeta de puntos con gráficos de tarta
Marco para la mejora de las infraestructuras críticas en ciberseguridad	Instituto Nacional de Estándares y Tecnología (INET)	Marco destinado a orientar las actividades de ciberseguridad y a gestionar los riesgos dentro de las instituciones.	Instituciones	N/D (4 niveles)	5 funciones básicas	Autoevaluación	-
Modelo catarí de madurez de la capacidad en ciberseguridad(Q-C2M2)	Facultad de Derecho de la Universidad de Catar	Proporcionar un modelo factible que pueda utilizarse para comparar, medir y desarrollar el marco de ciberseguridad catarí	Instituciones cataríes	5	5 dominios principales	-	-
Certificación del modelo de madurez de la ciberseguridad (CMMC)	Departamento de Defensa de EEUU (DdD)	Fomentar las mejores prácticas de ciberseguridad para salvaguardar la información	Organizaciones del sector de la Base Industrial de Defensa (BID)	5	17 dominios principales	Evaluación por parte de auditores externos	-
Modelo de madurez de la ciberseguridad comunitaria (MMCC))	Centro de Garantía y Seguridad de la Infraestructura Universidad de Texas	Determinar la situación actual de una comunidad en su ciberpreparación y proporcionar una hoja de ruta para que las comunidades la sigan en sus esfuerzos de preparación	Comunidades (gobiernos locales o estatales)	5	6 dimensiones principales	Evaluación dentro de las comunidades con la aportación del estado y las fuerzas o cuerpos de seguridad	-
Modelo de madurez de seguridad de la Información para el marco de ciberseguridad del INNT(Simposio internacional sobre la gestión de la fabricación)	Facultad de Ciencias Informáticas e Ingeniería Universidad del Petróleo y los Minerales Rey Fahd, Dhahran, Arabia Saudita	Permitir a las instituciones que midan el progreso de su implementación a lo largo del tiempo para asegurarse de que mantienen la posición de seguridad deseada	Instituciones	5	23 áreas evaluadas	-	-
Modelo de capacidad de auditoría interna (MC-AI) para el sector público	Fundación de Investigación del Instituto de Auditores Internos	Crear capacidad de auditoría interna y promoción mediante la autoevaluación en el sector público	Instituciones del sector público	5	6 elementos	Autoevaluación	-

Índice de Ciberseguridad Mundial (ICM)	Unión Internacional de Telecomunicaciones(ITU)	Examinar el compromiso y la situación de ciberseguridad y ayudar a los países a que determinen los aspectos que deben mejorarse en ese ámbito	Países	N/A	5 columnas	Autoevaluación	Tabla de clasificación
El Índice de Ciberpoder (ICP)	Unidad de Inteligencia de *The Economist* y Booz Allen Hamilton	Evaluar la capacidad de los países del G-20 para resistir a los ciberataques y usar la infraestructura digital necesaria para conseguir una economía próspera y segura.	Países del G-20	N/A	4 categorías	Proceso de análisis comparativo de la Unidad de Inteligencia de *The Economist*	Tabla de clasificación

Tabla 6 Comparativa de los niveles de madurez

Modelo	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Modelo de madurez de la capacidad de ciberseguridad de las naciones(CMM)	**Puesta en marcha** O bien no existe una madurez en ciberseguridad, o bien es de naturaleza muy embrionaria. Es posible que haya debates iniciales sobre la creación de capacidad en ciberseguridad, pero no se han tomado medidas concretas. En esta etapa no se observan pruebas.	**Formativa** Algunas características de los aspectos han comenzado a crecer y a formularse, pero pueden ser ad hoc, desorganizadas, mal definidas, o simplemente «nuevas». Sin embargo, pueden demostrarse claramente las pruebas de esta actividad.	**Establecida** Los elementos del aspecto están funcionando y en su sitio. No obstante, no se ha estudiado bien la asignación relativa de los recursos. Se han negociado pocas decisiones sobre la inversión «relativa» de los elementos varios del aspecto. Sin embargo, el aspecto es funcional y está definido.	**Estratégica** Se han tomado decisiones sobre qué partes del aspecto son importantes y cuáles son menos importantes para la organización o país concreto. La etapa estratégica muestra el hecho de que se han tomado estas decisiones condicionadas a las circunstancias del país u organización; y	**Dinámica** Existen mecanismos claros que modifiquen la estrategia en función de las circunstancias imperantes, como la tecnología del entorno de la amenaza, el conflicto mundial o un cambio significativo en un área de interés (por ejemplo, la ciberdelincuencia o la privacidad). Las organizaciones dinámicas han desarrollado métodos que cambian las estrategias a pasos agigantados. Son características de esta etapa la rápida toma de decisiones, la reasignación de recursos y la atención constante al cambio del entorno.
Modelo de madurez de las capacidades en ciberseguridad(C2M2)	**NIM0** No se realizan prácticas.	**NIM1** Las prácticas iniciales se realizan, pero puede que sean ad hoc.	**NIM2** Características de la gestión: Las prácticas se documentan; Se proporcionan recursos adecuados para respaldar el proceso; El personal que realiza las prácticas tiene las aptitudes y los conocimientos adecuados; y Se asignan la responsabilidad y la autoridad para llevar a cabo las prácticas. Característica de aproximación: Las prácticas son más completas o avanzadas que en la NIM1.	**NIM3** Características de la gestión: Las actividades se guían a través de políticas (u otras directivas organizativas); Se establecen y se supervisan objetivos de rendimiento para las actividades del dominio a fin de hacer un seguimiento de los logros; y Las prácticas documentadas para las actividades de dominio se normalizan y mejoran en toda la empresa. Característica de aproximación:	-

				Las prácticas son más completas o avanzadas que en la NIM2.	
Modelo de madurez de seguridad de la Información para el marco de ciberseguridad del INNT (MMSI)	**Proceso realizado**	**Proceso gestionado**	**Proceso establecido**	**Proceso predecible**	**Proceso optimizado**
Modelo catarí de madurez de la capacidad en ciberseguridad(Q-C2M2)	**Inicial** Emplea prácticas ad hoc de ciberseguridad y procesos bajo algunos de los dominios.	**En desarrollo** Implementar políticas y prácticas que desarrollen y mejoren las actividades de ciberseguridad bajo los dominios con el fin de sugerir nuevas actividades que implementar.	**Implementado** Se adoptan políticas que implementan todas las actividades de ciberseguridad previstas en cada dominio con el fin de completar la implementación en un momento determinado.	**Adaptativo** Vuelve y revisa las actividades de ciberseguridad y adopta las prácticas basadas en los indicadores predictivos que se derivan de experiencias previas y mediciones.	**Ágil** Continúa practicando la etapa de adaptación, con un énfasis añadido en la agilidad y en la velocidad cuando implementa actividades en los dominios.
Certificación del modelo de madurez de la ciberseguridad (CMMC)	**Procesos Realizado** Dado que la organización sólo puede llevar a cabo estas prácticas con carácter ad hoc y puede o no confiar en la documentación, no se evalúa la madurez del proceso para el Nivel 1. **Prácticas: Ciberhigiene básica** El nivel 1 se centra en la protección de la ICF (Información de Contratos Federales) y consiste únicamente en prácticas que corresponden a los requisitos básicos de salvaguardia.	**Procesos: Documentado** el nivel 2 requiere que una organización establezca y documente prácticas y políticas que guíen la implementación de sus esfuerzos de CMMC. La documentación de las prácticas permite a los particulares repetirlas. Las organizaciones desarrollan capacidades maduras al documentar sus procesos y luego practicarlos tal como están documentados. **Prácticas: Ciberhigiene intermedia** El nivel 2 sirve como una transición entre el nivel 1 y el nivel 3 y consiste en un subconjunto de los requisitos de seguridad especificados en la NIST SP 800-171, así como las prácticas de otras normas y referencias.	**Procesos: Gestionado** el nivel 3 requiere que una organización establezca, mantenga y dote de recursos un plan que demuestre la gestión de las actividades para que implemente la práctica. El plan podrá incluir información sobre las misiones, los objetivos, los planes de proyecto, los recursos, la formación necesaria y la participación de los interesados relevantes. **Prácticas: Ciberhigiene correcta** El nivel 3 se centra en la protección de la información no clasificada controlada (CUI) y abarca todos los requisitos de seguridad especificados en la NIST SP 800-171, así como las prácticas adicionales de otras normas y referencias para mitigar las amenazas.	**Procesos: Revisado.** El nivel 4 requiere que una organización examine y mida las prácticas y su eficacia. Además de medir las prácticas y su eficacia, las organizaciones de este nivel pueden adoptar medidas correctivas cuando sea necesario e informar a los directivos de nivel superior sobre la situación o los problemas con carácter recurrente. **Prácticas: Proactivo** El nivel 4 se centra en la protección de la información no clasificada controlada y abarca un subconjunto de los requisitos de seguridad reforzada. Estas prácticas mejoran las capacidades de detección y respuesta de una organización para que aborde y se adapte a las tácticas, técnicas y procedimientos que cambian.	**Procesos: Optimizado** El nivel 5 requiere que una organización estandarice y optimice la implementación del proceso en toda la organización. **Prácticas: Avanzado/Proactivo** El nivel 5 se centra en la protección de la información no clasificada controlada (INC). Las prácticas añadidas aumentan la profundidad y la sofisticación de las capacidades de ciberseguridad.
Modelo de madurez de la ciberseguridad comunitaria (CCSMM)	**Consciencia de la seguridad** El tema principal de las actividades a este nivel es hacer que las personas y las organizaciones sean conscientes de las amenazas, los problemas	**Desarrollo del proceso** Nivel diseñado para ayudar a las comunidades a que establezcan y mejoren los procesos de seguridad necesarios para abordar con eficacia los problemas de ciberseguridad.	**Información habilitada** Diseñado para mejorar los mecanismos de intercambio de información dentro de la comunidad para permitir a la misma que establezca correlaciones eficaces con las	**Desarrollo de Tácticas** Los elementos de este nivel están diseñados para desarrollar métodos mejores y más proactivos que detecten y respondan a los ataques. Para este nivel la mayoría de los	**Capacidad operativa de seguridad completa** Este nivel representa los elementos que deberían estar en vigor para que cualquier organización se considere plenamente preparada desde el

	y las cuestiones relacionadas con la ciberseguridad		informaciones aparentemente dispares.	métodos de prevención deberían estar en funcionamiento.	punto de vista operativo para que haga frente a cualquier tipo de ciberamenaza.
Modelo de capacidad de auditoría interna (MC-AI) para el sector público	**Inicial** No hay capacidades sostenibles y repetibles - depende de los esfuerzos individuales	**Infraestructura** Prácticas y procedimientos sostenibles y repetibles	**Integrado** Prácticas de gestión y profesionales aplicadas de modo homogéneo	**Gestionado** Integra la información de toda la organización para mejorar la gobernanza y la gestión de los riesgos	**Optimizado** Aprender de dentro y fuera de la organización para mejorar continuamente

Cuadro 7: Comparativa de características/dimensiones

	Modelo de madurez de la capacidad de ciberseguridad de las naciones(CMM)	Modelo de madurez de las capacidades en ciberseguridad(C2M2)	Modelo catarí de madurez de la capacidad en ciberseguridad(Q-C2M2)	Certificación del modelo de madurez de la ciberseguridad (CMMC)	Certificación del modelo de madurez de la ciberseguridad (CMMC)	Modelo de madurez de seguridad de la Información para el marco de ciberseguridad del INNT (MMSI)	Marco para la mejora de las infraestructuras críticas en ciberseguridad	Índice de Ciberseguridad Mundial (ICM)	El Índice de Ciberpoder (ICP)
Niveles	Cinco dimensiones divididas en varios factores, incluidos múltiples aspectos e indicadores (Figura 4)	Diez dominios, incluyendo una gestión única Objetivo y diversos objetivos del enfoque (Figura 6)	Cinco dominios divididos en subdominios	Diecisiete dominios detallados en procesos y de una a muchas capacidades, que luego se detallan en Prácticas (Figura9).	Seis dimensiones principales	Veintitrés áreas evaluadas	Cinco funciones con categorías y subcategorías claves subyacentes (Figura 8).	Cinco columnas que incluyen varios indicadores	Cuatro categorías con varios indicadores
Características/Dimensiones	i Diseñar la política y la estrategia de ciberseguridad; ii Fomentar una cultura de la ciberseguridad responsable dentro de la sociedad; iii Desarrollar el conocimiento de la ciberseguridad; iv Creación de marcos jurídicos y normativos eficaces; y v Controlar los riesgos a través de normas, organizaciones y tecnologías.	i Gestión de riesgos; ii Gestión de activos, cambios y configuración; iii Gestión de la identidad y el acceso; iv Gestión de amenazas y vulnerabilidad; v Consciencia situacional vi Respuesta a acontecimientos e incidentes; vii Gestión de la cadena de suministro y de las dependencias externas; viii Gestión de la plantilla; ix Arquitectura de la ciberseguridad; x Gestión de programas de ciberseguridad.	i (Cibergobernabilidad, activos, riesgos y formación); ii Asegurar (seguridad de datos, seguridad de la tecnología, seguridad del control de acceso, seguridad de las comunicaciones y seguridad del personal); iii Exponer (monitoreo, gestión de incidentes, detección, análisis y exposición); iv Responder (planificación de la respuesta, mitigación y comunicación de la respuesta); v Mantener (planificación de la recuperación, gestión de la continuidad, mejora y dependencias externas).	i Control de acceso; ii Gestión de activos; iii Auditoría y responsabilidad financiera iv Concienciación y formación; v Gestión de la configuración; vi Identificación y autenticación; vii Respuesta a incidentes viii Mantenimiento; ix Protección de los medios; x Seguridad del personal; xi Protección física; xii Recuperación xiii Gestión de riesgos; xiv Evaluación de la protección; xv Consciencia situacional; xvi Protección de sistemas y comunicaciones; xvii Integridad de los sistemas y la información.	i Amenazas tratadas; ii Mediciones; iii Intercambio de información; iv Tecnología v Formación; vi Testeo.	i Gestión de activos; ii Entorno empresarial iii Gobernabilidad; iv Evaluación de riesgos; v Estrategia de gestión de riesgos; vi Evaluación del cumplimiento; vii Control de acceso; viii Concienciación y formación; ix Seguridad de los datos; x Procesos de protección de la información y procedimientos; xi Mantenimiento; xii Tecnología orientada a la protección; xiii Anomalías y acontecimientos; xiv Monitoreo continuo de la seguridad; xv Procesos de detección; xvi Planificación de la respuesta; xvii Comunicaciones de respuesta; xviii Análisis de respuesta; xix Mitigación de respuesta; xx Mejoras de respuesta; xxi Planificación de recuperación; xxii Mejoras de recuperación	i Identificar; ii Proteger; iii Detectar; iv Responder; v Recuperar;	i Jurídico; ii Técnico; iii Organizativo; iv Creación de capacidad; v Cooperación.	i Marco jurídico y reglamentario: ii Contexto político y social; iii Infraestructura tecnológica; iv Aplicación industrial.

						xxiii	Comunicaciones de recuperación.		

ANEXO B – BIBLIOGRAFÍA DE INVESTIGACIÓN DOCUMENTAL

Almuhammadi, S. y Alsaleh, M., (2017), «*Information Security Maturity Model for Nist Cyber Security Framework,* (modelo de madurez de seguridad de la información para el marco de ciberseguridad del INNT)», en la publicación Ciencia informática y Tecnología de la información (CI & TI). (Sexta Conferencia Internacional sobre la Convergencia de la Tecnología de la Información y los Servicios, Centro de Colaboración para la Investigación de la académica e industrial), (AIRCC).

Almuhammadi, S. y Alsaleh, M., (2017), «*Information Security Maturity Model for Nist Cyber Security Framework,* (modelo de madurez de seguridad de la información para el marco de ciberseguridad del INNT)», en la publicación Ciencia informática y Tecnología de la información (CI & TI). Disponible en: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. y otros. *Stocktaking, analysis and recommendations on the protection of CIIs* , (2016), (Inventario, análisis y recomendaciones sobre la protección de las IIC. Disponible en: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. y otros. *Developing Maturity Models for IT Management – A Procedure Model and its Application,* (2009), (Desarrollo de modelos de madurez para la gestión de las tecnologías de la información: un modelo de procedimiento y su aplicación). Disponible en: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Gobierno de Bélgica (2012), estrategia en ciberseguridad. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. y otros. *Developing Cibersecurity Capacity:* (Desarrollo de la capacidad de ciberseguridad), (2018): *A proof-of-concept implementation guide,* (guía de implementación de la prueba de concepto). *RAND Corporation.* Disponible en: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. ,(2012), «*Introduction to Return on Security Investment,* (introducción al retorno de la inversión en seguridad)».

Instituto de Ingeniería de Software de la Universidad *Carnegie Mellon Pittsburgh* Estados Unidos, (2019) «*Cybersecurity Capability Maturity Model,* (modelo de madurez de la capacidad de ciberseguridad), (C2M2) Versión 2.0.». Disponible en https://europa.eu/european-union/sites/europaeu/files/docs/body/fiche_15_sent_to_ep_cons_2011-07-20_en.pdf

Centro de Estudios de Seguridad (CES), ETH *Zürich,* (2019), *National Cybersecurity Strategies in Comparison - Challenges for Switzerland,* (estrategias nacionales de ciberseguridad en retos comparativos de Suiza). Disponible en: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Consejo de Ministros (2019) Diario Oficial Portugués, Serie 1 - Nº 108 - Resolución del Consejo de Ministros Nº 92/2019. Disponible en: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016), *Cybersecurity Capacity Maturity Model for Nations* (CMM), (modelo de madurez de la capacidad de ciberseguridad de las naciones) (MMC), Universidad de Oxford.

Herramienta de autoevaluación de madurez CSIRT (sin fecha). Disponible en: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Proyecto *CyberCrime*@IPA del Consejo de Europa y la Unión Europea, proyecto mundial sobre Ciberdelincuencia del Grupo de Tareas sobre Ciberdelincuencia del Consejo de Europa y la Unión Europea (2011), Unidades especializadas en ciberdelincuencia - Estudio de buenas prácticas. Disponible en: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Sistema de análisis e informe de incidentes de ciberseguridad - Herramienta de análisis visual (sin fecha). Disponible en: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017), *Public Private Partnerships* (PPP), (asociaciones publico-privadas) (APP),

Darra, E. (sin fecha), *«Welcome to the NCSS Training Too*l, (bienvenido a la herramienta de entrenamiento de la ENCS)».

Dekker, M. A. C. (2014), *Technical Guideline on Incident Reporting,* (guía técnica para la notificación de incidentes). Disponible en: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014), *Technical Guideline on Security Measures,* (guía técnica sobre medidas de seguridad). Disponible en: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015), *Guideline on Threats and Assets,* (guía sobre amenazas y activos). Disponible en: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Estrategia de ciberseguridad digital en Eslovenia (2016). Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. y otros. ENISA: «Privacy and data protection by design - from policy to engineering», 2014. Disponible en: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Comisión Europea (2012), Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios fiduciarios para las transacciones electrónicas en el mercado interior. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0238&from=EN

Agencia Europea de Seguridad de las Redes y de la Información,(2012), ENCS: ENISA *Practical Guide on Development and Execution*., (guía práctica de desarrollo y ejecución) Heraclión: La ENISA.

Agencia Europea de Seguridad de las Redes y de la Información, (2012), ENCS: ENISA «*Setting the course for national efforts to strengthen security in cyberspace,* (marcar el rumbo de los esfuerzos nacionales en el fortalecimiento de la seguridad en el ciberespacio)». Heraklion: ENISA.

Agencia Europea de Seguridad de las Redes y de la Información (2016), *Guidelines for SMEs on the security of personal data processing,* (directrices para las PYME sobre la seguridad del tratamiento de datos personales).

Agencia Europea de Seguridad de las Redes y de la Información (2016), *NCSS good practice guide: designing and implementing national cyber security strategies,* (guía de buenas prácticas de la ENCS: diseño y aplicación de estrategias nacionales de ciberseguridad). Heraklion: ENISA.

Unión Europea y Agencia de Seguridad de las Redes y de la Información, (2017), *Handbook on security of personal data processing*, (manual sobre la seguridad del tratamiento de datos personales). Disponible en: http://dx.publications.europa.eu/10.2824/569768

Unión Europea y Agencia para la Seguridad de las Redes y la Información (2014), *ENISA CERT inventory inventory of CERT teams and activities in Europe,* (Inventario CERT de la ENISA de los equipos y actividades del CERT en Europa). Disponible en: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Oficina Ejecutiva del Presidente, (2015), Memorando para los Jefes de Departamentos y Organismos Ejecutivos. Disponible en: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Cancillería Federal de la República de Austria (2013) Estrategia austríaca de ciberseguridad. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Ministerio Federal del Interior (2011) Estrategia de ciberseguridad para Alemania. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Ferette, L., (2016), *NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises,* (Directiva NIS y normas nacionales de seguridad de la información y la privacidad para las PYMES: recomendaciones para mejorar la adopción de normas de seguridad de la información y la privacidad en las pequeñas y medianas empresas). Disponible en: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., Unión Europea y Agencia Europea de Seguridad de las Redes y de la Información (2015) *The 2015 report on national and international cyber security exercises: survey, analysis and recommendations,* (informe de 2015 sobre ejercicios de ciberseguridad nacionales e internacionales: encuestas, análisis y recomendaciones). Disponible en: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Oficina del Primer Ministro francés (2014), Estrategia Nacional de Seguridad Digital de Francia. Disponible en: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Galan Manso, C. y otros. *Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises*, (Normas de seguridad de la información y de privacidad para las PYME: recomendaciones para mejorar la adopción de normas de seguridad de la información y de privacidad en las pequeñas y medianas empresas), (2015). Disponible en: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Universidad de Gante y otros. *«Evaluating Business Process Maturity Models» Journal of the Association for Information Systems,* (La evaluación de modelos de madurez de los procesos de negocio), (2017). Disponible en: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Gobierno de Bulgaria (2015) Estrategia Nacional de Ciberseguridad, Bulgaria ciberresistente 2020.

Gobierno de Croacia (2015) Estrategia Nacional de ciberseguridad de la República de Croacia. Disponible en: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Gobierno de Grecia (2017) Estrategia Nacional de ciberseguridad. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Gobierno de Hungría, (2018), Estrategia para la seguridad de las redes y los sistemas de información. Disponible en: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Gobierno de Irlanda, (2019), Estrategia Nacional de ciberseguridad. Disponible en: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Gobierno de España, (2019), Estrategia Nacional de ciberseguridad. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Instituto de Auditores Internos (ed.) (2009) *Internal audit capability model (IA-CM) for the public sector: overview and application guide, (*Modelo de Capacidad de Auditoría Interna para el Sector Público (MC-AI)). *Altamonte Springs,* Florida: Instituto de Auditores Internos, Fundación de Investigación.

Unión Internacional de Telecomunicaciones (UIT), (2018), *The Global Cybersecurity Index,* (índice de ciberseguridad mundial). Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Unión Internacional de Telecomunicaciones (UIT), (2018), Guía para la elaboración de una estrategia nacional de ciberseguridad. Disponible en: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B., (2019), «*Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework,* (hacia un modelo catarí de madurez de la capacidad en ciberseguridad con un marco legislativo)», International Review of Law, (revista internacional de derecho).

Gobierno de Letonia, (2014), estrategia en ciberseguridad. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. y otros. *An evaluation framework for national cyber security strategies,* (un marco de evaluación de las estrategias nacionales de ciberseguridad), (2014) Heraklion: La ENISA. Disponible en: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. y otros. *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks,* (metodologías para la identificación de bienes y servicios de infraestructura de información crítica: directrices para el trazado de redes de comunicación electrónica de datos), (2014). Disponible en: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Ministerio de Competitividad y Economía Digital, Marítima y de Servicios (2016) Estrategia de Ciberseguridad de Malta. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Ministerio de Asuntos Económicos y Comunicaciones, (2019), Estrategia de Ciberseguridad, República de Estonia. Disponible en: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministerio de Defensa Nacional República de Lituania, (2018), Estrategia Nacional de Ciberseguridad.

Centro Nacional de Ciberseguridad, (2015), Estrategia Nacional de Ciberseguridad de la República Checa. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Estrategias Nacionales de Ciberseguridad - Mapa Interactivo (sin fecha). Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

National Cybersecurity Strategies Evaluation Tool, (herramienta de evaluación de estrategias nacionales de ciberseguridad (2018). Disponible en:

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Instituto Nacional de Estándares y Tecnología, (2018), *Framework for Improving Critical Infrastructure Cybersecurity,* (marco de mejora de la infraestructura crítica de ciberseguridad), Versión 1.1. Gaithersburg, MD: Instituto Nacional de Estándares y Tecnología Disponible en: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Grupo de Gestión de Objetos, (2008), Modelo de madurez de los procesos industriales. Disponible en: https://www.omg.org/spec/BPMM/1.0/PDF

OCDE, Unión Europea y Centro Común de Investigación - Comisión Europea, (2008), *Handbook on Constructing Composite Indicators,* (manual de construcción de indicadores compuestos). *Methodology and User Guide*, (metodología y guía del usuario). OCDE. Disponible en: https://www.oecd.org/sdd/42495745.pdf.

Oficina del Comisionado de Comunicaciones Electrónicas y Reglamentos Postales (2012) Estrategia de Ciberseguridad de la República de Chipre.

Diario Oficial de la Unión Europea (2008) DIRECTIVA 2008/114/CE DEL CONSEJO, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Organización para la Cooperación y el Desarrollo Económico (OCDE) (2012) La elaboración de políticas de ciberseguridad en un momento decisivo. Disponible en: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E.,(2012), «*National Cyber Security Strategies - Practical Guide on Development and Execution*, (estrategias nacionales de ciberseguridad: guía práctica de desarrollo y ejecución)».

Ouzounis, E. ,(2012), «*Good Practice Guide on National Exercises*, (guía de buenas prácticas sobre ejercicios nacionales)».

Portesi, S. (2017), *Improving Cooperation between CSIRTs and Law Enforcement,* (mejorar la cooperación entre CSIRTs y fuerzas de seguridad): *Legal and Organisational Aspects,* (Aspectos jurídicos y organizativos)

Presidencia del Consejo de Ministros (2017), plan de acción de Italia en materia de ciberseguridad. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Rady Ministrów, (2019), Dziennik Urzędowy Rzeczypospolitej Polskiej. Disponible en: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Gobierno de Rumanía, (2013), estrategia en ciberseguridad. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. y Agencia de la Unión Europea para la Ciberseguridad ,(2019), *Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies* (buenas prácticas en innovación sobre ciberseguridad bajo la ENCS: buenas prácticas en innovación sobre ciberseguridad bajo las estrategias de ciberseguridad nacional). Disponible en: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Secretariado del Comité de Seguridad, (2019), estrategia de Ciberseguridad de Finlandia para 2019. Disponible en: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Gobierno de Eslovaquia, (2015), concepto de ciberseguridad de la República Eslovaca. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R., (2015), Directiva 2010/41/UE del Parlamento Europeo y del Consejo de 7 de julio de 2010

Smith, R, (2016), «Directiva 2010/41/UE del Parlamento Europeo y del Consejo del 7 de julio de 2010», en Smith, R., *Core EU Legislation*. Londres: *Macmillan Education.* Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Stavropoulos, V. (2017), mes de la Ciberseguridad Europea 2017.

Gobierno de Suecia, (2017), *Nationell strategi för samhällets informations- och cybersäkerhet,* (estrategia nacional de información y ciberseguridad). Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Gobierno danés, Ministerio de Finanzas, (2018) Estrategia danesa de ciberseguridad e información. Disponible en: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Consejo Federal, (2018), Estrategia nacional de protección de Suiza contra los ciberriesgos.

Consejo de Gobierno de Luxemburgo, (2018), Estrategia nacional de ciberseguridad. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Gobierno de los Países Bajos, (2018), Programa Nacional de Ciberseguridad. Disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

La Casa Blanca, (2018), Ciberestrategia Nacional de los EE.UU. de América Disponible en: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P. y otros. (2011) Informe Cyber Europa. Disponible en: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. y Agencia Europea de Seguridad de las Redes y de la Información (2013), *National level risk assessments: an analysis report,* (evaluación del nivel de riesgo nacional: informe del análisis). Disponible en: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R. y otros. (2015), informe sobre la cooperación y la gestión de las cibercrisis. Disponible en: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A. y otros. (2015), *Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises,* (informe sobre la cooperación y la gestión de las cibercrisis: prácticas comunes de gestión de crisis a nivel de la UE y aplicabilidad a las cibercrisis). Disponible en: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

Estrategia Nacional de Ciberseguridad del Reino Unido 2016-2021 (2016). Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Universidad de Innsbruck y otros. (2009), *Understanding Maturity Models,* (comprender los modelos de madurez).

Wamala, D. F., (2011), *ITU National Cybersecurity Strategy Guide,* (guía de estrategia de ciberseguridad nacional de la UIT). Disponible en: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. ,(2007), «*The Community Cyber Security Maturity Model» , in 2007, 40th Annual Hawaii International Conference on System Sciences* (modelo de madurez de la ciberseguridad

comunitaria en 2007: 40 Conferencia Internacional Anual de Hawái sobre las Ciencias de Sistemas, (HICSS'07),

ANEXO C - OTROS OBJETIVOS DE ESTUDIO

Los objetivos que se detallan a continuación se han estudiado en el marco de la fase de investigación documental y de las entrevistas realizadas por la ENISA. Los siguientes objetivos no forman parte del Marco Nacional de Evaluación de Capacidades, pero enfocan la atención sobre temas que merece la pena que se debatan. En cada uno de los subcapítulos siguientes se explicará por qué se destaca el objetivo.

- Desarrollar estrategias de ciberseguridad específicas para cada sector;
- Luchar contra las campañas de desinformación;
- Asegurar las tecnologías de vanguardia (5G, IA, informática cuántica...);
- Garantizar la soberanía de los datos; y
- Proporcionar incentivos para el desarrollo de la industria de los ciberseguros.

Desarrollar estrategias de ciberseguridad específicas para cada sector

La adopción de estrategias específicas para cada sector, que se centran en las intervenciones e incentivos sectoriales, presenta, sin lugar a dudas, una mayor capacidad de descentralización. Se amolda especialmente a los Estados Miembros cuyas OSE deben ocuparse de diferentes marcos y reglamentos y en los que existen muchas dependencias debido al carácter transversal de la ciberseguridad. De hecho, en varios Estados Miembros es habitual contar con docenas de autoridades nacionales y organismos reguladores conocedores de las especificidades de cada sector, que tienen la potestad para hacer cumplir la reglamentación específica de cada sector.

Dinamarca, por ejemplo, puso en marcha seis estrategias específicas que abordan las actividades de ciberseguridad y de la información de los sectores más críticos que desarrollan una capacidad descentralizada más sólida en ciberseguridad y en información. Cada «unidad sectorial» contribuirá a la evaluación de las amenazas a nivel sectorial, a la vigilancia, a los ejercicios de preparación, al establecimiento de sistemas de seguridad, al intercambio de conocimientos e instrucciones, entre otras cosas. Las estrategias sectoriales abarcan los siguientes sectores:

- Energía;
- Atención sanitaria;
- Transporte;
- Telecomunicaciones;
- Finanzas; y
- Marítimo.

Otros Estados Miembros han expresado su interés en considerar estrategias de ciberseguridad específicas para cada sector que reflejen todos los requisitos reglamentarios. Sin embargo, cabe señalar que ese objetivo podría no ser adecuado para todos los Estados Miembros, dependiendo de su tamaño, sus políticas nacionales y su madurez. La gran dificultad de garantizar que el marco pueda tener en cuenta todas las especificidades llevó a la ENISA a no incluir este objetivo en el marco.

Luchar contra las campañas de desinformación

Los Estados Miembros integran la protección de principios fundamentales como los derechos humanos, la transparencia y la confianza pública en sus estrategias nacionales de ciberseguridad. Esto es muy importante, especialmente cuando se trata de desinformación que se difunde a través de los medios de comunicación tradicionales o las plataformas de redes sociales. Además, actualmente la ciberseguridad es uno de los mayores desafíos electorales. De hecho, actividades como la difusión de información falsa o propaganda negativa se han observado en varios países en el período previo a importantes elecciones. Esta amenaza puede socavar el proceso democrático de la Unión Europea. En el plano europeo, la Comisión ha esbozado un Plan de Acción[32] para intensificar los esfuerzos por contrarrestar la desinformación en Europa: este plan se centra en cuatro áreas clave (detección, cooperación, colaboración con plataformas en línea y concienciación) y sirve para aumentar la capacidad de la UE y fortalecer la cooperación entre los Estados Miembros.

4 de los 19 países entrevistados han expresado su intención de abordar el tema de la desinformación y la propaganda en su ENCS.

Por ejemplo, la ENCS francesa[33] señala que: «es responsabilidad del Estado informar a los ciudadanos de los riesgos de las técnicas de manipulación y propaganda que utilizan los agentes malintencionados en Internet. Por ejemplo, tras los atentados terroristas contra Francia en enero de 2015, el Gobierno estableció una plataforma de información sobre los riesgos relacionados con la radicalización islámica a través de las redes de comunicación electrónica: «Stop-djihadisme.gouv.fr »». Este enfoque podría extenderse para responder a otros fenómenos de propaganda o desestabilización.

En otro ejemplo, la ENCS[34] 2019-2024 de Polonia establece que: «contra las actividades manipuladoras, como las campañas de desinformación, se necesitan acciones sistémicas para desarrollar la conciencia de los ciudadanos en el contexto de la verificación de la autenticidad de la información y la respuesta a los intentos de distorsionarla».

Sin embargo, durante las entrevistas realizadas por la ENISA, varios Estados Miembros señalaron que no abordan la cuestión como parte de su ENCS como una amenaza a la ciberseguridad, sino que la abordan a un nivel social más amplio, por ejemplo, mediante iniciativas políticas.

Tecnologías innovadoras seguras (5G, IA, informática cuántica...)

A medida que el panorama actual de las ciberamenazas siga ampliándose, el desarrollo de nuevas tecnologías dará lugar, muy probablemente, a un aumento de la intensidad y del número de los ciberataques y a la diversificación de los métodos, medios y objetivos empleados por los agentes de la amenaza. Mientras tanto, estas nuevas soluciones tecnológicas en forma de tecnologías de vanguardia tienen el potencial de convertirse en los componentes básicos del mercado digital europeo. A fin de salvaguardar la creciente dependencia digital de los Estados Miembros y la aparición de nuevas tecnologías deben establecerse incentivos y políticas de pleno derecho que apoyen el desarrollo y el despliegue seguros y fiables de esas tecnologías en la UE.

Durante la fase de investigación documental realizada sobre las ENCS de los Estados Miembros se presentaron las siguientes tecnologías de vanguardia que presentan interés para

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

los Estados Miembros: 5G, IA, informática cuántica, criptografía, edge computing, vehículos conectados y autónomos, big y smart data, cadena de bloques, robótica e IoT.

Más concretamente, a principios de 2020, la Comisión Europea publicó una comunicación en la que se pedía a los Estados Miembros que adoptaran acciones para que se aplicara el conjunto de medidas recomendadas en las conclusiones de la caja de herramientas 5G

[35]. Esta caja de herramientas 5G se produce a raíz de la Recomendación (UE) 2019/534 sobre la ciberseguridad de las redes 5G, adoptada por la Comisión en 2019, en la que se pedía un enfoque europeo unificado para la seguridad de las redes 5G[36].

Durante las entrevistas realizadas por la ENISA se destacó que este tema es más bien transversal y que se aborda en toda la ENCS, y no un objetivo específico en sí mismo.

Asegurar la soberanía de los datos

Por una parte, el ciberespacio puede considerarse como un formidable espacio mundial común, de fácil acceso, que ofrece un alto grado de conectividad y puede brindar grandes oportunidades de crecimiento socioeconómico. Por otra parte, el ciberespacio también se caracteriza por su débil jurisdicción, la dificultad de atribuir acciones, la falta de fronteras y los sistemas interconectados que pueden ser porosos y cuyos datos pueden robarse o incluso pueden ser accesibles para gobiernos extranjeros. Además de estas dos perspectivas, el ecosistema digital se caracteriza por la concentración de plataformas de servicios e infraestructuras en línea en manos de muy pocos interesados. Todos los aspectos mencionados llevan a los Estados Miembros a promover la soberanía digital. Lograr la soberanía digital significa que los ciudadanos y las empresas pueden prosperar plenamente utilizando servicios digitales y productos de las TIC dignos de confianza, sin temor alguno en cuanto a los datos personales, los activos digitales, la autonomía económica o la influencia política.

La soberanía de los datos o soberanía digital la defienden los Estados Miembros a nivel nacional y a nivel europeo. Si bien los Estados Miembros no parecen abordar la cuestión directamente en su ENCS como un objetivo específico, la abordan como un principio transversal o esbozan su intención de garantizar la soberanía digital a nivel nacional en publicaciones ad hoc centradas en las tecnologías clave. Por ejemplo, en el examen estratégico francés de la ciberdefensa de 2018 se afirma que «el control de las siguientes tecnologías es de gran importancia para garantizar la soberanía digital: encriptar las comunicaciones, detectar los ciberataques, redes de telefonía móvil profesionales, la informática en la nube y la inteligencia artificial»[37].

En el plano europeo, los Estados Miembros participan activamente en la definición de la estrategia europea de datos (COM/2020/66 final) y en la elaboración del marco de certificación de la UE para los productos, servicios y procesos digitales de las TIC establecido por la Ley de Ciberseguridad de la UE (2019/881) que garantice la autonomía digital estratégica a nivel europeo.

La fase de entrevistas con los Estados Miembros muestra que el asunto de la soberanía digital suele considerarse una cuestión más amplia que la que se limita a la ciberseguridad. Por lo tanto, los Estados Miembros no abarcan el tema en sus ENCS y, los pocos que lo hacen, no lo contemplan como un objetivo específico *per se*.

[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission
[36] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534
[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

Proporcionar incentivos para el desarrollo de la industria de los ciberseguros

La situación actual de la industria de los ciberseguros nos muestra que el mercado mundial ha crecido indiscutiblemente. Sin embargo, todavía está en sus inicios, ya que hay que recopilar datos y sentar muchos precedentes (por ejemplo, la cobertura silenciosa, los ciberriesgos sistémicos...). Además, las pérdidas estimadas resultantes de los ciberataques en todo el mundo están a varios órdenes de magnitud por encima de la capacidad de cobertura actual de la industria de los ciberseguros, (documento de trabajo del FMI - El ciberriesgo para el sector financiero: Un marco para la evaluación cuantitativa WP/18/143). Sin embargo, el desarrollo de la industria de los ciberseguros puede producir beneficios y sentar las bases de los dispositivos eficaces. De hecho, los dispositivos para los ciberseguros pueden contribuir a:

- Concienciar sobre los riesgos de la ciberseguridad en las empresas;
- Evaluar la exposición a los ciberriesgos de manera cuantitativa;
- Mejorar la gestión de los riesgos de la ciberseguridad;
- Prestar apoyo a las entidades que sean víctimas de ciberataques; y
- Cubrir los daños (materiales o no) producidos por un ciberataque.

Algunos Estados Miembros han empezado a trabajar en este asunto. Por ejemplo:

- Estonia adoptó un planteamiento para «esperar y ver» en su ENCS: «Para mitigar los ciberriesgos generales del sector privado, se analizará la oferta y la demanda en el servicio de ciberseguros de Estonia y, basándonos en esto, acordaremos principios de cooperación para los relacionados, incluyendo el intercambio de información, la preparación de la evaluación de los riesgos, etc. Hoy en día, en el mercado estonio hay pocos proveedores de servicios de ciberseguros y en primer lugar es necesario determinar quién ofrece qué. La complejidad de la protección de los seguros se considera a menudo un obstáculo para el desarrollo del mercado de los ciberseguros».
- Luxemburgo, en especial, respalda el desarrollo de la industria de los ciberseguros en su ENCS: Objetivo 1: Crear nuevos productos y servicios. Para agrupar los riesgos y animen a las víctimas de ciberincidentes digitales a que busquen la ayuda de expertos que gestionen el incidente y restauren un sistema afectado por un acto malicioso se alentará a las compañías de seguros para que creen productos específicos para el área de los ciberseguros».

Las opiniones de los entrevistados sobre este tema fueron muy diversas: algunos Estados Miembros afirmaron que el tema del ciberseguro se ha convertido en un asunto de debate reciente, mientras que otros compartieron que, aunque el tema es prometedor, la industria no está aún lo suficientemente madura. Sin embargo, un gran número de entrevistados declaró que el tema no se aborda como parte de la ENCS, ya sea porque se consideró que era demasiado específico o porque no entraba en el alcance de la ENCS.

TP-02-21-253-ES-N

Acerca de la ENISA - Agencia de la Unión Europea para la Ciberseguridad

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada por el Reglamento sobre la Ciberseguridad de la UE, la Agencia de la Unión Europea para la Ciberseguridad contribuye a la política de seguridad cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC mediante programas de certificación de la ciberseguridad, coopera con los Estados miembros y con los organismos de la UE y ayuda a Europa a prepararse para los desafíos del mañana en materia de ciberseguridad. A través del intercambio de conocimientos, la creación de capacidades y la sensibilización, la Agencia coopera con sus partes interesadas clave para fortalecer la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para para mantener la seguridad digital de la sociedad y de los ciudadanos de Europa. Para más información, visite www.enisa.europa.eu.:

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-478-7
DOI: 10.2824/895115