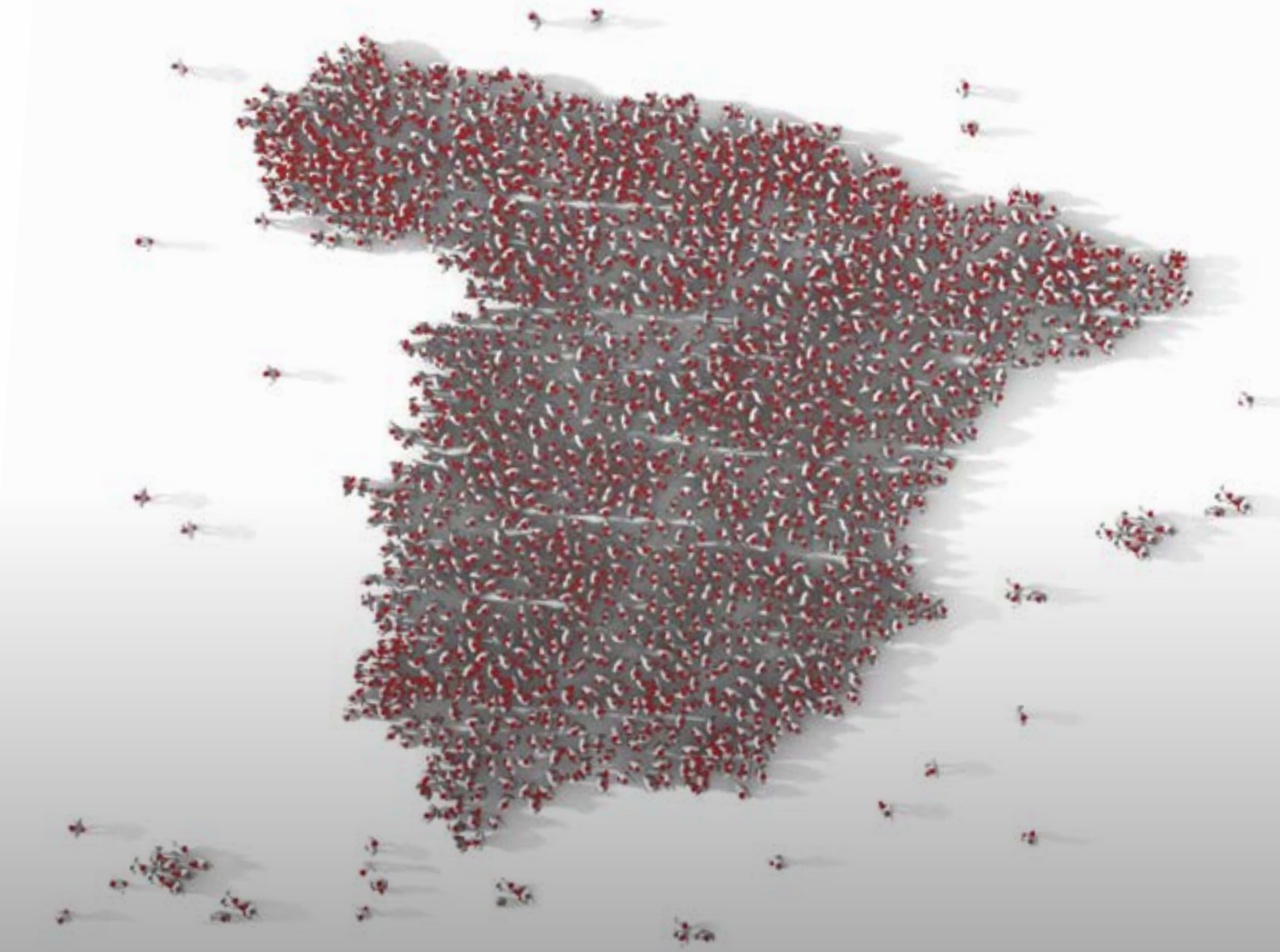
FORO NACIONAL DE CIBERSEGURIDAD

+ + +



2021

+ + +

FORO NACIONAL DE CIBERSEGURIDAD

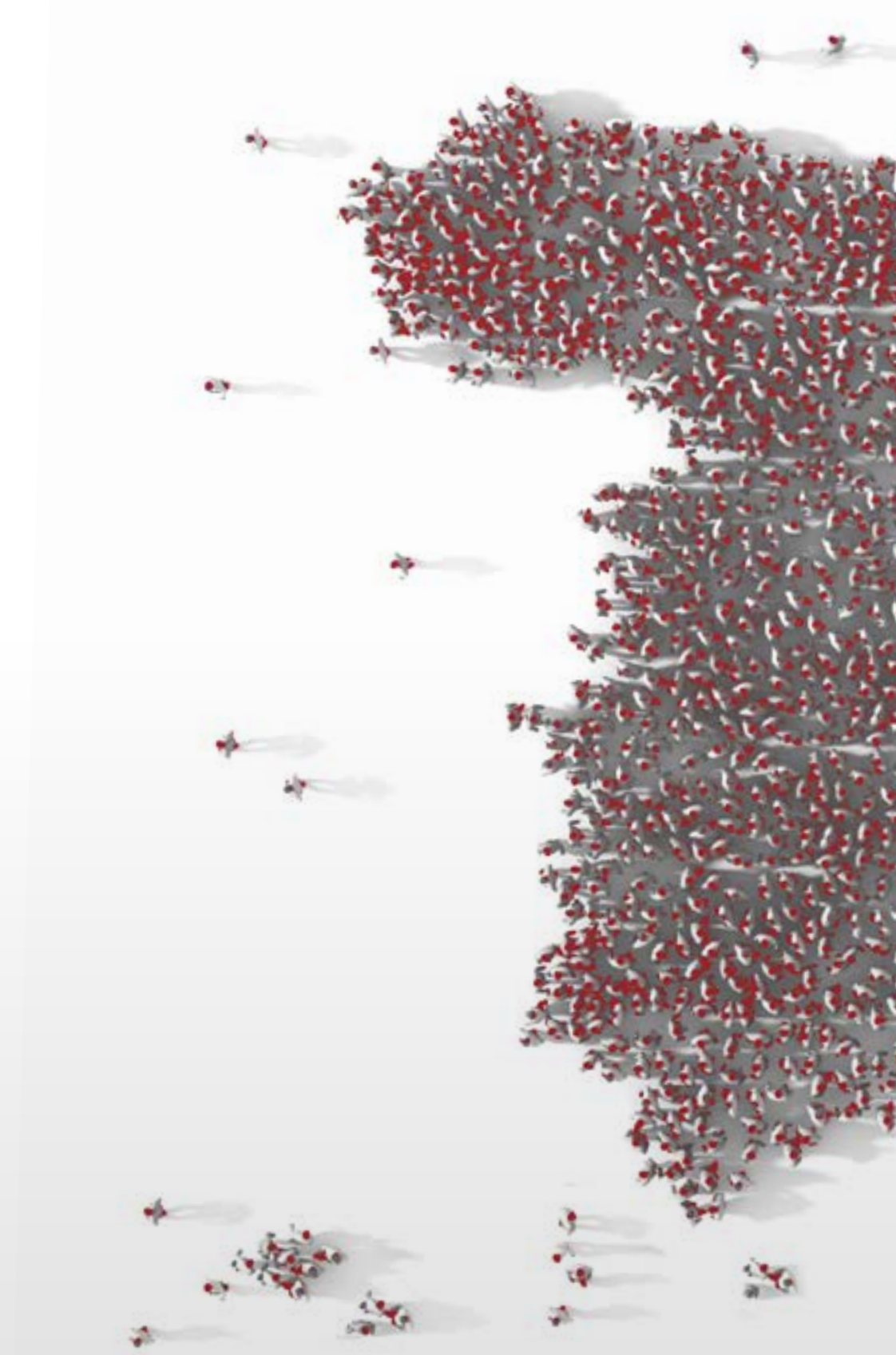
MOTOR DE LA COLABORACIÓN PÚBLICO-PRIVADA

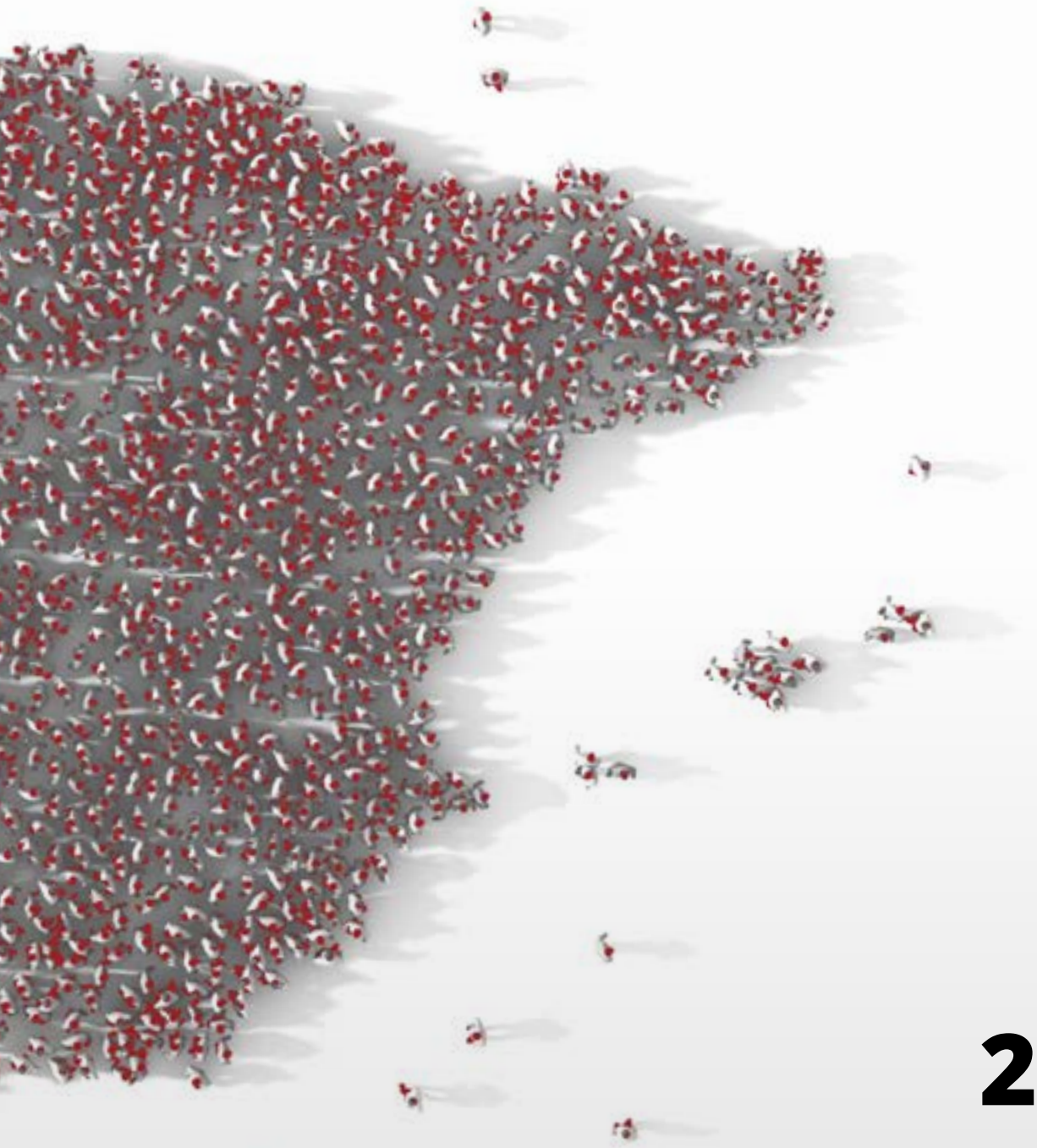
+++

- Informe sobre la cultura de la ciberseguridad en España.
- Informe sobre la industria e investigación españolas en ciberseguridad.
- Esquema Nacional de Certificación de Responsables de ciberseguridad.

Depósito Legal: M-31914-2021
NIPO En papel: 089-21-031-2
NIPO En línea: 089-21-032-8
Imprenta: Estugraf
Imprime: MPR

Índice global





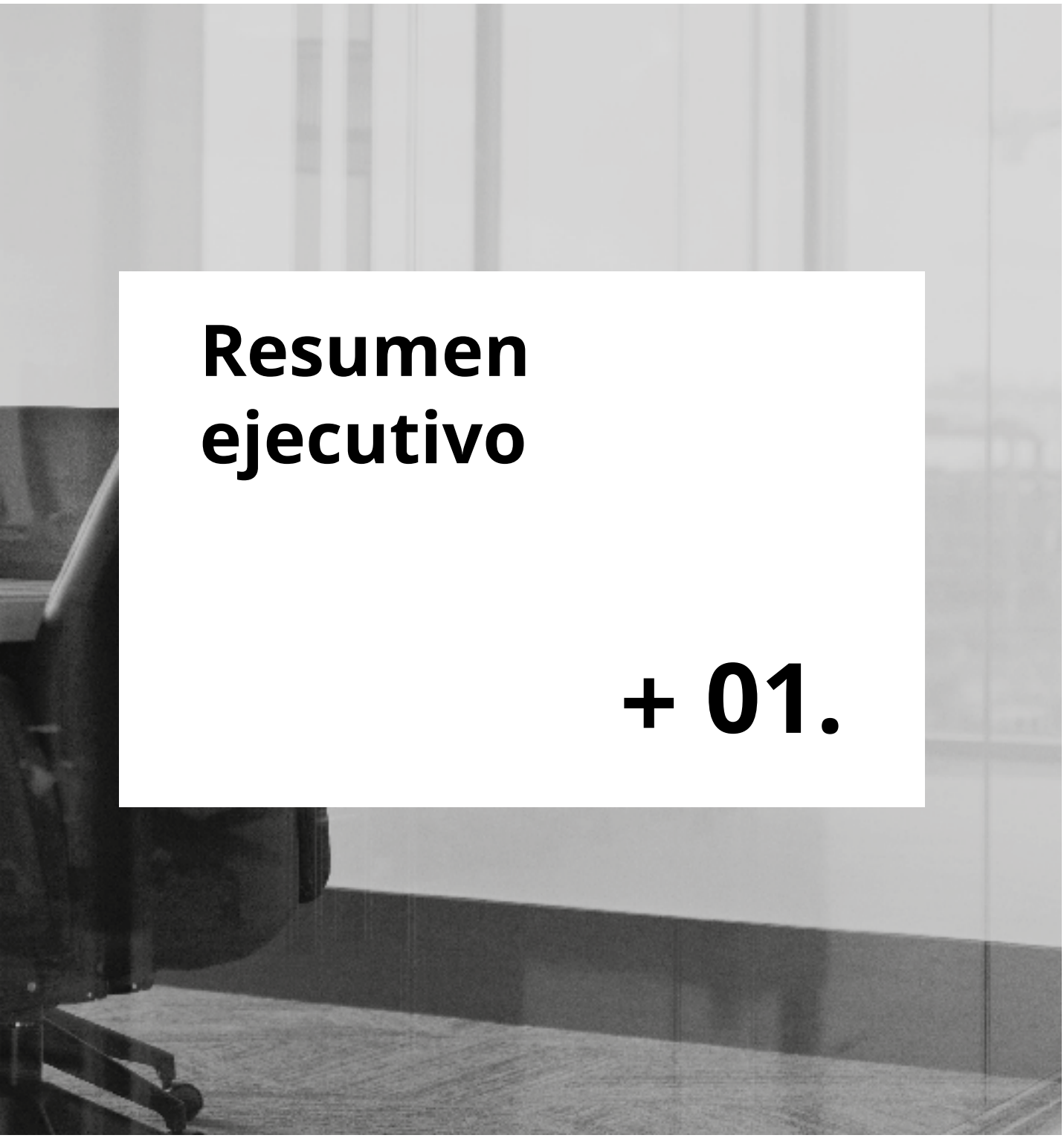
2021

INFORME SOBRE LA CULTURA DE LA CIBERSEGURIDAD EN ESPAÑA

FORO NACIONAL DE CIBERSEGURIDAD

Índice

+ Informe sobre la cultura de la ciberseguridad en España



Resumen ejecutivo

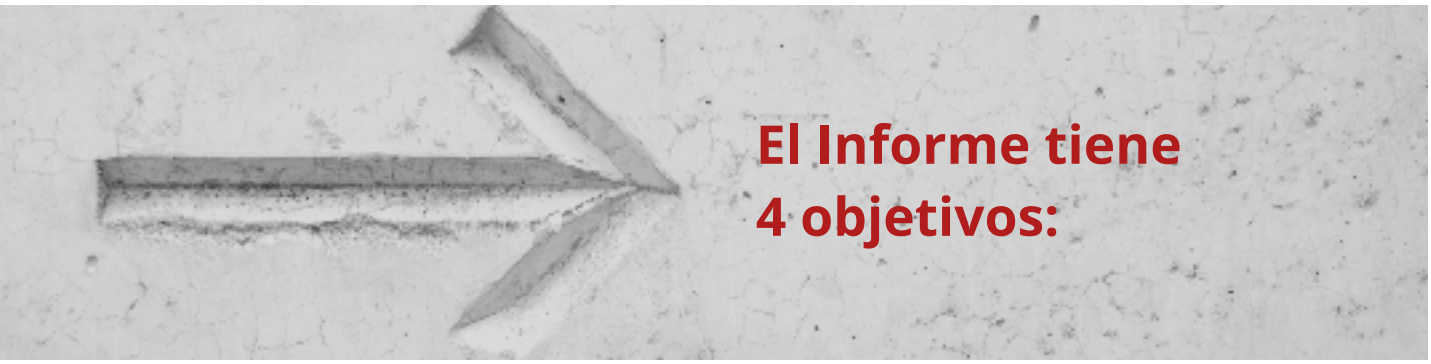
+ 01.

Resumen ejecutivo

La **Estrategia Nacional de Ciberseguridad de 2019** (ENCS)[1] establece en su Objetivo IV la necesidad de mejorar la ciberseguridad colectiva difundiendo la cultura de la ciberseguridad mediante la colaboración entre organismos públicos y entidades privadas, potenciando mecanismos de información y asistencia a los ciudadanos, y fomentando espacios de encuentro de la sociedad civil, las administraciones y las empresas.

La ENCS señala el fomento de la Cultura de Ciberseguridad como uno de los ejes centrales para alcanzar una sociedad más conocedora de las amenazas y desafíos a los que se enfrenta, atendiendo al derecho a disfrutar de un uso seguro y fiable del ciberespacio y a la obligación de contribuir a que así sea.

Con este fin, el Foro Nacional de Ciberseguridad creó el Grupo de Trabajo de Cultura de Ciberseguridad que, decidió comenzar sus trabajos mediante el presente Informe donde se ha realizado un análisis orientativo de las principales iniciativas existentes a nivel nacional e internacional, ha identificado áreas de mejora, ejes de actuación y programas que faciliten el desarrollo de nuevos proyectos orientados a elevar la cultura de ciberseguridad en España, y que deben entenderse como propuestas y recomendaciones al Consejo Nacional de Ciberseguridad.



El Informe tiene 4 objetivos:

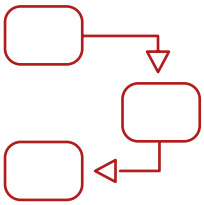
Objetivo 1:

Analizar las iniciativas y tendencias existentes a nivel nacional e internacional dirigidas al impulso de la cultura de ciberseguridad.

A nivel internacional, se han analizado las principales iniciativas de algunos países como Reino Unido, Estados Unidos, Francia, Lituania, Estonia y Singapur, que, junto con España, y por este orden, constituyen el TOP del ranking del Global Cybersecurity Index 2018 (CGI) de la Unión Internacional de Telecomunicaciones (UIT) de Naciones Unidas.

A nivel nacional, se recogen las principales iniciativas existentes llevadas a cabo tanto por el sector público como privado, a nivel central, autonómico y regional.

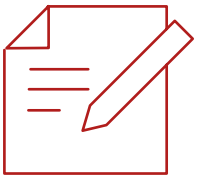
[1] https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019



Objetivo 2:

Fundamentar posibles acciones encaminadas a fomentar la cultura de ciberseguridad nacional y generar una conciencia social compartida sobre la importancia de la ciberseguridad.

Para cada medida de la ENCS se recoge un eje de acción, identificando posibles áreas donde se pueden realizar mejoras que puedan ayudar al alcanzar la implementación de estas medidas.



Objetivo 3:

Extraer conclusiones del estado actual de la cultura de ciberseguridad en España y valorar espacios de mejora.

Del análisis realizado de las iniciativas tanto a nivel internacional como nacional, se han extraído una serie de conclusiones respecto al estado de la cultura de ciberseguridad en España, entre las que destacan:

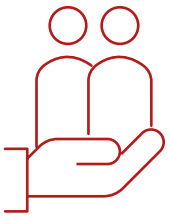
· Existe desconexión entre las numerosas iniciativas dirigidas a la concienciación y sensibilización y el desconocimiento de su existencia.

· No existe una visión global y exacta del estado de la cultura de ciberseguridad en la sociedad, así como del impacto de las iniciativas emprendidas.

· Desconocimiento de los ciberriesgos a los que se exponen los profesionales autónomos y las pequeñas empresas de ámbitos sectoriales específicos.

· La ciberseguridad en los actuales diseños curriculares es insuficiente y las actividades de concienciación en ciberseguridad en los centros de enseñanza son puntuales.

· La colaboración y participación de medios de comunicación en las campañas de ciberseguridad es muy limitada.

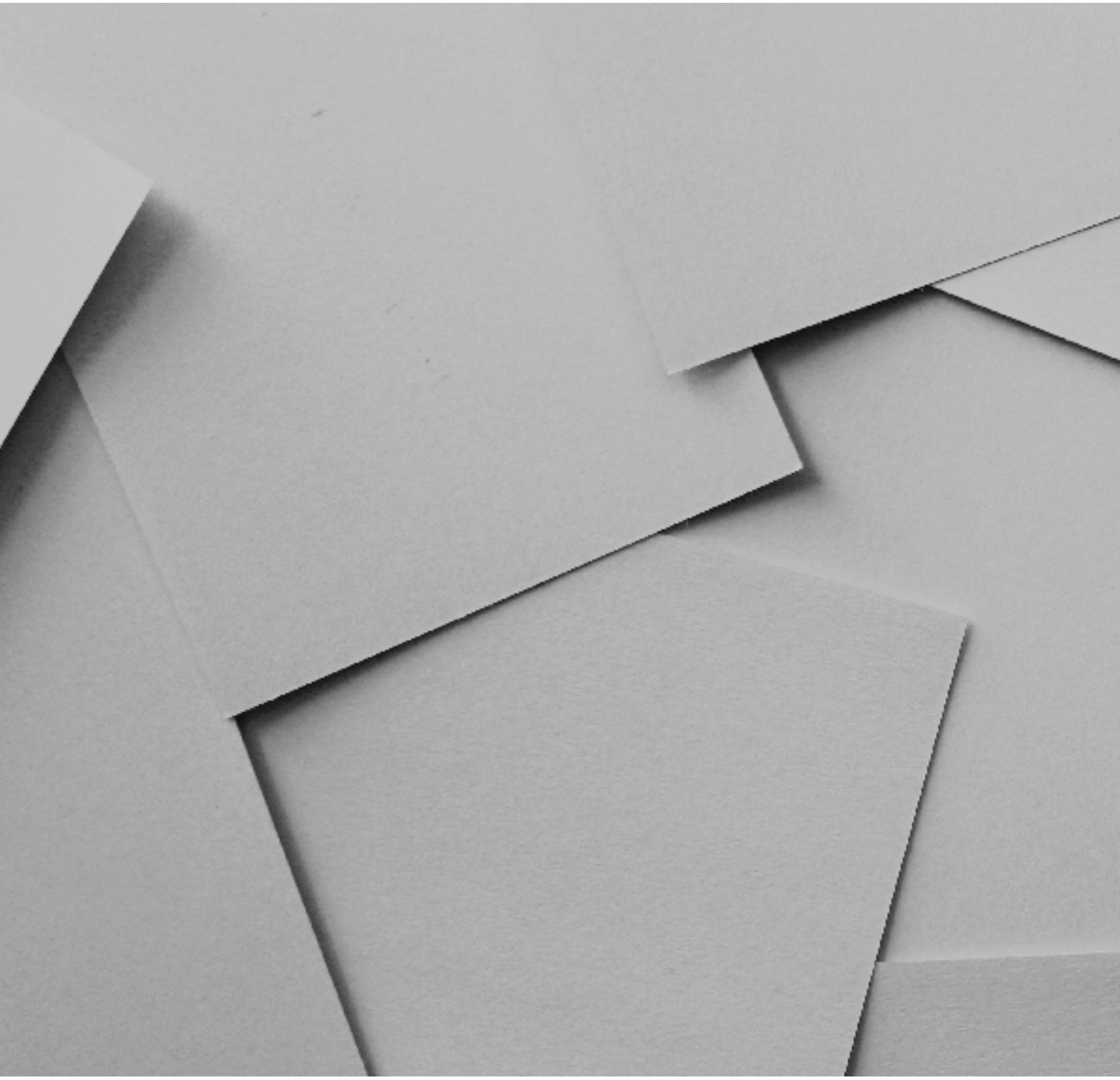


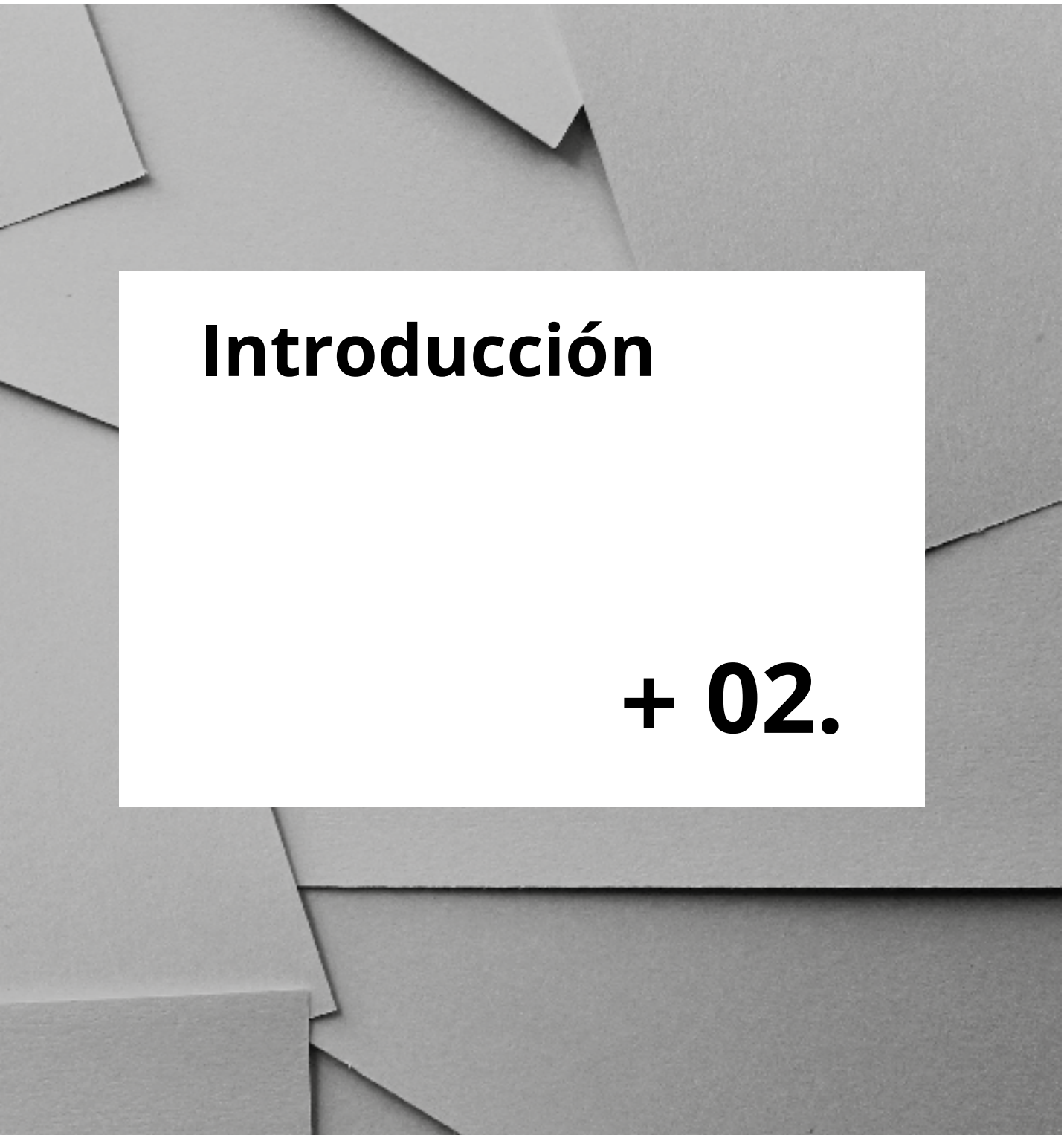
Objetivo 4:

Formular propuestas para mejorar el estado de la ciberseguridad y generar una conciencia social sobre su importancia.

A la vista de las iniciativas emprendidas tanto en el ámbito nacional como internacional, resulta evidente la necesidad de adoptar una serie de medidas dirigidas al incremento de la cultura de ciberseguridad y promoción de una conciencia social compartida. Entre ellas destacan acciones formativas y de concienciación en varios ámbitos, el refuerzo de la cultura en el ámbito educativo y para el impulso de alfabetización digital.

Sin duda, la medida más importante es la necesidad de contar con una visión global y exacta del estado de la cultura de ciberseguridad en la sociedad, así como del impacto de las iniciativas recogidas y de las futuras campañas. Este cuadro de mando sería parte de un **Observatorio para la elaboración y seguimiento del Barómetro Integral de Ciberseguridad** en la que participe el ecosistema de industria e investigación, los sectores público y privado y la ciudadanía en general, con especial dedicación a un sistema para la medición de la cultura de la ciberseguridad en España.





Introducción

+ 02.

Introducción

La **Ley 36/2015, de 28 de septiembre, de Seguridad Nacional**, establece que el Gobierno promoverá una cultura de Seguridad Nacional que favorezca la implicación activa de la sociedad en su preservación y garantía, como requisito indispensable para el disfrute de la libertad, la justicia, el bienestar, el progreso y los derechos de los ciudadanos. Señala, además, que uno de los ámbitos de especial interés es la ciberseguridad. Un ámbito que por sus singulares características y transversalidad requiere de la actuación del conjunto de las administraciones y de la sociedad en general para incrementar el conocimiento y la sensibilización sobre la materia.

Por otro lado, y como respuesta a dicho mandato, se ha desarrollado el **Plan Integral de Cultura de Seguridad Nacional**, un documento marco donde se definen las líneas de acción que desarrollarán el Estado, las Comunidades Autónomas, las entidades locales y otros organismos públicos y entidades privadas en materia de Seguridad Nacional. El objetivo es elevar el conocimiento de la sociedad civil proponiendo ámbitos de actuación relacionados con la formación, la comunicación pública y la divulgación, la internacionalización e influencia, y la participación.

El fomento de la Cultura de Ciberseguridad constituye pues, uno de los ejes centrales para alcanzar una sociedad más conocedora de las amenazas y desafíos a los que se enfrenta, atendiendo al derecho a disfrutar de un uso seguro y fiable del ciberespacio y a la obligación de contribuir a que así sea.

En este contexto, se entiende por **Cultura de Ciberseguridad** *el conocimiento y la sensibilidad de la sociedad en general y de cada persona en particular, de los riesgos y amenazas susceptibles de comprometerla, del esfuerzo de los actores y organismos implicados en su salvaguarda y la corresponsabilidad de todos en las medidas de anticipación, prevención, detección, protección, resistencia, colaboración y recuperación respecto a dichos riesgos y amenazas*.

Como se ha dicho, la ENCS de 2019 fija el objetivo de impulsar la cultura y el compromiso con la ciberseguridad, y potenciar las capacidades humanas y tecnológicas. Su desarrollo se plasma en la línea de acción siete articulada a través de ocho medidas, que constituyen el eje vertebrador del Informe.

2.1. La ciberseguridad: una responsabilidad compartida

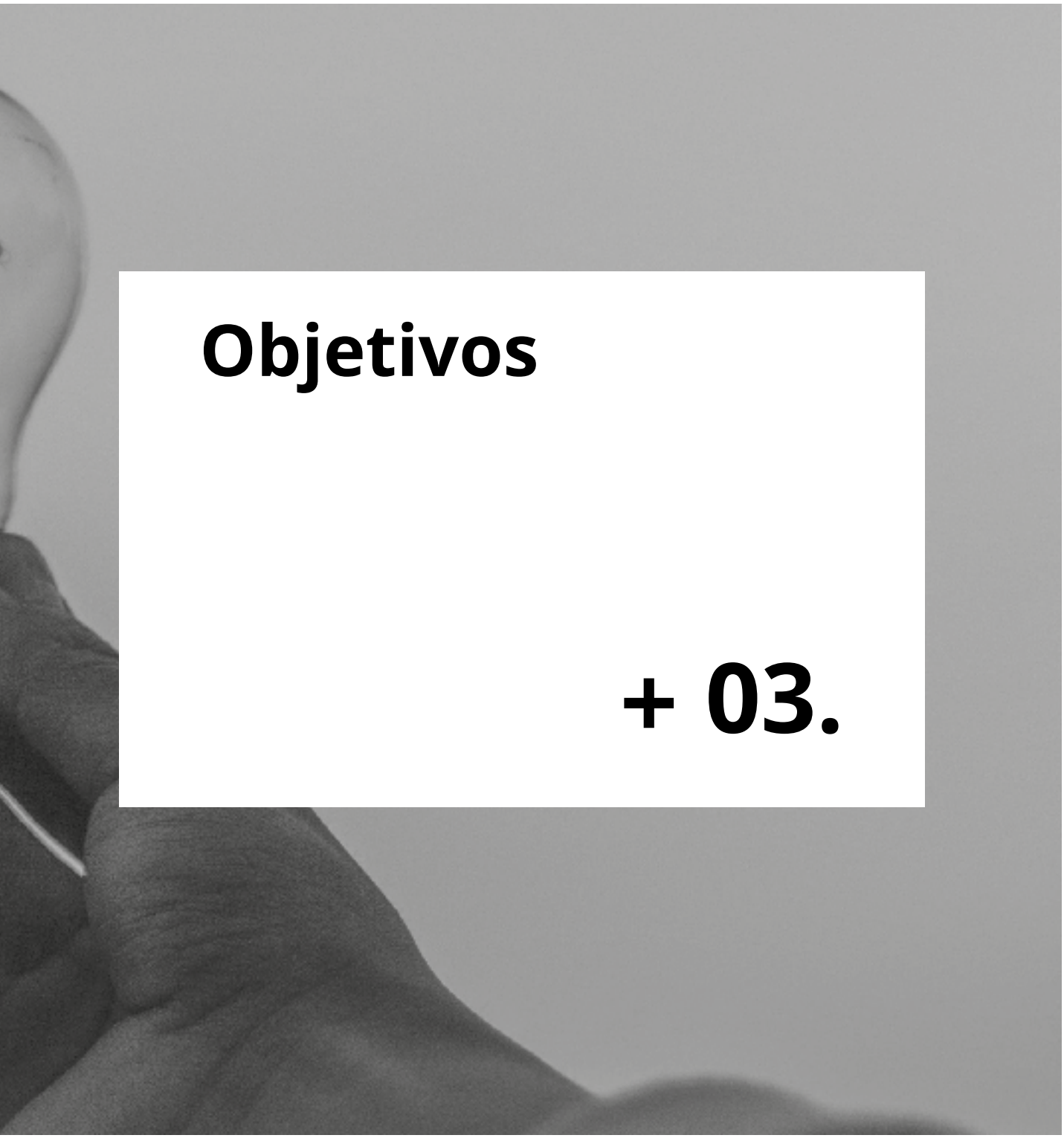
Los riesgos en el ciberespacio están en constante evolución, tanto en relación a su número como a su complejidad e impacto. La rápida adopción por la sociedad de tecnologías emergentes está causando un aumento preocupante en el número y peligrosidad de incidentes detectados.

El derecho a hacer un uso seguro y fiable del ciberespacio y el contribuir a que así sea –en definitiva, **alcanzar la confianza digital**–, es una responsabilidad compartida entre todos los actores públicos y privados y el conjunto de la sociedad.

Desde la perspectiva **del sector público** es fundamental promover una normativa eficaz que permita el adecuado desarrollo socioeconómico de España, a la vez que se impulsan medidas que garanticen la protección de los derechos de las personas. Por otro lado, es clave establecer medidas de defensa de la seguridad nacional, robustas y directas, dotando de recursos suficientes al Estado para alcanzar los objetivos de la ciberseguridad nacional.

En este marco, y puesto que la ciberseguridad es una responsabilidad compartida, las Administraciones Públicas deben mantener una coordinación eficaz con el **sector privado**, especialmente con quienes gestionan los sistemas de información y telecomunicaciones (STIC) relevantes para los intereses nacionales. Se deben favorecer buenas prácticas de gestión y medidas conducentes a la seguridad común, tanto en el empleo de las capacidades de análisis y evaluación, como en las de reacción ante los nuevos desafíos. Todo ello, colaborando en iniciativas y propiciando el intercambio de información y de conocimiento.

La **ciudadanía y la sociedad civil** también son corresponsables de la ciberseguridad nacional. Su comportamiento puede afectar a su propia seguridad y a la de otras personas, así como a los servicios e infraestructuras y a la seguridad nacional. Los usuarios deben conocer y tomar conciencia de los riesgos a los que se enfrentan, buscando su compromiso en la tarea común de proteger a la sociedad. En este sentido, debe promoverse el uso seguro de los servicios basados en STIC, así como la adopción de medidas preventivas que eviten o minimicen los riesgos cibernéticos propios de una sociedad conectada.



Objetivos

+ 03.

Objetivos

Los objetivos específicos de este Informe de la Cultura de la Ciberseguridad son los siguientes:

Objetivo 1

Analizar las iniciativas y tendencias existentes a nivel nacional e internacional dirigidas al impulso de la cultura de ciberseguridad.

Objetivo 2

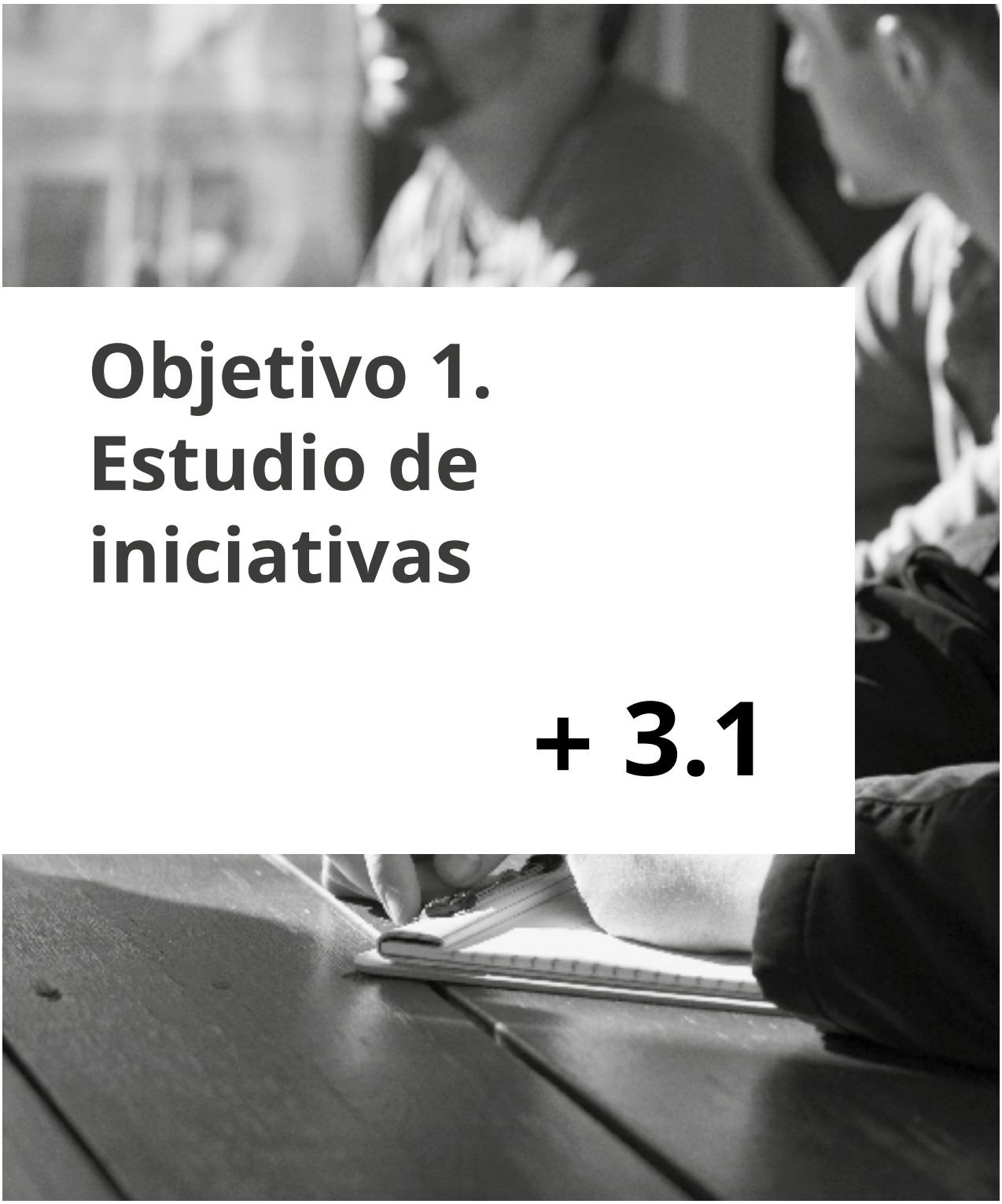
Fundamentar posibles acciones encaminadas a fomentar la cultura de ciberseguridad nacional y generar una conciencia social compartiida sobre la importancia de la ciberseguridad.

Objetivo 4

Formular propuestas para mejorar el estado de la cultura de la ciberseguridad y generar una conciencia social sobre su importancia.

Objetivo 3

Extraer conclusiones del estado actual de la cultura de la ciberseguridad en España y valorar espacios de mejora.



Objetivo 1. Estudio de iniciativas

+ 3.1

3.1.1. Ámbito internacional

Existen **multitud de iniciativas** para dirigidas **a mejorar la cultura en ciberseguridad de diferentes colectivos**. Aunque muchas de ellas son lideradas por organizaciones internacionales sin ánimo de lucro u organismos como universidades o institutos tecnológicos, su amplio alcance y público generalista hace que difícilmente se profundice más allá de sencillos consejos o formación online básica.

Para acotar el análisis orientativo a un universo razonable, se han tomado en consideración iniciativas de Reino Unido, Estados Unidos, Francia, Lituania, Estonia y Singapur, países que, junto con España, y por este orden, constituyen el **TOP del ranking del Global Cybersecurity Index 2018 (CGI) de la Unión Internacional de Telecomunicaciones (UIT[2])**.

En consecuencia, se han seleccionado algunas de las iniciativas identificadas en los seis primeros países mencionados, que podrían servir a España como inspiración o guía.

3.1.1.1 Reino Unido

El organismo gubernamental NCSC[3] (National Cyber Security Centre) ofrece soporte al sector público, privado y a la ciudadanía en general, tanto en la gestión de incidentes, como en las acciones de concienciación y prevención, basadas en su experiencia, así como en el conocimiento de la industria y el sector académico.

Entre sus iniciativas, destacan:

• **Cyber Aware**, con consejos dirigidos a individuos y pequeños negocios para protegerse en su actividad online contra el cibercrimen.

• **Cyber Essentials**, con guías para las empresas sobre prácticas básicas a considerar para protegerse contra las ciberamenazas.

• **Cyber Security, Information Sharing Partnership (CISP)**, proyecto conjunto con la industria para compartir entre organizaciones información de amenazas.

• **Takedown Service**, enfocado al cierre de sitios fraudulentos vinculados con objetivos de suplantación de la identidad de los servicios y marcas corporativas del Gobierno.

• **CyberFirst**, un programa para introducir a jóvenes de edades entre 7 y 17 años en el mundo de la ciberseguridad. Entre otras acciones desarrolla la iniciativa CyberFirst Schools and Colleges (CISSE) dentro de los colegios para impulsar la educación en ciberseguridad de forma estructurada. Los centros pueden obtener un certificado de excelencia según su nivel en el desarrollo de contenidos.

• **ACE-ASR (Academic Centres Of Excellence in Cyber Security Research)**, una iniciativa en el ámbito de la investigación de la que forman parte diecinueve universidades.

[2] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[3] NCSC/ https://www.ncsc.gov.uk/section/about-ncsc/what-we-do / diciembre 2020

3.1.1.2 Estados Unidos

En la última década, la ciberseguridad se ha convertido en una prioridad federal. Así lo constata su Estrategia Nacional de Ciberseguridad de 2018[4], en la que se señala que, para proteger la seguridad nacional y la prosperidad de los americanos, es fundamental asegurar el ciberespacio. Para ello apela a la responsabilidad de ciudadanos y compañías.
Entre sus iniciativas, destacan:

• **Stop. Think. Connect**[5], lanzada en 2009 por el Departamento de Seguridad Nacional. Es una campaña de concienciación para comprender los peligros de estar en línea y las iniciativas que permitan protegerse de las amenazas del ciberespacio. La iniciativa recuerda a la ciudadanía que la ciberseguridad es una responsabilidad compartida en casa, en las escuelas, centros de educación y en las comunidades.

• **NICE framework - National Initiative for Cybersecurity Education (NICE)**[6], para mejorar la contratación y retención de profesionales de ciberseguridad altamente cualificados.

• **READY**[7], lanzada en febrero de 2003. Es una campaña nacional de servicio público diseñada para educar y capacitar al pueblo estadounidense para prepararse, responder y mitigar emergencias, incluidos desastres naturales y provocados por el hombre.

• **Alianza Nacional de Ciberseguridad (NCSA-National Cybersecurity Alliance**[8]**)**, creada en 2001 para favorecer alianzas público-privadas. Su objetivo es crear e implementar esfuerzos de educación y concienciación de amplio alcance para empoderar a los usuarios en el hogar, el trabajo y la escuela, y fomentar una cultura de ciberseguridad en todas ellas.

3.1.1.3 Francia

Francia es otro de los países con mayor nivel de compromiso en la materia. Uno de los cinco objetivos de su Estrategia Nacional de Ciberseguridad se centra precisamente en sensibilizar y formar a su población. La mayoría de las acciones están dirigidas por la **French National Cybersecurity Agency, ANSSI**.

Además, existen otras iniciativas, que brindan servicios de concienciación y gestión de la ciberseguridad, como www.cybermalveillance.gouv.fr, la cual dispone de un formulario interactivo para ayudar a ciudadanos y empresas a identificar y conseguir asistencia ante incidentes de seguridad de la información. La web también contiene otros recursos formativos interesantes en formato de artículos.

Recientemente, también ha creado el Campus Ciber, un hub de ciberseguridad que para este año espera reunir a los principales actores nacionales e internacionales en la materia, albergando en el mismo edificio a empresas (desde grandes grupos hasta pymes), departamentos gubernamentales, academia, sector de investigación y asociaciones. Hasta la fecha, más de 60 actores de diversos sectores han manifestado su voluntad de participar en el Campus.

[4] https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[5] https://www.stopthinkconnect.org/
[6] https://www.nist.gov/itl/applied-cybersecurity/nice
[7] https://www.ready.gov/cybersecurity
[8] https://staysafeonline.org/

3.1.1.4 Lituania

Lituania publicó en 2017 un informe[9] en el que evaluó sus capacidades nacionales de ciberseguridad.

Una iniciativa destacable de este país es su evento **CYBERteens**[10], en el cual se dan cita jóvenes, profesores y expertos, y donde los niños pueden participar activamente en la creación de soluciones para mejorar su seguridad en Internet. Resulta también de interés la existencia de teléfonos de asistencia a menores[11] y herramientas *online* de denuncia anónimas destinadas a ser utilizadas por menores[12]; también se ofrecen estadísticas abiertas sobre el uso que se da de este servicio[13].

3.1.1.5 Estonia

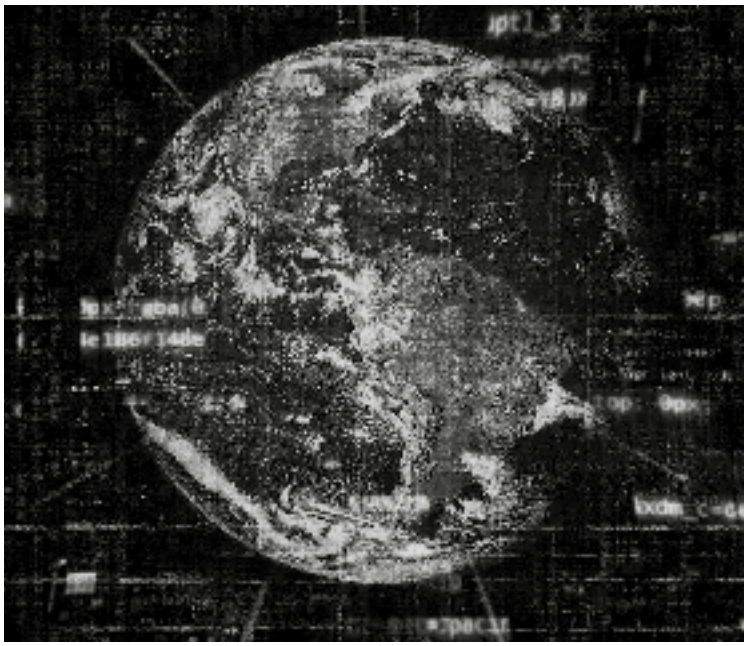
Estonia se ha convertido en un referente en el desarrollo y la aplicación de STIC. Ha desarrollado su Estrategia Nacional de Ciberseguridad para el periodo 2019-2022, basada en cuatro pilares: **sociedad digital sostenible**, **industria e I+D en ciberseguridad**, convertirse en **proveedor internacional líder** y ser una **sociedad *ciberilustrada***.

Para cada uno de estos pilares, a su vez, se concretan actividades bien definidas para alcanzar los objetivos estratégicos marcados.

3.1.1.6 Singapur

Singapur cuenta con numerosas iniciativas. Destacan las siguientes:

- **Cybersecurity Challenge Singapore**, que contiene retos y competiciones destinadas a atraer a aficionados a la ciberseguridad y convertirlos en profesionales.
- **Cybersecurity Career Mentoring Programme**[14] y **Cyber Security Associates and Technologists**[15], iniciativas destinadas a poner en contacto a jóvenes estudiantes o profesionales junior con especialistas y empresas que actúan como mentores o lanzaderas de sus carreras profesionales.
- **Go Safe Online**[16], contiene multitud de recursos para todos los públicos.



[9] https://www.nrdcs.lt/file/repository/resources/Lithuania_Report_10_8_2017_FINAL.pdf

[10] https://www.draugiskasinternetas.lt/en/about-sid/sid-2020/

[11] https://www.draugiskasinternetas.lt/en/about-safer-internet/helpline/

[12] https://svarusinternetas.lt/en

[13] https://svarusinternetas.lt/statistika/5

[14] https://www.csa.gov.sg/programmes/cybersecurity-career-mentoring-programme

[15] https://www.csa.gov.sg/programmes/csat

[16] https://www.csa.gov.sg/gosafeonline

3.1.2. Ámbito nacional

En España, también existen multitud de iniciativas en línea con la definición de cultura de ciberseguridad adoptadas en este documento. Se mencionan aquí las más significativas.

3.1.2.1 Foro Nacional de Ciberseguridad

Es un órgano de asistencia al Consejo Nacional de Ciberseguridad, basado en la colaboración público-privada, y creado en base a lo previsto en la en la Estrategia Nacional de Ciberseguridad de 2019. Precisamente, uno de sus grupos de trabajo se centra exclusivamente en la cultura[17].

3.1.2.2. Ministerio de Defensa

La dirección y coordinación de las acciones de concienciación en el Ministerio de Defensa corresponde al **Mando Conjunto del Ciberespacio (MCCE)**[18], mientras que la ejecución de las diversas actividades corre a cargo del propio MCCE y de los Ejércitos/Armada en sus respectivos ámbitos.

Entre las principales **actividades**, se encuentran las siguientes: **difusión de boletines** informativos sobre aspectos básicos de ciberseguridad; difusión de boletines reactivos ante campañas de *phishing*, *malware*, *ransomware*, etc., o en momentos especialmente sensibles; difusión de recomendaciones en redes sociales; **jornadas de concienciación** a los contingentes que se van a desplegar en misiones internacionales, entre otras.

3.1.2.3. Ministerio del Interior

A través del Plan director para la convivencia y mejora de la seguridad escolar de la Secretaría de Estado de Seguridad[19], son varias las líneas de compromiso con la concienciación para ciudadanos y empresas en general.

La **Guardia Civil** despliega acciones de interés, como:

• **Liga interuniversitaria de ciberseguridad** (National Cyber League[20]), que consiste en una competición entre equipos de estudiantes universitarios dirigida a identificar talento y a ofrecerle ayudas materiales y profesionales (becas, prácticas y empleo en distintas empresas patrocinadoras).

[17] https://foronacionalciberseguridad.es/

[18] https://emad.defensa.gob.es/unidades/mcce/

[19] http://www.interior.gob.es/web/servicios-al-ciudadano/planes-de-prevencion/plan-director-para-la-convivencia-y-mejora-escolar

[20] https://www.nationalcyberleague.es/

• Acción constante en **redes sociales**, donde ofrece consejos de ciberseguridad a ciudadanos y empresas, especialmente dirigidos a los colectivos más vulnerables.

• **Conferencias *online* a pymes y centros educativos**.

La **Policía Nacional** organiza las siguientes acciones:

• **C1b3rWall**[21], proyecto de difusión de cultura de ciberseguridad y capacitación digital con el objetivo de potenciar la lucha contra la ciberdelincuencia desde el ámbito de la prevención, mediante acciones de formación abierta y gratuita.

• Programas de colaboración público-privada como los proyectos **Ciberexperto, Sé genial en Internet y Controla tu red** que ofrecen un conjunto de recursos a familias y educadores para enseñar a los más pequeños a hacer un uso responsable de Internet.

• **Conferencias en centros educativos** y campañas informativas en **redes sociales**.

3.1.2.4. Centro Criptológico Nacional

De entre las iniciativas relacionadas con el fomento de la cultura de ciberseguridad que lleva a cabo el Centro Criptológico Nacional (CCN)[22], adscrito al Centro Nacional de Inteligencia, destacan las siguientes:

• Portal **Ángeles**, de formación y talento en ciberseguridad. En él se ofrece un **programa de cursos formativos** y *webinars* para los profesionales del sector público. Cuenta con una sección dedicada a consejos de ciberseguridad.

• **Atenea**. Es una **plataforma de desafíos del CCN-CERT** que, mediante una serie de retos de distinta dificultad y muy diversas temáticas (criptografía y esteganografía, *exploiting*, forense, análisis de tráfico, *reversing*, etc.), **permite al usuario demostrar sus conocimientos** y destrezas.

• **Atenea Escuela**. Es una plataforma básica de desafíos de ciberseguridad.

• **ELENA**. Es una solución que acompaña a un programa de formación multidisciplinar de analistas e investigadores de *cibervigilancia*. Facilita al profesional el ensayo y entrenamiento de los conceptos teóricos aprendidos en cursos de *cibervigilancia* o en su propia experiencia profesional.

[21] https://c1b3rwallacademy.usal.es/

[22] https://www.ccn.cni.es/index.php/es/

• El CCN elabora de manera periódica **Informes de Buenas Prácticas, Guías CCN-STIC, Informes de Amenazas y de Código Dañino**.

• **Avisos y alertas** sobre vulnerabilidades o amenazas reales que requieren atención inmediata por parte de las organizaciones.

• **Organización de eventos para profesionales de la ciberseguridad**. A lo largo del año, el CCN organiza cuatro eventos de cara a los profesionales: Jornadas STIC, Jornadas del SAT (Sistema de Alerta Temprana del CCN-CERT), Encuentro del Esquema Nacional de Seguridad (ENS) y, desde este mismo año, Jornadas STIC-Capítulo Colombia.

3.1.2.5. Instituto Nacional de Ciberseguridad (INCIBE)

INCIBE, sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, pone a disposición de los ciudadanos los siguientes **servicios**:

• **"Protege tu empresa"**[23].

• Organización de eventos dirigidos a distintos fines, como concienciación (CyberCamp, Día de Internet Segura, Jornadas "Espacios ciberseguridad"), apoyo a profesionales e investigadores (ENISE, Cybersecurity Summer Bootcamp, #mujeresciber, RENIC), o ciberejercicios, como International CyberEx.

• **Línea de Ayuda en ciberseguridad (017)**. Servicio de **atención telefónica** a empresas y ciudadanos, que atiende **consultas y denuncias** relacionadas con la **ciberseguridad**.

• **Oficina de Seguridad del Internauta** (OSI).

• **Fomento del emprendimiento**. (Cybersecurity Ventures y Ciberemprende).

• **Concienciación de familias y menores**. **Línea** específica de **concienciación al menor**, denominada **Internet Segura For Kids (IS4K)**, a través de la cual se pone a disposición de padres, educadores y menores, contenidos y herramientas que ayuden a educar y a proteger la navegación.

• **Programa de voluntariado ("Cibercooperantes")**, que permite a cualquier persona impartir una sesión formativa en **ciberseguridad** en aquellos **centros escolares y educativos** que así lo soliciten.

[23] https://www.incibe.es/protege-tu-empresa

3.1.2.6. Comunidades Autónomas

Todas las Comunidades Autónomas desarrollan o prestan su apoyo a iniciativas relacionadas con la ciberseguridad o la promoción de su cultura, desde la creación de CSIRT a la implementación de diversas acciones de concienciación. Destacan entre otras las siguientes iniciativas:

A. Andalucía CERT[24] (Andalucía)

Entre sus funciones se encuentra la elaboración y distribución de boletines de ciberseguridad, de carácter divulgativo, sobre nuevas amenazas, tecnologías de seguridad, buenas prácticas y temas de actualidad del sector. Por otra parte, AndalucíaCERT imparte cursos y ponencias orientados a la mejora en la gestión de riesgos digitales y el mantenimiento de la seguridad en los equipos y sistemas.

B. Agencia de Ciberseguridad de Cataluña[25] (Cataluña)

Es la encargada de establecer el servicio público de ciberseguridad y trabaja para garantizar y aumentar el nivel de seguridad de las redes y los sistemas de información en Cataluña, así como la confianza digital de los ciudadanos. Destaca en materia de concienciación y sensibilización el Programa Internet Segura[26].

C. Centro Vasco de Ciberseguridad[27] (País Vasco)

Organización designada por el Gobierno Vasco cuya misión es promover y desarrollar una cultura de ciberseguridad entre la sociedad vasca, dinamizar la actividad económica relacionada con la aplicación de la ciberseguridad y fortalecer el sector profesional.

Desde su departamento de Educación se lanzó la iniciativa Bizikasi, que pretende contribuir a que los centros educativos sean espacios seguros.

D. CIBER.gal[28] (Galicia)

Se ha desarrollado CIBER.gal, un nodo conformado por las administraciones públicas gallegas, e instituciones privadas que de manera colaborativa buscan hacer frente a la creciente amenaza que suponen los ataques cibernéticos y aprovechar las oportunidades que presenta la nueva era digital. Con iniciativas como Rapaciños. A Tecnoloxía ben segura se intenta fomentar el conocimiento de la ciberseguridad en los hogares.

---

[24] https://www.juntadeandalucia.es/organismos/presidenciaadministracionpublicaeinterior/areas/tecnologias-informacion/seguridadyconfianzadigital/paginas/andaluciacert-jda.html

[25] https://ciberseguretat.gencat.cat/es/agencia/

[26] https://ciberseguretat.gencat.cat/es/detalls/noticia/Internet-Segura-esdeve-el-Programa-oficial-de-la-Generalitat-en-conscienciacio-sobre-ciberseguretat

[27] https://www.basquecybersecurity.eus/es/

[28] https://amtega.xunta.gal/es/cibergal

E. CSIRT-CV[29] (Comunidad Valenciana)

El CSIRT de la Comunidad Valenciana ha diseñado y ejecutado un conjunto de acciones dirigidas al ciudadano y a las empresas ubicadas en dicho territorio: Cursos, guías, campañas de concienciación o herramienta para que las pymes autoevalúen su seguridad.

F. CyberMadrid[30] (Comunidad de Madrid)

El Clúster de Ciberseguridad CyberMadrid tiene la finalidad de sensibilizar y formar a empresas y ciudadanos en la importancia crítica de la ciberseguridad; reforzar el emprendimiento, incluyendo el desarrollo de nuevas empresas y el crecimiento de las ya existentes; contribuir a generar talento; y mejorar la empleabilidad.

G. Cybersecurity Innovation HUB[31] (Junta de Castilla y León)

El Cybersecurity Innovation Hub tiene el objetivo de mejorar el conocimiento que tienen las empresas de las políticas de ciberseguridad activas que deben adoptar y acompañarlas en sus procesos de transformación digital.

[29] https://www.csirtcv.gva.es/

[30] comunidad.madrid/noticias/2021/02/11/comunidad-madrid-ciberseguridad

[31] https://www.cyberdih.com/

3.1.2.7. Iniciativas del sector privado y medios de comunicación

Numerosas empresas y organizaciones vinculadas al sector privado, **elaboran guías de buenas prácticas y difunden consejos** sobre ciberseguridad, que ponen a disposición del público en general y, especialmente, de sus propios trabajadores y asociados.

Entre las iniciativas llevadas a cabo, caben destacar:

· **Acciones dirigidas a** la concienciación de los **internautas**.

· Acciones de **concienciación** sobre ciberseguridad en el **sector profesional e industrial** de la seguridad y en el ámbito de las Infraestructuras Críticas y Servicios Esenciales en particular.

· Acciones de **promoción y desarrollo, conocimiento y cultura de la seguridad** de la información en España.

· Acciones de **formación y servicios** para **pequeñas y medianas empresas** para dar a conocer y reforzar su ciberseguridad.

· Inclusión de **consejos y recomendaciones** de ciberseguridad en páginas **web empresariales** dirigidas a usuarios.

· **Asociaciones** dedicadas al **intercambio de conocimiento y experiencias** de los sectores económicos para mejorar el nivel de ciberseguridad de la industria.

· Asociaciones dirigidas al **apoyo del desarrollo de metodologías y certificaciones** para la realización de actividades de **auditoría, control y gestión** de ciberseguridad.

· Acciones de **promoción** dirigidas **a colectivos en riesgo** de exclusión social.

· ***Think thanks*** dedicados al análisis estratégico de la ciberseguridad.

Otras iniciativas privadas:

· Acciones de promoción del **uso saludable de la tecnología** a través de la formación, la difusión de materiales didácticos e investigaciones y estudios o la difusión de programas televisivos centrados en la ciberseguridad y el *hacking*.

· Difusión de **contenidos educativos para menores, padres y educadores**. Canales de YouTube sobre seguridad en la red, portales y sitios web con contenidos y materiales educativos y formativos dirigidos al uso fiable y seguro de las nuevas tecnologías en familia, así como los destinados a madres y padres para ayudar a guiar a sus hijos en Internet.

· **Teléfonos de asistencia** en materia de situaciones que pueden afectar **al menor en Internet** que incluyen asesoramiento psicológico y jurídico.

· Actividades de **promoción de la privacidad y seguridad digital**.

· **Libros especializados sobre ciberseguridad**. Ya sea en medio digital o impreso, existen excelentes obras en castellano, la mayoría dirigidas a perfiles técnicos. Sin embargo, también existen iniciativas en el campo de la cultura de ciberseguridad dirigidos a madres y padres; consejos para tener vidas digitales más seguras; cuentos de ciberseguridad; la evolución de la ciberseguridad, entre otros.

28

No se puede entender la ciberseguridad sin aludir al papel de la **comunidad *hacker*** porque en ella se han gestado los primeros pasos de la cultura de ciberseguridad. En España se realizan numerosas reuniones de expertos en ciberseguridad en este marco.

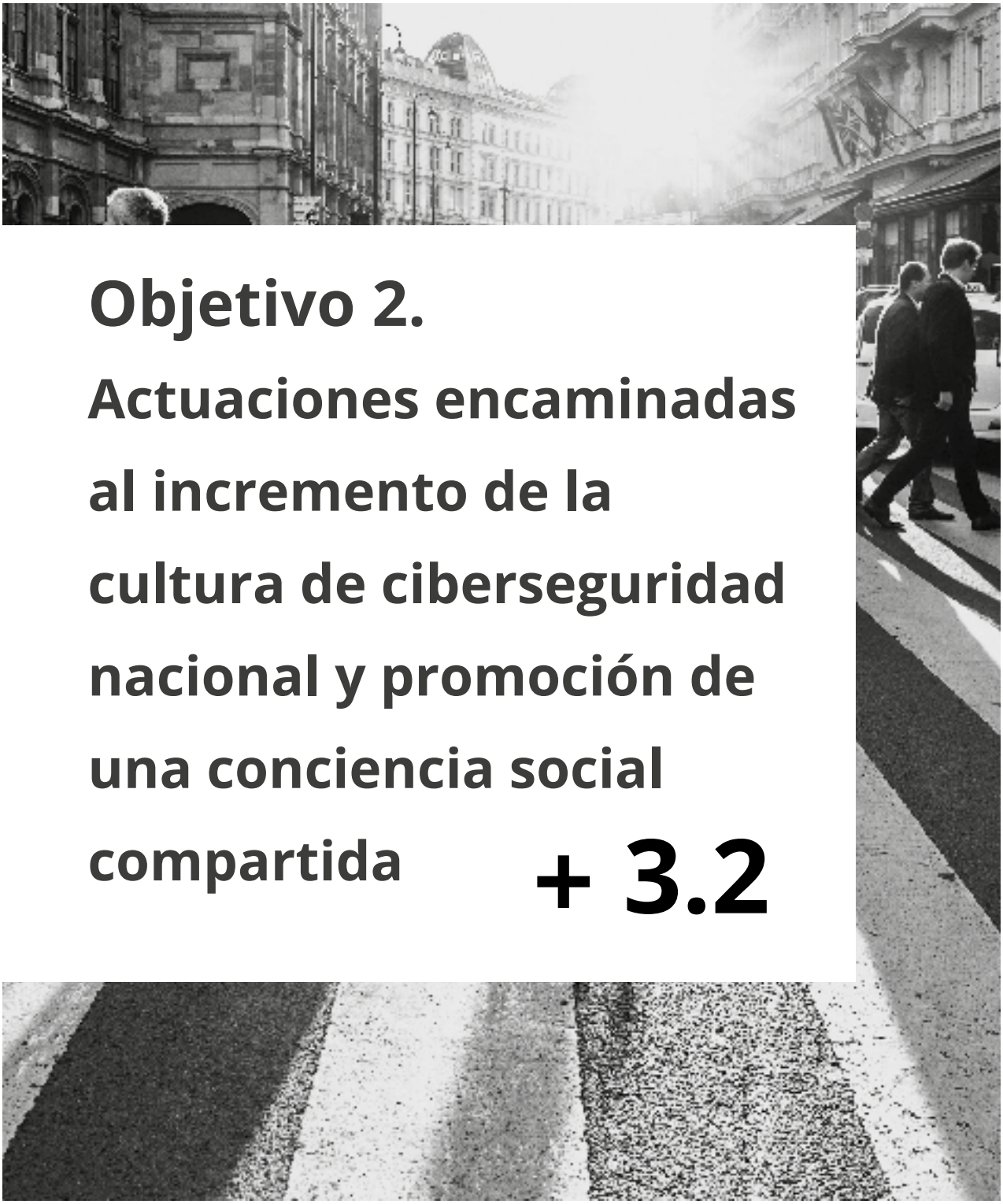
Es innegable la labor de los **medios de comunicación de información general en la promoción de la cultura de ciberseguridad**, ámbito al que vienen prestando una creciente atención.

Por un lado y a nivel público, destaca el papel de **Radio Televisión Española**, que ha difundido una serie de programas dedicados a la temática de la ciberseguridad. Por ejemplo, a la carta 24h, o Alianza 2030 (RNE) le han dedicado programas íntegros a esta materia, y el programa "Seguridad del Internauta", que emiten semanalmente RTVE e INCIBE en Radio 5.

Por otro lado, existen programaciones y espacios de radio nacional y local dedicados a la ciberseguridad, que abordan noticias de actualidad, entrevistas a profesionales, entre otras, con un objetivo divulgativo tanto para empresas como para usuarios, pero también persiguiendo una visión informativa y didáctica.

Merecen una mención especial los medios de comunicación especializados. Medios impresos y digitales que aportan visiones multidisciplinares de la ciberseguridad, la privacidad o el derecho de las TIC. Se pueden encontrar publicaciones monográficas y especializadas, portales de contenidos, redes sociales, newsletter, entre otros, que a su vez organizan eventos muy demandados y apoyados por el sector público y privado, a la par que otorgan premios anuales de reconocimiento y puesta en valor buenas prácticas en materia de ciberseguridad.

También los medios de comunicación online especializados en actualidad e información sobre ciberseguridad, así como tecnología e innovación, que apoyan la publicación de contenido divulgativo y de concienciación sobre ciberseguridad.



Objetivo 2.

Actuaciones encaminadas al incremento de la cultura de ciberseguridad nacional y promoción de una conciencia social compartida

+ 3.2

3.2.1. Eje 1. Concienciación

Medida Estrategia Nacional de Ciberseguridad 1: Incrementar las campañas de concienciación a ciudadanos y empresas, y poner a su disposición información útil adaptada a cada perfil, especialmente en el ámbito de los autónomos, pequeñas y medianas empresas.

La **concienciación en ciberseguridad** debe formar parte de las habilidades de cualquier itinerario formativo, para que cualquier persona tenga ciertas destrezas en este ámbito. Dado que las personas constituyen la primera línea de defensa en las organizaciones o en el hogar, es importante que tomen conciencia de los riesgos a los que se enfrentan. En especial los niños, en cuya educación es importante introducir conceptos de ciberseguridad.

La concienciación, si bien es una herramienta útil, debe estar cuidadosamente planificada, además de ser continua y metódica para que tenga éxito. Esta carrera de fondo de la concienciación debe obedecer a una estrategia perfectamente diseñada, dotada de recursos, con objetivos claros, un camino de hitos que vayan alertando de la consecución, o no, de los objetivos y un sistema eficiente de adaptación a los cambios, partiendo de un plan completo y estructurado de comunicación y difusión a nivel nacional.

Esta estrategia debería tener en cuenta los siguientes principios:

1. **Utilizar métodos y medios ligados a** las ciencias de la **comunicación** ampliamente entendidas.

2. **Segmentar las audiencias** de población con base en la sociología. Y en el terreno empresarial/profesional, centrar las acciones en autónomos y pymes, segmentando por tamaños y por actividad.

3. **Ligar las acciones** concretas de concienciación **con valores éticos y principios**: libertad, responsabilidad, honestidad/ honradez, respeto, trabajo bien hecho, compañerismo, amistad, solidaridad...

3.2.2. Eje 2. Potenciar actuaciones encaminadas al incremento de la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional

Medida Estrategia Nacional de Ciberseguridad 2:
Potenciar actuaciones encaminadas al incremento de la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional.

Los **riesgos** cibernéticos **evolucionan**, tanto en variedad como en complejidad e impacto. El uso seguro del ciberespacio es una aspiración reconocida en la normativa nacional y europea y, además, una responsabilidad compartida, en la medida en que unas buenas o malas prácticas en el uso de STIC de unos repercuten en la ciberseguridad de todos.

Ante este hecho, tal y como determina nuestra Estrategia de Seguridad Nacional 2017, los **sectores público y privado deben colaborar** en la mejora continua de la vigilancia y protección eficaz de sus STIC frente a las ciberamenazas. Sin embargo, la defensa de los ciudadanos y las empresas no puede limitarse a confiar en el uso responsable de la tecnología, ni en la eficacia de las eventuales medidas de autoprotección que puedan tomar. Antes bien, deben **diseñarse espacios de colaboración público-privados** para proponer desarrollar y difundir **sistemas cooperativos para la ciberdefensa activa** de estos agentes.

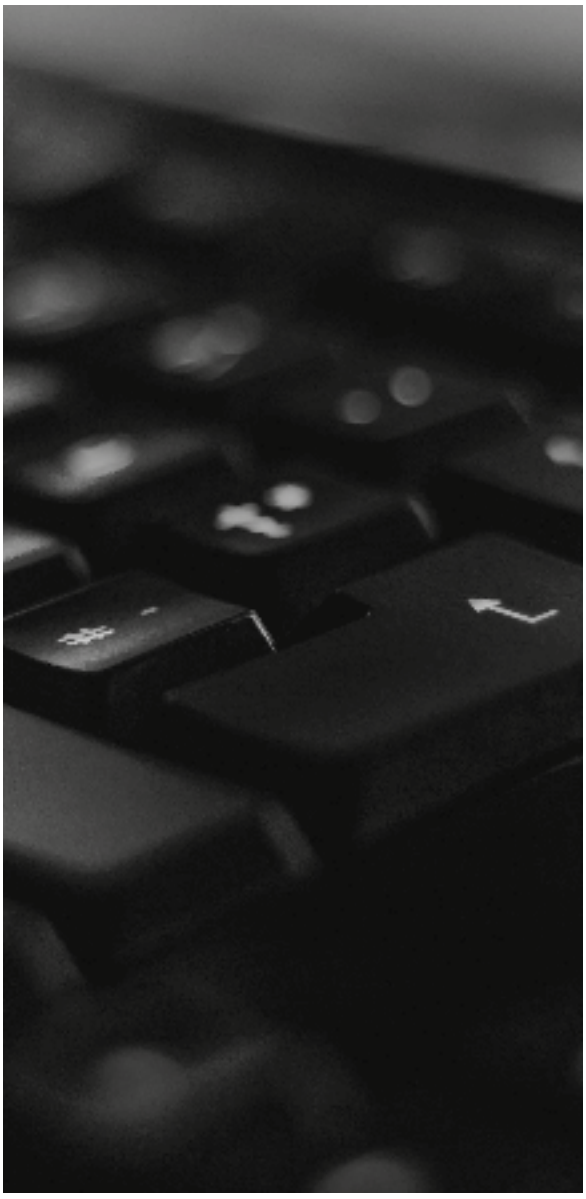
Este objetivo solo puede alcanzarse a través de una verdadera **cultura de ciberseguridad**, que **aglutine medidas técnicas y organizativas, preventivas y reactivas**. El fomento de esta cultura requiere contar con una sociedad más y mejor conocedora de las, cada vez mayores, más cambiantes y complejas, amenazas y desafíos a los que se enfrenta. Sobre la base del principio de responsabilidad compartida, todos los agentes involucrados deben fomentar continuas acciones de sensibilización, de concienciación, de formación y de capacitación en competencias digitales, entendiendo la ciberseguridad como un elemento más de responsabilidad social.

Por otra parte, sería deseable disponer de un **marco jurídico** que establezca expresamente el **alcance de la corresponsabilidad**, para que Administración, operadores y ciudadanos asuman, cada uno en su medida, la responsabilidad de su seguridad mediante acciones concretas de planificación y protección.

El objetivo de estas iniciativas debe ser **fomentar** la asunción de un **rol responsable** por parte de la **ciudadanía** en su conjunto en todas las actuaciones de las cuales pueden derivar riesgos relacionados con el uso de las nuevas tecnologías.

3.2.3. Eje 3. Impulsar iniciativas y planes de alfabetización digital en ciberseguridad

Medida Estrategia Nacional de Ciberseguridad 3: Impulsar iniciativas y planes de alfabetización digital en ciberseguridad



La mayoría de los expertos señalan que los **usuarios** forman el **eslabón más débil** de la cadena de gestión de riesgos de ciberseguridad, hecho que lamentablemente se potencia por el escaso esfuerzo que se realiza, a efectos generales, en su formación y concienciación.

El Consejo de Derechos Humanos de las Naciones Unidas, a través del Documento A/HRC/32/L.20[29], sitúa el **acceso a Internet como un derecho fundamental** por ofrecer grandes oportunidades para una educación asequible e inclusiva a nivel mundial, y subraya la necesidad de abordar la alfabetización digital y la brecha digital. Del mismo modo, exhorta a todos los Estados a asegurar la libertad y la seguridad en la Red para que pueda seguir siendo un motor enérgico del desarrollo económico, social y cultural.

En este mismo sentido, la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD)[30], en su artículo 81 establece el **derecho a acceder a Internet** independientemente de su condición personal, social, económica o geográfica, garantizando acceso universal, asequible, de calidad y no discriminatorio para toda la población, al tiempo que se promulga el derecho a la seguridad y a la educación digital.

Por tanto, toda la **formación y alfabetización** en el uso de las TIC y de Internet debe ir acompañado, indisolublemente, por la **instrucción** en materia de ciberseguridad.

[29] https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf

[30] https://boe.es/buscar/act.php?id=BOE-A-2018-16673

3.2.4. Eje 4. Ciberseguridad como una buena práctica empresarial

Medida Estrategia Nacional de Ciberseguridad 4:
Promover la difusión de la cultura de la ciberseguridad como una buena práctica empresarial, y reconocer la implicación de las empresas en la mejora de la ciberseguridad colectiva como responsabilidad social corporativa.

El compromiso con una protección efectiva de los sistemas y datos que soportan la actividad económica puede representar la base de la **confianza digital en un mercado multicanal dinámico y plural**.

El sector privado debe embeber la ciberseguridad en todos sus procesos de negocio. La **seguridad desde el diseño** es uno de los paradigmas que la Unión Europea ha asumido como criterio de actuación base en el desarrollo de la regulación comunitaria en materia de protección de datos.

Por extensión, este paradigma debería ser parte integrante de todas las metodologías para el diseño de los procesos. En consecuencia, debería ser también requisito imprescindible de todos sus modelos de evaluación.

Solo un sector privado capaz de incorporar la ciberseguridad en su modelo de gestión y operación puede asegurar la sostenibilidad del sistema económico y productivo a largo plazo. El soporte regulatorio debe tutelar al ciudadano estableciendo los límites de la competencia entre los operadores para evitar posibles fallos del mercado.

34

3.2.5. Eje 5. Ciberseguridad y deinformación

Medida Estrategia Nacional de Ciberseguridad 5:
Promover un espíritu crítico en favor de una información veraz y de calidad, y que contribuya a la identificación de las noticias falsas y la desinformación.

Si bien los actores de las **campañas de desinformación** utilizan también el ciberespacio para sus fines, el tratamiento en la seguridad nacional de esta amenaza no debe considerarse únicamente desde la perspectiva de la gestión de riesgos de ciberseguridad, ya que es una amenaza transversal y puede tener implicaciones en diversos ámbitos, a los que utiliza como medio conductor o como vector iniciador o desencadenante.

En este sentido, para **abordar los desafíos** de las campañas de desinformación, es de vital importancia la **acción conjunta y los planes existentes a nivel europeo**, como el Plan de Acción contra la Desinformación y el Plan de Acción para la Democracia Europea, que contempla la promoción de unas elecciones libres y justas, y la libertad y el pluralismo de los medios de comunicación, además de la necesidad de contrarrestar la desinformación, dando respuestas políticas a fenómenos que incluyen las operaciones de influencia en la información o la interferencia extranjera en el espacio informacional y planteando la posibilidad de imponer sanciones a los responsables.

Por otro lado, hay que tener en cuenta las acciones que se realizan en el marco del cumplimiento del Código de Buenas prácticas por parte de las plataformas y su abordaje desde la perspectiva de la comunicación estratégica en un entorno de **colaboración con expertos de la sociedad civil y el sector privado** en la lucha contra las campañas de desinformación, en el que participan medios de comunicación, la academia, las plataformas, los *think tanks* y otros expertos en la materia.

3.2.6. Eje 6. Concienciar a directivos de las organizaciones

Medida Estrategia Nacional de Ciberseguridad 6:
Concienciar a directivos de organizaciones, a los efectos de que habiliten los recursos necesarios y promuevan los proyectos de ciberseguridad que sus entidades puedan necesitar.

Pese a que son las grandes empresas las que llevan a cabo un mayor número de iniciativas relacionadas con la ciberseguridad, en general aún no existe la conciencia por parte de los directivos de las empresas sobre la correlación de la seguridad con la continuidad de negocio, las iniciativas de recuperación ante desastres o la confiabilidad de la misma.

Tampoco está asumida culturalmente la idea de que la seguridad es responsabilidad de todos los empleados y áreas, y que no puede circunscribirse la responsabilidad y ejecución de acciones únicamente a los departamentos de ciberseguridad o de TI. Para llevar a cabo un cambio cultural de esta magnitud, es preciso que cualquier solución se vaya imponiendo desde la dirección hasta el último trabajador de la compañía.

En definitiva, la digitalización de los procesos y capacidades supone una gran oportunidad, pero también presenta riesgos que deben analizarse y gestionarse. El principal vector de cambio de las organizaciones son sus directivos. Por ello resulta esencial que las iniciativas en materia de cultura de ciberseguridad pasen por su compromiso y concienciación. Para ello deben proyectarse acciones y medidas **específicas**.

Por último, debería prestarse una atención especial a la concienciación y puesta a disposición de herramientas de ciberseguridad para los directivos de las **pymes**, debido a que en general disponen de menos medios y tienen un menor grado de conocimiento en la materia, además de no sentirse, en general, blanco potencial de ciberataques.

3.2.7. Eje 7. Centros de enseñanza

Medida Estrategia Nacional de Ciberseguridad 7:
Promover la concienciación y formación en ciberseguridad en los centros de enseñanza adaptada a todos los niveles de formación y especialidades.

El avance digital en los centros de enseñanza hace que hoy en día estén expuestos a los mismos riesgos tecnológicos que cualquier organización o empresa. Denegaciones de servicio, robo de datos, espionaje y aprovechamiento financiero son algunos de los escenarios y posibilidades a los que los centros se encuentran expuestos. Es sabido que los centros de enseñanza son conocidos blancos para los ciberataques e incluso de las amenazas internas (alumnos con intención de tener alguna ventaja de forma ilícita). Por otra parte, el incremento de la enseñanza en remoto favorece riesgos añadidos, como el acceso no seguro a herramientas tecnológicas y datos de los centros.

En este sentido, y dado que la educación es una materia transferida a las Comunidades Autónomas, es fundamental incrementar la colaboración con sus consejerías, a fin de difundir las campañas de concienciación en todos los centros educativos del país (educación primaria, secundaria y universidad).

A la hora de diseñar estas campañas, ha de tenerse presente que han de dirigirse tanto a los centros de enseñanza de cualquier tipo (Universidades, Institutos de Educación Secundaria y Formación Profesional o Centros de Educación Primaria), como a los profesores y alumnos.

En particular, la labor del profesorado en este caso es básica, especialmente en las etapas no universitarias, por su extraordinaria capacidad para actuar como catalizadores y facilitadores de información. De ahí la necesidad de formarles en la materia para que, a su vez, y de forma transversal, puedan sensibilizar a los padres y alumnos de un buen uso de todo tipo de herramientas, plataformas y dispositivos.

3.2.8. Eje 8. Medios de comunicación - Ciudadanos, menores y colectivos en riesgo de exclusión social

Medida Estrategia Nacional de Ciberseguridad 8:
Buscar y reconocer la colaboración y participación de medios de comunicación, para lograr un mayor alcance en las campañas dirigidas a ciudadanos y, en especial, a menores de edad.

La comunicación, en sus distintas vertientes, se erige como protagonista y como herramienta indispensable para la concienciación y la divulgación de la cultura de la ciberseguridad en España, máxime en un momento en el que la ciudadanía está inmersa en una serie de cambios muy importantes en su comportamiento, entre los que se encuentra la digitalización en todos sus ámbitos: trabajo, ocio, consumo, etc.[31]

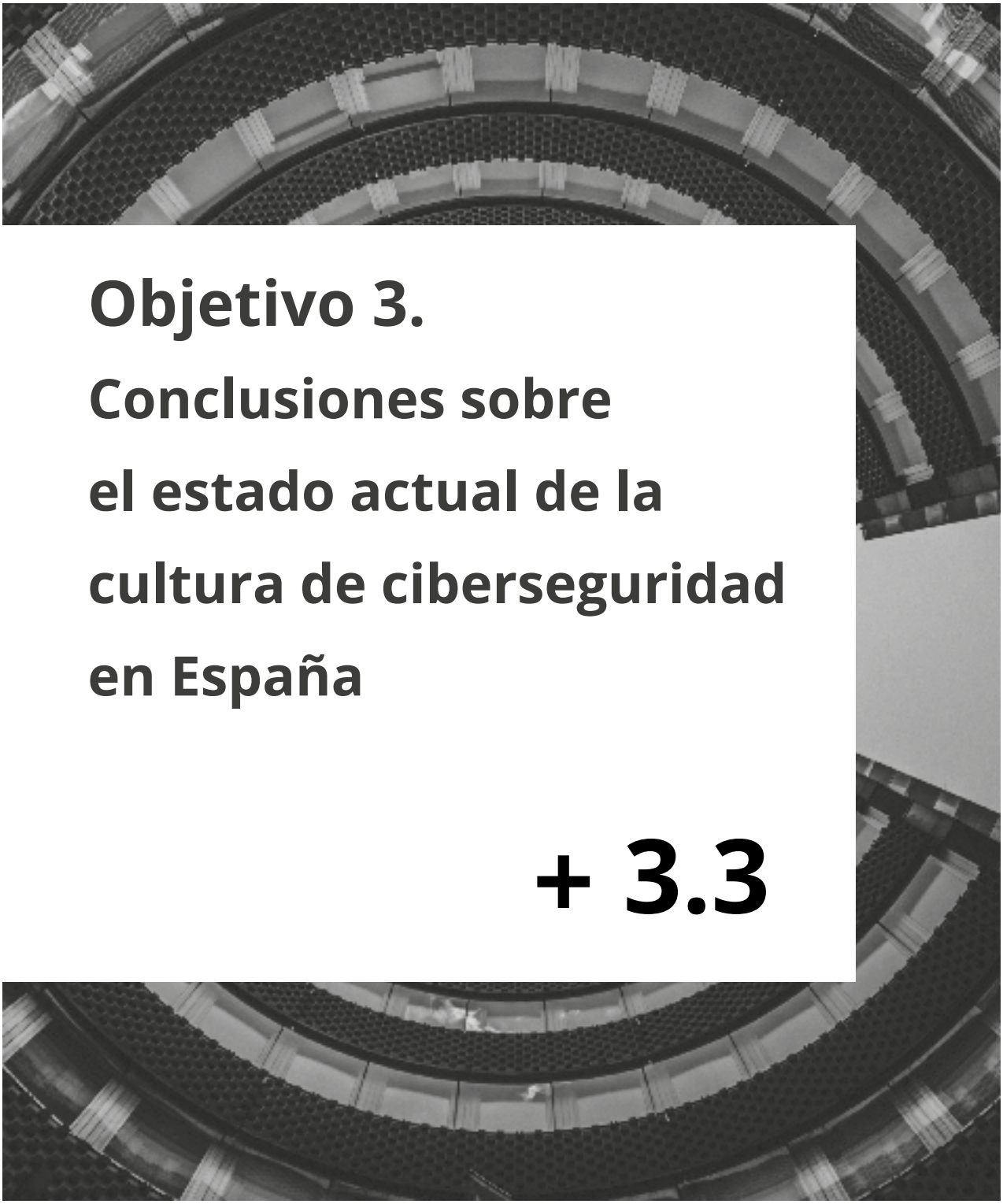
En este sentido, el papel de los medios de comunicación, en su concepción más amplia, sigue siendo un factor decisivo a la hora de influir en el cambio de conductas, la formación de la opinión pública y en lograr la máxima repercusión y alcance de cualquier campaña, sea cual sea el público objetivo al que se quieran dirigir los mensajes (en este caso, la ciudadanía, y particularmente los menores de edad y colectivos en riesgo de exclusión social).

Además de involucrar a los medios de comunicación periodísticos, se debería buscar también la de otros medios o procedimientos alternativos y fiables, de modo que se utilicen los canales y herramientas más adecuados al público objetivo.

Para conseguir mayor impacto en las campañas dirigidas a menores, deberían personalizarse estableciendo dos tramos de edad: hasta 13 años y entre 13 y 18 años. Respecto a este colectivo, conviene resaltar la importancia de los modelos o ejemplos de personas a seguir e *influencers*, así como los nuevos canales de comunicación basados en redes sociales para buscar el máximo impacto y llegada en los mensajes.

La identificación extensa y pormenorizada de los **colectivos de exclusión social** permitirá realizar acciones de comunicación más dirigidas y en colaboración con los organismos y referentes.

[31] Estudio de Deloitte: Perspectivas sobre el comportamiento del consumidor. Camino hacia la recuperación (30 abril 2020). https://www2.deloitte.com/content/dam/Deloitte/es/Documents/bienes-consumo-distribucion-hosteleria/Deloitte-ES-consumer-perspectivas-comportamiento-consumidor.pdf



Objetivo 3.
Conclusiones sobre el estado actual de la cultura de ciberseguridad en España

+ 3.3

Se aprecia cierta desconexión entre las numerosas iniciativas dirigidas a la concienciación y sensibilización, que, por otra parte, no son evaluadas ni reportadas. Como consecuencia, no existe una visión global y exacta del **estado de la cultura de ciberseguridad** en la sociedad, así como del impacto de las iniciativas emprendidas.

Algunas empresas (sobre todo las grandes y multinacionales) han apostado por la ciberseguridad como una buena práctica empresarial; sin embargo, no es una práctica extendida en pequeñas organizaciones: pequeños ayuntamientos, pymes y microempresas. Puede observarse un desconocimiento de los ciber riesgos a los que se exponen los profesionales autónomos y las pequeñas empresas de **ámbitos sectoriales específicos** (jurídico o sanitario, por ejemplo).

Pese a que son las grandes empresas las que llevan a cabo un mayor número de iniciativas relacionadas con la ciberseguridad, en general, aún no existe la conciencia por parte de los directivos de las empresas sobre la correlación de la seguridad con la continuidad del negocio, las iniciativas de recuperación ante desastres o la confiabilidad de la misma.

En España, la extensión de los programas de *bug bounty* todavía es reducida, aunque los resultados suelen ser muy positivos y lo mismo ocurre con los programas de *mentoring* con empresas.

Además de que la ciberseguridad en los actuales diseños curriculares es insuficiente, las actividades de concienciación en ciberseguridad en los centros de enseñanza son puntuales y no acaban de llegar a su público objetivo, pese a que existe abundante material a disposición.

Algunas de las principales iniciativas y servicios para impulsar la cultura de ciberseguridad son desconocidas para la ciudadanía. La sociedad, en general, desconoce proyectos como Internet Segura for Kids (IS4K), la existencia del teléfono de ayuda 017, la Oficina de Seguridad del Internauta o cuál es el CERT/CSIRT de referencia al que acudir en caso de tener un ciberincidente.

Existen iniciativas específicas sectoriales e intersectoriales, pero no se ha identificado ninguna relevante para colectivos, como el de personas mayores y personas en situación de reinserción. También son escasas las iniciativas encaminadas al

incremento de la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional; las existentes en alfabetización, resultan inconexas.

Respecto a las campañas de comunicación, para alcanzar la máxima difusión será preciso segmentar las audiencias para potenciar, desarrollar y difundir el mensaje adecuado, a través de los canales y de las herramientas de comunicación más efectivas, teniendo en cuenta que los diferentes canales proporcionan lenguajes y maneras distintas de acceder a cada colectivo.

El avance digital en los centros de enseñanza hace que estén expuestos a los mismos riesgos tecnológicos que cualquier organización o empresa, favorecidos por el incremento de la enseñanza en remoto.

Dado que la educación es una materia transferida a las Comunidades Autónomas, es fundamental incrementar la colaboración con sus consejerías, a fin de difundir las campañas de concienciación en todos los centros educativos del país (educación primaria, secundaria y universidad).

El papel de los medios de comunicación, en su concepción más amplia, sigue siendo un factor decisivo a la hora de influir en el cambio de conductas, la formación de la opinión pública y en lograr la máxima repercusión y alcance de cualquier campaña. No obstante, la colaboración y participación de **medios de comunicación** en las campañas de ciberseguridad es muy limitada.

Deben tenerse en cuenta también otros medios o procedimientos de comunicación alternativos y fiables, de modo que se utilicen los canales y herramientas más adecuados al público objetivo.

En particular, hay que resaltar la importancia de los modelos o ejemplos de personas a seguir e *influencers*, así como de los nuevos canales de comunicación basados en redes sociales, para buscar el máximo impacto y llegada en los mensajes.

La identificación extensa y pormenorizada de los colectivos de exclusión social permitirá realizar acciones de comunicación más dirigidas y en colaboración con los organismos, referentes y medios de comunicación que tengan mejor enfoque y adaptación a cada uno de ellos.

Objetivo 4. Propuesta de acciones

+ 3.4

A la vista de las iniciativas emprendidas tanto en el ámbito nacional como internacional, en base a los Ejes de Acción propuestos y a las conclusiones del anterior apartado, resulta evidente la necesidad de adoptar una serie de actuaciones dirigidas a incrementar la eficacia y la eficiencia para mejorar la cultura de ciberseguridad nacional y promocionar una conciencia social compartida, a cuyo fin se formula la siguiente propuesta de acciones concretas, a poner en marcha desde diferentes instancias:

3.4.1 Acciones para potenciar la Concienciación

A. **Formación**. Como vector de concienciación, puede facilitarse su acción agrupando todos los cursos que se lleguen a realizar sobre temáticas diferentes, guías de utilidad para los receptores, laboratorios y simulacros que hagan entender bien los conceptos, pequeños tutoriales sobre ámbitos concretos, etc.

B. **Sensibilización**. Grandes campañas nacionales de comunicación destinadas al público en general, donde se pueden agrupar folletos, vídeos, salvapantallas, pequeñas animaciones, productos de *merchandising*, ilustraciones gráficas, consejos, infografías, cartelería en general, tiras cómicas, etc.

C. **Comunicación**. A través de notificaciones a los usuarios, boletines, alertas o eventos de interés, *banners* en sitios web de interés, etc.

D. **Juegos educativos**. Con la creación de concursos digitales, juegos de estilo *escape room*, clásicos pasatiempos atemporales, escenarios de 360 grados, experiencias en realidad virtual, juegos de acción de plataformas clásicos, etc.

E. **Apoyo o consultas**. A través de FAQs, creación de una Wikipedia de ciberseguridad, bibliotecas de aplicaciones de ciberseguridad, así como de contenidos y recursos interesantes, creación de buzones de preguntas y/o sugerencias, etc.

F. **Identificación y captación del talento.** Dirigida a generar un sentimiento de urgencia entre la población como catalizador que acelere los procesos formativos y de concienciación.

3.4.2. Acciones dirigidas al incremento de la corresponsabilidad y obligaciones de la sociedad

En este ámbito, destacamos iniciativas orientadas a impulsar la diligencia debida como un deber de todos los individuos y organizaciones.

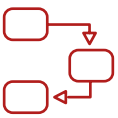
A. Elaboración de un **Código de Ciberseguridad para el Ciudadano** donde se recojan las buenas prácticas para el uso seguro y la protección de los sistemas y tecnologías de la información. El respeto y aplicación de las medidas y mecanismos de protección recogidos en el código valdría para demostrar la diligencia debida del individuo u organización frente a los posibles daños ocasionados a terceros disminuyendo la responsabilidad por daños y perjuicios.

B. Impulso de un **Ciber Seguro de Responsabilidad Civil** para los daños ocasionados a terceros, personas o bienes como consecuencia de la falta de seguridad de los sistemas y tecnologías operados por un individuo u organización.

C. Institución de un **Servicio Público de Ciber-Diagnóstico** que permita analizar la seguridad de las políticas y configuraciones establecidas en los sistemas y tecnologías de la información de particulares y organizaciones. Este servicio permitiría a la ciudadanía poder verificar de forma remota y relativamente sencilla la configuración de seguridad de los sistemas (nivel de parcheado de S.O., actualización de aplicaciones, configuración de antivirus, configuración de personal FW, políticas de seguridad, etc.).

D. Impulsar una **Reforma Legal** para disciplinar la obligaciones y responsabilidad del individuo y de las organizaciones en la protección efectiva de los sistemas y tecnologías de la información de las cuales son propietarios o usuarios a cualquier título. Esta iniciativa debe estar encaminada a desarrollar criterio de diligencia debida en el ámbito de la ciberseguridad.

E. Fomentar la inclusión de **cursos, certificaciones y exámenes** en los diferentes ciclos formativos del sistema de educación español para reforzar el mensaje de corresponsabilidad y diligencia debida.



F. **Planes de reacción** entre la población y campañas de información pública diseñadas para preparar a la población en la respuesta y comportamiento ante ciberataques masivos.

3.4.3. Acciones para impulsar planes de alfabetización digital en ciberseguridad

A. Mensajes de alfabetización en las empresas

Transmitir por todos los medios disponibles a los empleados que son la primera línea de defensa en el propósito y objetivo de gestionar adecuadamente los riesgos de ciberseguridad.

B. Promoción de la ciberseguridad entre los profesionales de la seguridad

Promover y apoyar toda clase de foros y eventos de cualquier naturaleza, dedicados al tratamiento de cuestiones de ciberseguridad entre profesionales de la seguridad de cualquier ámbito.

C. Mensajes de alfabetización para el público en general

Sea cual sea el segmento de población elegido, existen una serie de recomendaciones básicas que no pueden hurtarse: elección de contraseñas, antivirus, actualización del software y copias de seguridad.

A la hora de elaborar el mensaje, es efectivo ejemplificar con ataques notorios que se hayan producido por no seguir estas recomendaciones y buscar lemas efectivos.

En el ámbito empresarial, sería recomendable contar con la colaboración de las diferentes organizaciones y asociaciones empresariales, así como con los colegios profesionales.

Respecto a otros colectivos, como niños, convendría buscar la complicidad de las AMPAS y sus distintas federaciones y confederaciones, así como las consejerías de Educación de las Comunidades Autónomas. Para los jóvenes y, sobre todo adultos, las organizaciones de consumidores y usuarios serían excelentes aliados. Finalmente, para las personas de más edad, las asociaciones de jubilados podrían prestar un gran servicio. La FEMP puede también jugar un papel relevante en la alfabetización.

A efectos generales, **las infografías** son muy recomendables a tal fin, al igual que los **vídeos cortos**, para centrar la atención en un consejo concreto. En el escenario empresarial, conviene tener en cuenta que **los manuales de seguridad, en formato digital o en papel** deben ser breves, precisos y con ilustraciones sencillas.

3.4.4. Acciones para adoptar la ciberseguridad como una buena práctica empresarial

A. Reformar el **código de buen gobierno** para entidades cotizadas para incluir la ciberseguridad como un requisito de gestión de la organización a través de una Política de Seguridad aprobada por la dirección.

B. Incluir **indicadores de gestión de** la **ciberseguridad** en los modelos de Memoria de Responsabilidad Empresarial (RSC).

C. Desarrollo de **portales para empleados** y creación de **canales de información**, con iniciativas motivadoras (por ejemplo, ciber agentes), donde los empleados puedan acceder a información, formación y otra serie de recursos útiles para el desarrollo de su actividad profesional.

D. Promover como evidente **buena práctica** la **obtención de certificaciones** de gestión de la ciberseguridad, dar preferencia a la adquisición de productos TIC y de ciberseguridad certificados (cuando existan) y a la contratación de servicios certificados (cuando existan).

E. **Instituir incentivos y créditos fiscales** para las empresas españolas que inviertan en tecnologías y programas de ciberseguridad que tengan como objetivo incrementar la resiliencia de la organización.

F. Estimular la **organización coordinada de ejercicios de ciberseguridad** nacional a escala sectoriales e intersectoriales en ambientes de confianza público-privados.

G. Creación de **foros de comunidades integradas** formadas por los equipos de ciberseguridad de los centros de enseñanza superior y de empresas.

H. Puesta en marcha de **actuaciones de concienciación por sectores** de actividad.

I. Explorar la creación de un **marco general de comunicación de vulnerabilidades**.

J. Incluir la **ciberseguridad en** los **planes de formación** para empleados e impulsar el desarrollo de programas de *mentoring* mediante la creación de una guía que facilite su ejecución.

K. **Apoyar a los responsables de seguridad** de la información en las empresas en su actuación como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, facilitándoles guías y contenidos para la elaboración manuales internos.

L. **Promover y apoyar** toda clase de **foros y eventos** de cualquier naturaleza, dedicados al tratamiento de cuestiones de ciberseguridad entre profesionales de la seguridad de cualquier ámbito.

3.4.5. Acciones para concienciar a directivos de las organizaciones

A. **Visibilidad y difusión de incidentes de ciberseguridad**. Se requiere mayor transparencia y normalidad en la comunicación de incidentes.

B. **Anuncios en prensa económica**. Puesto que los directivos son consumidores de prensa económica en mayor grado que la población general, se propone llevar a cabo campañas de comunicación específicas para directivos en los principales medios nacionales de esta área.

C. **Campañas en redes sociales**. Si bien las redes sociales son utilizadas por la población general, existen algunas que, por sus características, como por ejemplo LinkedIn, es empleada con mayor intensidad por los directivos. Se propone por tanto llevar a cabo acciones de comunicación a este respecto.

D. **Capilaridad y prescripción**. Contar con entidades e instituciones por sectores que actúen como embajadores de seguridad y extiendan el conocimiento, confiabilidad y credibilidad en las acciones necesarias.

E. **Acciones formativas específicas para directivos**. INCIBE dispone en su sitio web de numerosas herramientas formativas para ciudadanos y empresas. Dentro de las herramientas para empresas, se encuentran una serie de vídeos formativos por sectores de actividad. Sin embargo, faltan herramientas de esta índole específicas para directivos.

F. **Formación específica en ciberseguridad en las escuelas de negocio**. Las escuelas de negocio son una opción a la que recurren frecuentemente las empresas para formar a sus directivos.

G. **Creación de puntos de atención a pymes especializados en ciberseguridad**. Se propone un modelo similar al de los Puntos de Atención al Emprendedor[32] del Ministerio de Industria, Comercio y Turismo, pudiendo, incluso, integrarse en estos mismos puntos.

H. **Impulsar la implantación de acciones básicas de seguridad**. Homogeneizar desde la administración pública y en relación con la industria y el sector, los conceptos y entendimiento sobre las medidas, controles, tipología de productos y servicios que permiten incrementar el nivel de seguridad en las empresas.

I. **Fomento de la ciberseguridad en la alta dirección**. Se deberían fomentar los comités de seguridad, en los que debe participar el RSI, de forma que escalen a la alta dirección todos los aspectos relativos a la ciberseguridad, sirviendo además como medio de coordinación.

[32] https://paeelectronico.es/es-es/CanalPAE/Paginas/QueEsPAE.aspx

3.4.6. Acciones para adoptar en el ámbito de la enseñanza

A. Centros de enseñanza

Universidades

Fomentar la creación de departamentos de ciberseguridad en las universidades. En este sentido, se recomienda difundir todos los recursos puestos a disposición de la red académica a través de INCIBE y Red.es-Rediris, y del Centro Criptológico Nacional para la protección de las universidades públicas, en colaboración con las Consejerías de Educación de las distintas autonomías y la CRUE (Conferencia de Rectores de las Universidades Españolas). Del mismo modo, se aboga por asociar por defecto a todos los dispositivos que vayan a ser utilizados por los alumnos (numerosas universidades ceden ordenadores a los estudiantes) un pequeño curso de sensibilización y principios básicos de ciberseguridad antes de poder utilizarlo, así como la repetición de cursos de forma periódica, que puede ser anual a modo de recuerdo de la información. Solo podrán acceder al mismo aquellos alumnos que lo hayan realizado.

Creación de foros de investigación universitaria que permitan canalizar el potencial universitario para el desarrollo de formación concreta en materias específicas relacionadas con la cultura de ciberseguridad.

Institutos de Educación Secundaria y Formación Profesional

Habilitar en las plataformas virtuales a las que acceden tanto alumnos como profesores y padres consejos de ciberseguridad, juegos o algún material al que puedan acceder todos los interesados. Proveer guías y políticas dirigidas a la formación sobre la seguridad en dispositivos, correo electrónico, cuentas de usuarios, seguridad en videoconferencias y otras materias como asegurar las conexiones de Internet en casa.

Centros de Educación Primaria

Enseñar buenos hábitos de ciberseguridad y formación sobre el *ciberbullying* y el ciberacoso a los maestros y padres es clave, ya que serán los encargados de proteger a los alumnos. Los miembros de la comunidad escolar también deben saber a quién han de informar en caso de incidente y qué decisiones deben tomar.

En todos los casos, y en función del recurso disponible, convendría dar publicidad en los centros educativos a iniciativas ya existentes como el Mes Europeo de la Ciberseguridad[33] promovido por ENISA, el Día de la Ciberseguridad (30 de noviembre), el Día de Internet Segura[34], Pantallas Amigas[35], etc.

El sector público debe colaborar con la enseñanza impartiendo conferencias en los centros y ofreciendo clases innovadoras y dinámicas sobre ciberseguridad que fomenten la discusión de conceptos básicos. Posibilidad de coordinar desde el Foro Nacional de Ciberseguridad.

B. Profesorado

Para facilitar su acción como catalizadores y facilitadores de información, convendría divulgar algunos de los recursos para el aprendizaje en línea que mantienen diferentes organismos:

· Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF)[36].

· Asegura TIC[37] (seguridad del menor en medios digitales) del Ministerio de Educación y Formación Profesional.

· INCIBE: Internet Segura for Kids (IS4K)[38] y la Oficina del Internauta (OSI)[39], así como su programa de Sectoriza2 que incluye a la Educación[40].

· Agencia Española de Protección de Datos que tiene en la Educación y Menores alguna de sus áreas de actuación

· Centro Criptológico Nacional. Guías, informes y ciberconsejos para el uso seguro de diferentes herramientas y plataformas.

[33] ECSM (cybersecuritymonth.eu)

[33] Home - Safer Internet Day

[34] https://www.pantallasamigas.net

[36] https://intef.es/recursos-educativos/recursos-para-el-aprendizaje-en-linea/recursos/ciberseguridad/

[37] https://intef.es/aseguratic/

[38] https://www.is4k.es/

[39] https://www.osi.es/es

[40] https://www.incibe.es/sites/default/files/contenidos/SECtoriza2/educacion.pdf

C. Alumnos

· **Cuestionarios interactivos para menores** a través de los cuales se pueda evaluar su nivel de conocimientos acerca de los ciberriesgos y, en base a ello, aportar aquellos contenidos que mejor se adecúen a las necesidades escolares concretas.

· **Incrementar los contenidos de ciberseguridad** en los diseños curriculares, estructurando la educación escolar para impulsar la formación en ciberseguridad, con evaluación y certificaciones por niveles para que los niños vayan acumulando certificaciones que puedan añadir a su currículo particular.

· Crear **bases de datos de conocimiento** en el ámbito de la educación en ciberseguridad, con recursos como *webinars*, *frameworks* o incluso cómics, al objeto de atraer talento infantil hacia estas carreras STEM.

· Potenciar **herramientas que creen conciencia sobre la seguridad cibernética**, como asambleas escolares, concursos, lecciones en el aula, material informativo disponible en sitios web, campañas de redes sociales y otros.

· Ofrecer **cursos básicos de ciberseguridad** a través de las plataformas de las distintas Consejerías de Educación, con certificados.

· Hacer presente la **ciberseguridad en ferias universitarias o de enseñanza**.

· **Concursos** que **contribuyan a crear conciencia y desarrollar el interés** por el mundo de la ciberseguridad, tales como *Capture The Flag* (CTF) o desarrollo de capacidades a través de contenidos lúdicos.

· Habilitar **cursos de verano** en formato presencial, *online* o mixtos para edades comprendidas entre los 8 y los 17 años.

· Elaborar **programas extracurriculares** para que los jóvenes tengan a su disposición juegos online mediante los que desarrollar sus capacidades digitales.

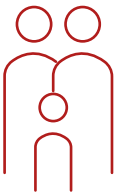
3.4.7. Acciones sobre los medios de comunicación para ciudadanos, menores y colectivos en riesgo de exclusión social

Entre otras acciones, y en función de las audiencias, se proponen:

A. Medios de comunicación

· **Jornadas/talleres** para **periodistas** sobre ciberseguridad, donde conozcan unas buenas prácticas del uso de las nuevas tecnologías.

· **Cortometrajes, series de televisión o largometrajes de ficción** en los que, de un modo u otro, la **ciberseguridad** sea protagonista. Al modo de las actuales series de promoción de cuerpos policiales, poner en marcha acciones de concienciación para el público en general, mediante series de televisión y películas con contenidos ejemplarizantes sobre los riesgos, amenazas, efectos y capacidades de respuesta, públicas y privadas, frente a ciberataques.



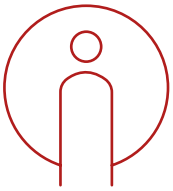
B. Menores de edad

· Identificación de los principales ***influencers*** de nuestro país para que colaboren en la difusión de los mensajes.

· **Creación de "héroes"**, personas que por sus distintas características conecten mejor con los menores y puedan concienciar de los distintos riesgos de la Red.

· Cortometrajes, series de televisión o largometrajes de **animación** en los que, de un modo u otro, la ciberseguridad sea protagonista.

· Plantear una **estrategia de colaboración** a nivel nacional con **Comunidades Autónomas y Ayuntamientos** (FEMP) para llega a todo el país con las campañas.



C. Colectivos en riesgo de exclusión social

· Plantear **campañas con las principales asociaciones**, ONG, foros o colectivos que atienden a cada colectivo.

· Elaborar **campañas en los puntos de acceso a Internet** (bibliotecas, locutorios, cibercafés, etc.).

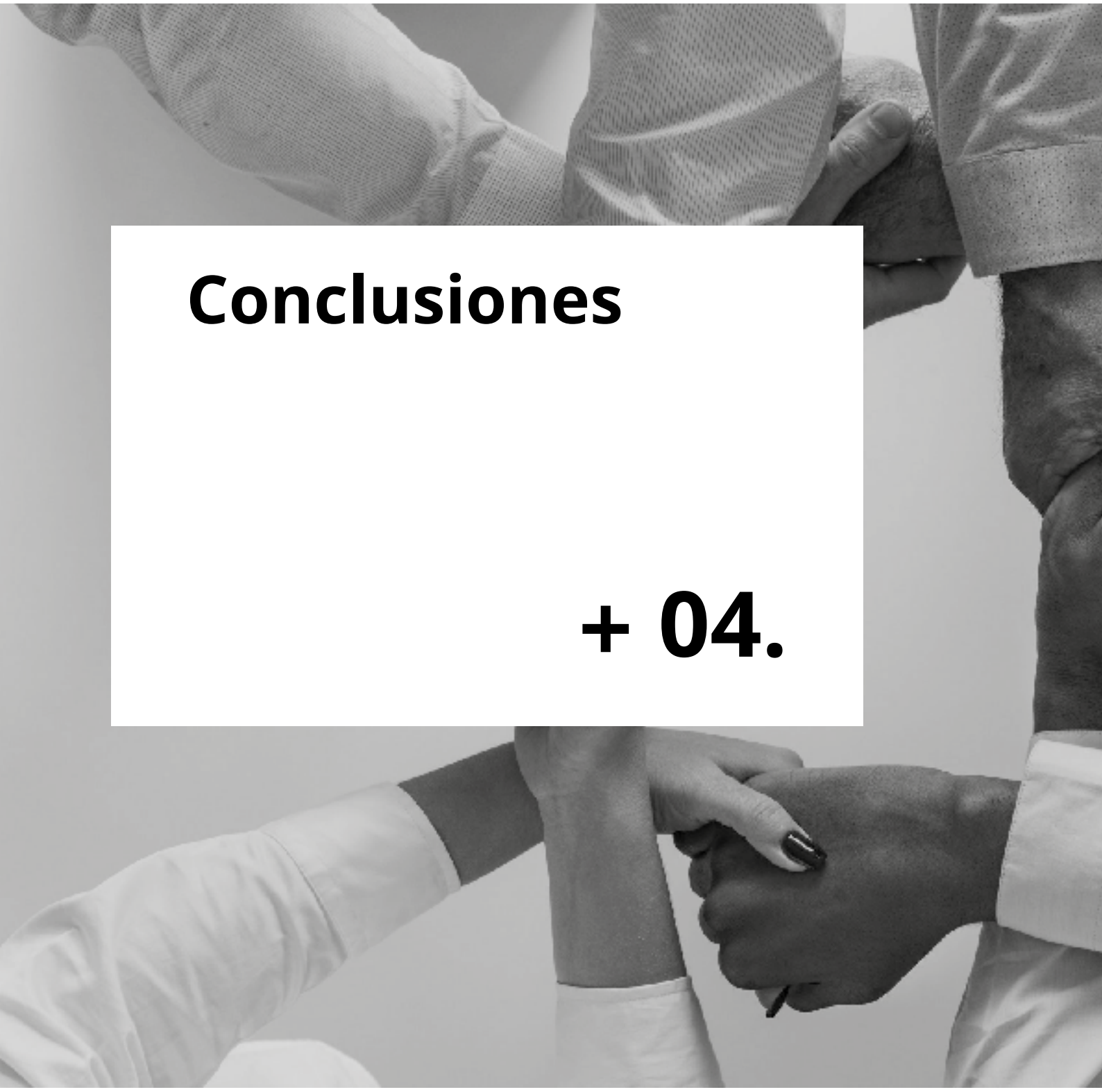
3.4.8. Creación de métricas para conocer el estado de la cultura de ciberseguridad en España

La conclusión principal extraída del estudio de la situación ha sido constatar la **carencia de una visión global y exacta del estado de la cultura de ciberseguridad** en la sociedad, así como del **impacto** de las iniciativas recogidas. En consecuencia, es prioritario definir y poner en práctica unos indicadores y métricas para evaluar el estado actual de la concienciación y cultura en ciberseguridad, así como el impacto de las futuras campañas.

Además de disponer de un repositorio de indicadores obtenido de entre las fuentes conocidas, se ha de decidir cuáles de ellos se van a establecer como referencia y su ponderación, fijando así un sistema de medida objetivo y constante.

Este cuadro de mando formaría parte de una propuesta más global realizada por el Foro Nacional de Ciberseguridad, que se trata de la creación de un **Observatorio para la elaboración y seguimiento del Barómetro Integral de Ciberseguridad**, en la que participe el ecosistema de industria e investigación, los sectores público y privado y la ciudadanía en general, con especial dedicación a un sistema para medición de la cultura de ciberseguridad en España.


,325
Link One
Link Eight
Account Balance



Conclusiones

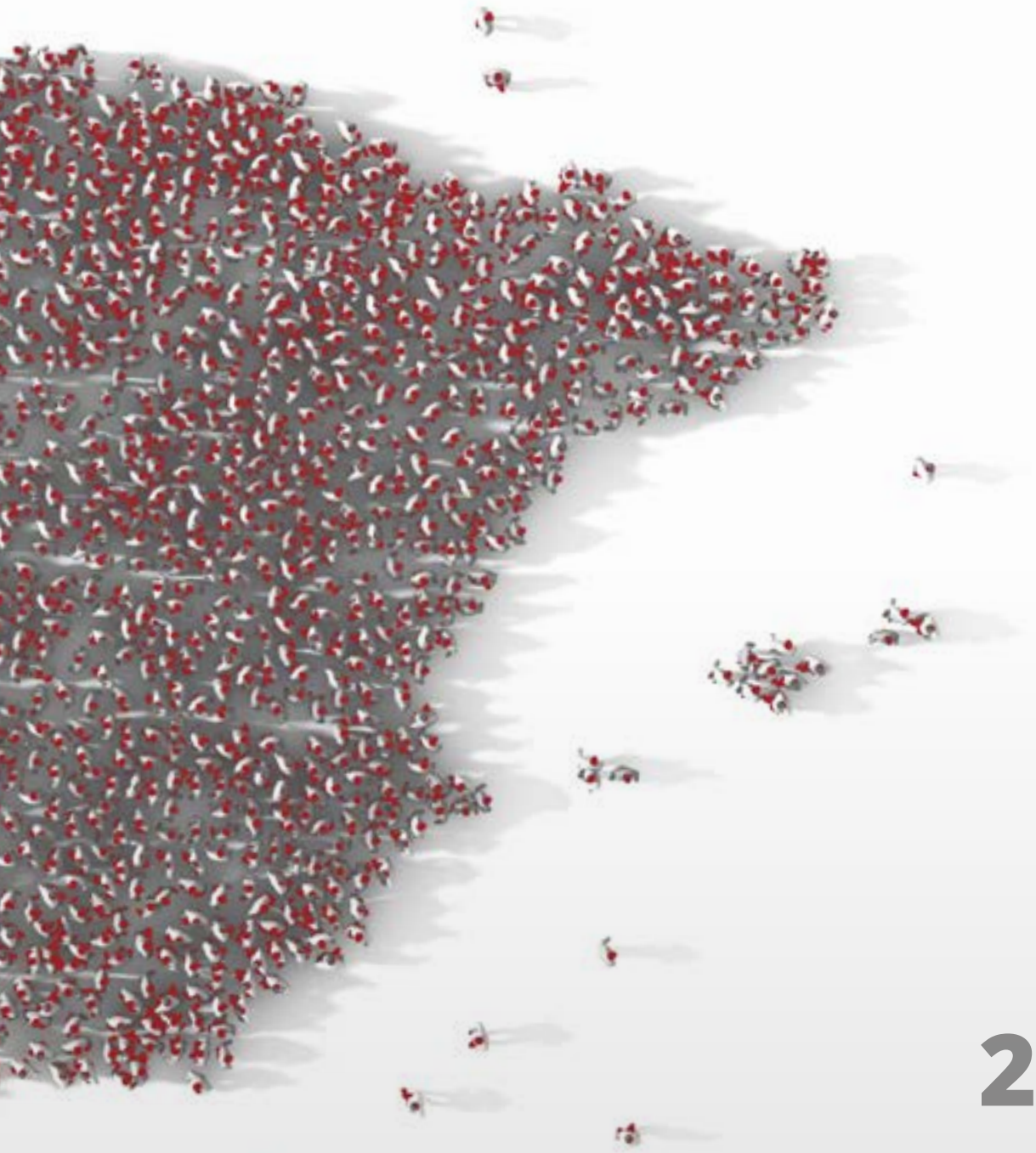
+ 04.

Conclusiones

El proceso de digitalización y transformación digital de nuestra sociedad se ha visto acelerado por la pandemia COVID-19, que ha impulsado la adaptación del sector privado, público y la sociedad en general a una nueva realidad sobre la que se debe sustentar el crecimiento económico, la recuperación y una transformación social a todos los niveles.

Por ello, garantizar la ciberseguridad de este proceso, debe ser una de las prioridades y para ello es imprescindible conocer los riesgos a los que se está expuesto. Así, el fomento de la Cultura de Ciberseguridad constituye uno de los ejes centrales para alcanzar una sociedad más conocedora de las amenazas y desafíos a los que se enfrenta, atendiendo al derecho a disfrutar de un uso seguro y fiable del ciberespacio y a la obligación de contribuir a que así sea.

Para alcanzar este objetivo es imprescindible el compromiso de todos. Por eso, en este Informe y, en línea con la Estrategia Nacional de Ciberseguridad, se proponen una serie de medidas y actuaciones para aumentar el grado de cultura de ciberseguridad en todos los sectores y la sociedad en general e incrementar la coordinación, eficacia y eficiencia de las actuales iniciativas, con el convencimiento que una mayor cultura de ciberseguridad nos hará más fuertes y resilientes ante los desafíos que tenemos que afrontar.



2021

INFORME SOBRE LA INDUSTRIA E INVESTIGACIÓN ESPAÑOLAS EN CIBERSEGURIDAD

FORO NACIONAL DE CIBERSEGURIDAD

Índice

+ Informe sobre la industria e investigación españolas en ciberseguridad

+ Informe sobre la industria e investigación españolas en ciberseguridad

Índice de figuras

Índice de tablas

Introducción

+ 01.

Objetivo

Este Informe, de vocación claramente propositiva, aspira a crear las condiciones para que se desarrollen a nivel práctico las medidas de la Estrategia Nacional de Ciberseguridad referentes a la cooperación público – privada, impulso de la oferta y demanda nacionales en ciberseguridad y reforzamiento de la I+D+i.

El objetivo último, por tanto, es elevar la competitividad de la industria y reforzar el papel de España en el mercado internacional de la ciberseguridad.

Alineamiento estratégico

La Estrategia Nacional de Ciberseguridad se vertebra en torno a cinco grandes objetivos relacionados con seis líneas de acción que, a su vez, se concretan en una serie de medidas encaminadas reforzar el papel que juega la ciberseguridad en el incremento de la competitividad de España y el bienestar de los ciudadanos.

Los **objetivos de la Estrategia Nacional de Ciberseguridad** son los siguientes:

· **Objetivo 1**: Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.

· **Objetivo 2**: Uso seguro y fiable del ciberespacio frente a un uso ilícito o malicioso.

· **Objetivo 3**: Protección del ecosistema empresarial y social de los ciudadanos.

· **Objetivo 4**: Cultura y compromiso con la ciberseguridad y protección de las capacidades humanas y tecnológicas.

· **Objetivo 5**: Seguridad del ciberespacio en el ámbito internacional.

El Informe aborda los objetivos 3 y 4 así como las líneas de acción 4 y 5 relacionadas con ellos, tal y como se plantea gráficamente en la Figura 1:

Figura 1: Líneas de acción de la Estrategia Nacional de Ciberseguridad

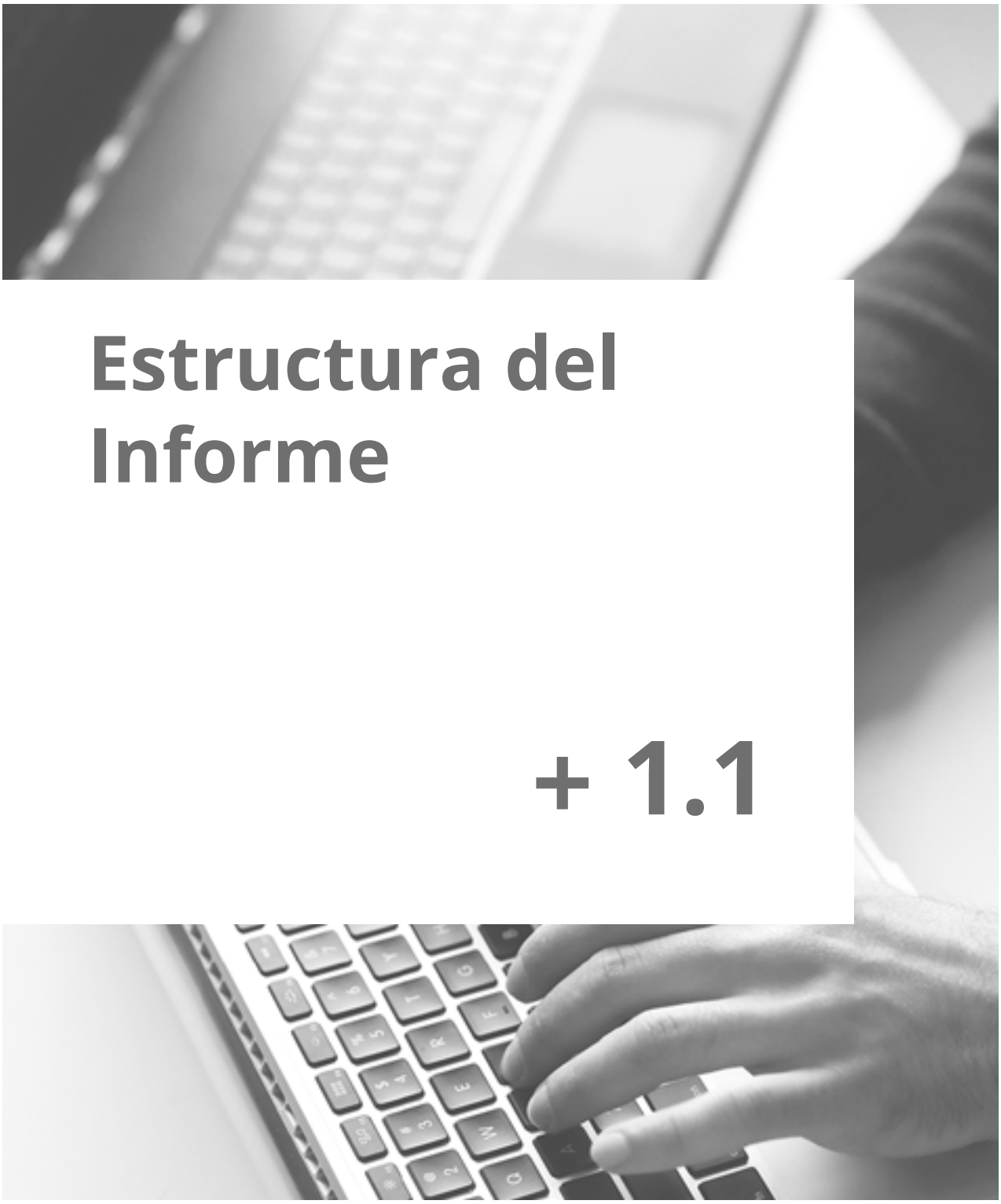
Las siguientes tablas relacionan el conjunto de medidas que han constituido la base de los trabajos.

[Ob_3] Objetivo 3 **Protección del ecosistema empresarial y social y de los ciudadanos**
[LA4] Línea de acción 4 **Impulsar la ciberseguridad de ciudadanos y empresas**
M1. Ofrecer a los ciudadanos y al sector privado un servicio público de ciberseguridad integrado, de calidad y fácil acceso, y que sea un estímulo a la demanda de los servicios que ofrece el sector empresarial de la ciberseguridad.
M2. Impulsar la ciberseguridad en las pymes, micropymes y autónomos mediante la articulación de políticas públicas en ciberseguridad, y especialmente con actuaciones dirigidas al fomento de la resiliencia.
M3. Promover la ciberseguridad para garantizar la privacidad y protección de datos personales dentro del marco de los derechos digitales del ciudadano acorde con el ordenamiento jurídico, promoviendo la protección de la «identidad digital».
M4. Crear mecanismos ágiles y seguros de denuncia para el sector privado y ciudadanos.
M5. Estimular la cooperación entre actores públicos y privados, en particular promoviendo el compromiso de los Proveedores de Servicios de Internet y de Servicios Digitales para mejorar la ciberseguridad. Se impulsará la regulación nacional en este sentido y se implementarán medidas de ciberdefensa activa de ciudadanos y pymes.
M6. Desarrollar mecanismos para la medida agregada del riesgo y su evolución, tanto de ciudadanos como de empresas, para priorizar medidas de ciberseguridad e informar adecuadamente a la sociedad.
M7. Impulsar en el sector empresarial la implantación de estándares reconocidos de ciberseguridad. Estimular, junto con las entidades de normalización nacional e internacional, la creación, difusión y aplicación de mejores prácticas sectoriales en materia de ciberseguridad, incluidos diferentes esquemas de certificación.
M8. Impulsar la implantación de sistemas fiables de identificación electrónica y servicios electrónicos de confianza.
M9. Promover la creación del Foro Nacional de Ciberseguridad, que integre a representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones, organismos sin ánimo de lucro, entre otros, con el objetivo de potenciar y crear sinergias público-privadas, particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

Tabla 1: Medidas asociadas a la Línea de Acción 4 de la Estrategia Nacional de Ciberseguridad

[Ob_4] Objetivo 4 **Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas**
[LA_5] Línea de acción 5 **Potenciar la industria española de ciberseguridad y la generación y retención de talento, para el fortalecimiento de la autonomía digital**
M1. Impulsar programas de apoyo a la I+D+i en seguridad digital y ciberseguridad en pymes, empresas, universidades y centros de investigación, facilitando el acceso a programas de incentivos nacionales e internacionales y mediante programas de compra pública innovadora.
M2. Dinamizar el sector industrial y de servicios de ciberseguridad, incentivando medidas de apoyo a la innovación, a la inversión, a la internacionalización y a la transferencia tecnológica en especial en el caso de micropymes y pymes.
M3. Incrementar las actividades nacionales para el desarrollo de productos, servicios y sistemas de ciberseguridad, y la seguridad desde el diseño, apoyando específicamente aquellas que sustenten necesidades de interés nacional para fortalecer la autonomía digital, y la propiedad intelectual e industrial.
M4. Promover las actividades de normalización y la exigencia de requisitos de ciberseguridad en los productos y servicios de Tecnologías de la Información y de las Comunicaciones, facilitar el acceso a productos y servicios que respondan a estos requisitos, promoviendo la evaluación de la conformidad y la certificación, y apoyando la elaboración de catálogos.
M5. Actualizar (o en su caso desarrollar) marcos de competencias en ciberseguridad, que respondan a las necesidades del mercado laboral.
M6. Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la formación continua, la formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional.
M7. Impulsar la inclusión de perfiles profesionales en ciberseguridad, con especial atención al campo de la investigación.
M8. Detectar, fomentar y retener el talento en ciberseguridad, con especial atención al campo de la investigación.
M9. Impulsar programas específicos de I+D+i en ciberseguridad y ciberdefensa.

Tabla 2: Medidas asociadas a la Línea de Acción 5 de la Estrategia Nacional de Ciberseguridad



Estructura del Informe

+ 1.1

El informe sobre la industria e investigación españolas en ciberseguridadanaliza en profundidad la industria e investigación en ciberseguridad desde los siguientes puntos de vista:

· **Conocimiento aplicado de ciberseguridad**. Bajo este epígrafe se han estudiado los siguientes aspectos:

  · cadena de valor de la ciberseguridad en España,
  · taxonomía, y
  · barómetro: indicadores de madurez del sector

· **Retos de ciberseguridad de las pymes** en su rol de demandantes de productos y servicios.

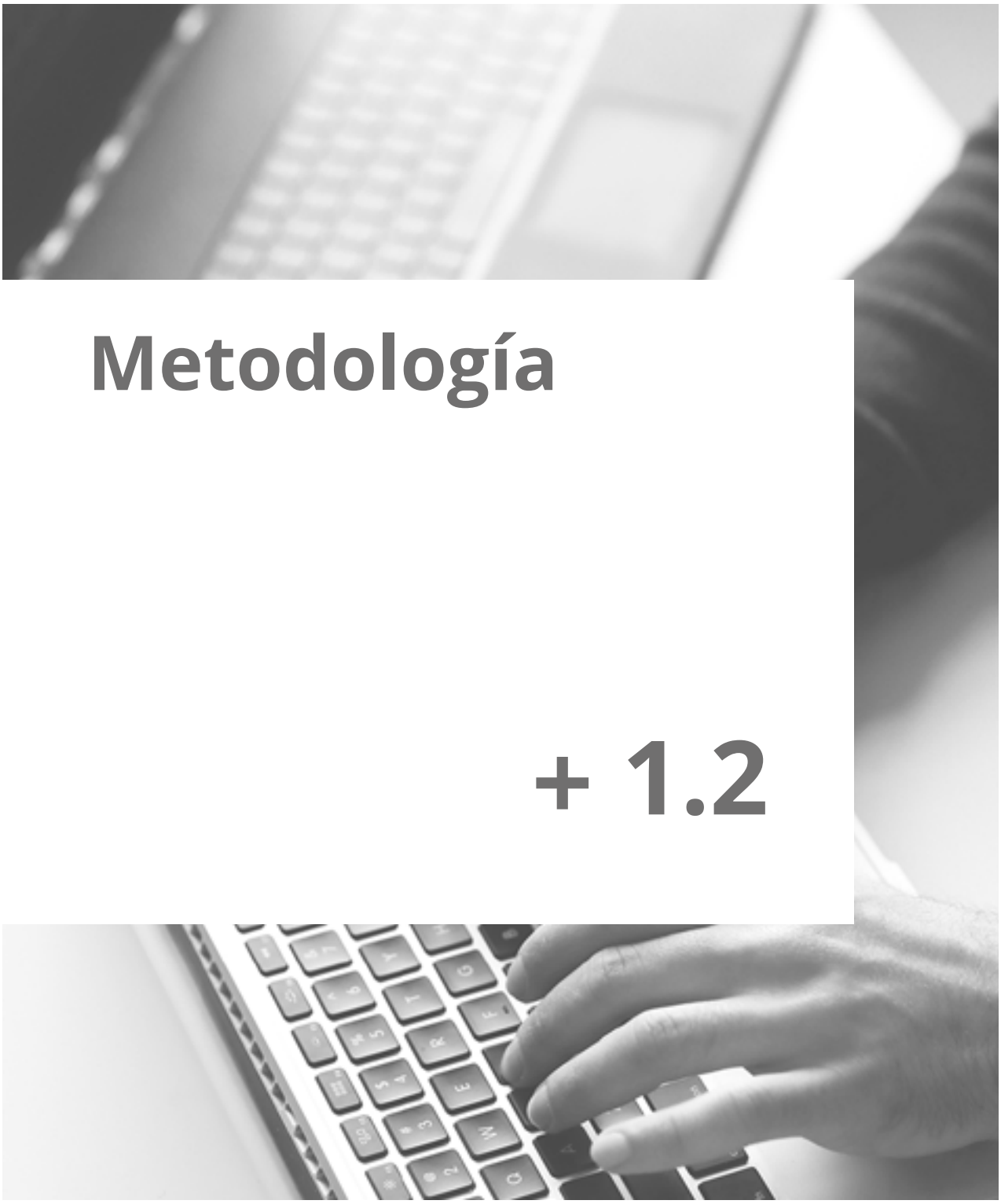
· **Colaboración Público-Privada**. Modelo de cooperación imprescindible para el desarrollo de las medidas previstas en la Estrategia Nacional de Ciberseguridad.

· **Oportunidades para la I+D+i**. Estudio de las capacidades españolas de I+D+i en ciberseguridad y de las fórmulas de financiación pública y privada.

· **Generación, transformación, retención y atracción de talento** para dar respuesta al doble reto al que se enfrenta la industria de la ciberseguridad: déficit vocacional que deriva en una falta de profesionales e inexistencia de regulación de las profesiones de ciberseguridad.

· **Difusión y gestión de impacto**.

El apartado 3 resume los puntos clave del diagnóstico de cada uno de ellos, mientras que el capítulo, 4 RECOMENDACIONES Y PRÓXIMOS PASOS, identifica propuestas concretas para avanzar hacia el objetivo concreto de desarrollar en la práctica la Estrategia Nacional de Ciberseguridad (ENCS) y reforzar la competitividad y autonomía del sector español.



Metodología

+ 1.2

El informe sobre la industria e investigación españolas en ciberseguridad ha sido elaborado sobre una base de transparencia, participación efectiva, representación de todos los agentes, responsabilidad y confianza.

Ha sido desarrollado por el Grupo de Trabajo «Impulso a la industria y a la I+D+i en ciberseguridad» del Foro Nacional de Ciberseguridad, que aglutina a diferentes agentes representantes del ecosistema español: organizaciones públicas y privadas, academia, asociaciones, organismos sin ánimo de lucro y sociedad civil. El presente Informe es fruto del consenso de todos ellos.

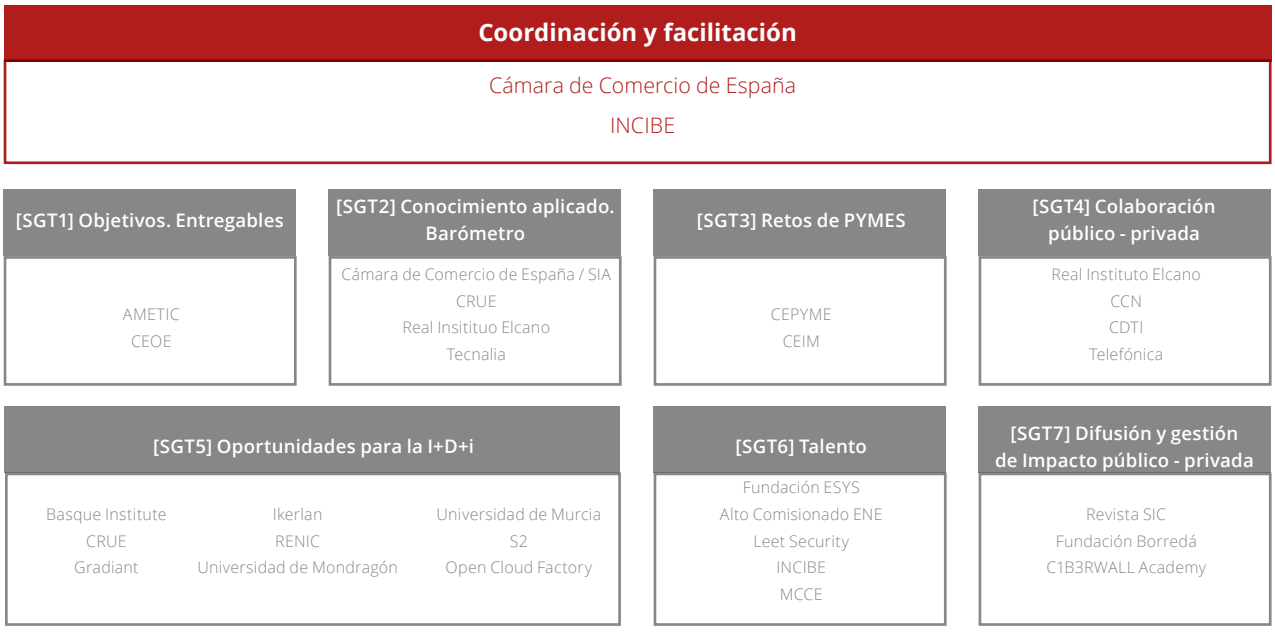
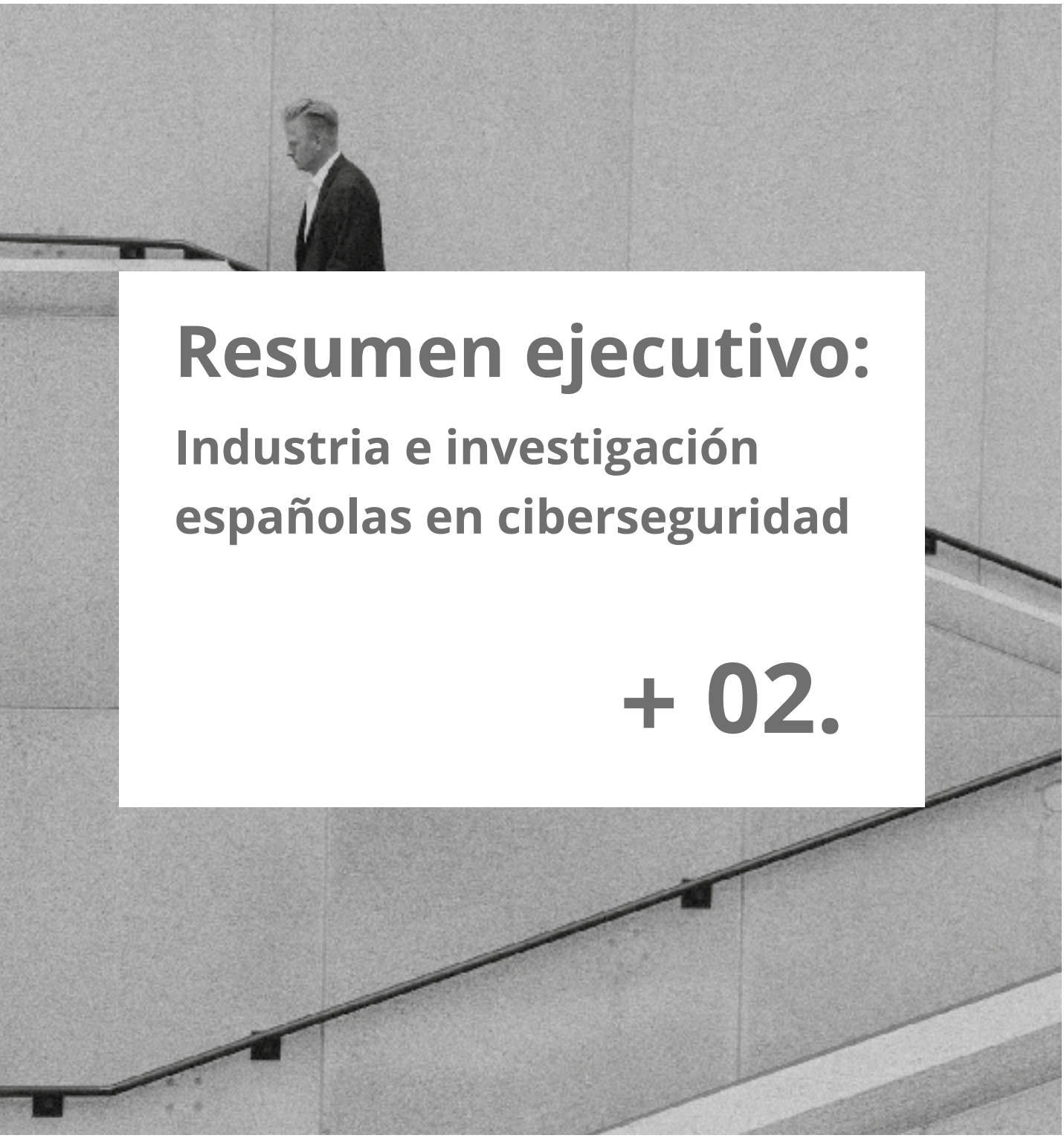


Figura 2: Composición de los 7 Subgrupos de Trabajo del GT2



Resumen ejecutivo:

Industria e investigación españolas en ciberseguridad

+ 02.

Resumen ejecutivo:

Industria e investigación españolas en ciberseguridad

El ecosistema español de ciberseguridad ha venido desarrollándose durante los últimos veinte años con unas sólidas bases legislativas. España es uno de los pocos países que dispone de un Código de Derecho de la Ciberseguridad [11], compendio de leyes aplicables a la ciberseguridad y privacidad, que proporcionan los cimientos del sector.

Al mismo tiempo, se ha venido desarrollado una red de investigación en ciberseguridad básica y aplicada en universidades y centros tecnológicos de investigación públicos y privados. Los resultados de dicha investigación no siempre se han conseguido transferir a la industria española. Aunque existen casos de éxito de tecnología española, estos casos se suelen encontrar fuera de España.

En lo que respecta a la industria española de ciberseguridad, existen grandes actores que proporcionan servicios de alta calidad nacional e internacionalmente, aunque muchos de ellos basados en tecnología no europea. Junto a ellos, un gran número de pequeñas y medianas empresas especializadas desarrollan productos y servicios de ciberseguridad con prestaciones de gran nivel, sin demasiada penetración en la demanda nacional y europea.

Desde las Administraciones Públicas se ha realizado un gran esfuerzo en potenciar a grandes organismos gubernamentales de ciberseguridad como Centro Criptológico Nacional (CCN), Instituto Nacional de Ciberseguridad Nacional (INCIBE), Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), Mando Conjunto del Ciberespacio (MCCE), Oficina de Coordinación de Ciberseguridad (OCC) y otros, que apoyan el desarrollo del sector.

Estos antecedentes han posicionado a España como uno de los países líderes en nivel de madurez en algunos frentes de la ciberseguridad a nivel global. No obstante, si se analizan indicadores específicos de la industria e investigación, la posición descendería en el ranking.

Hasta ahora, los actores trabajan en silos de forma poco coordinada. La colaboración público-privada que se ha establecido en el Foro Nacional de Ciberseguridad puede contribuir a eliminar dichos silos e impulsar el trabajo conjunto de todos los actores.

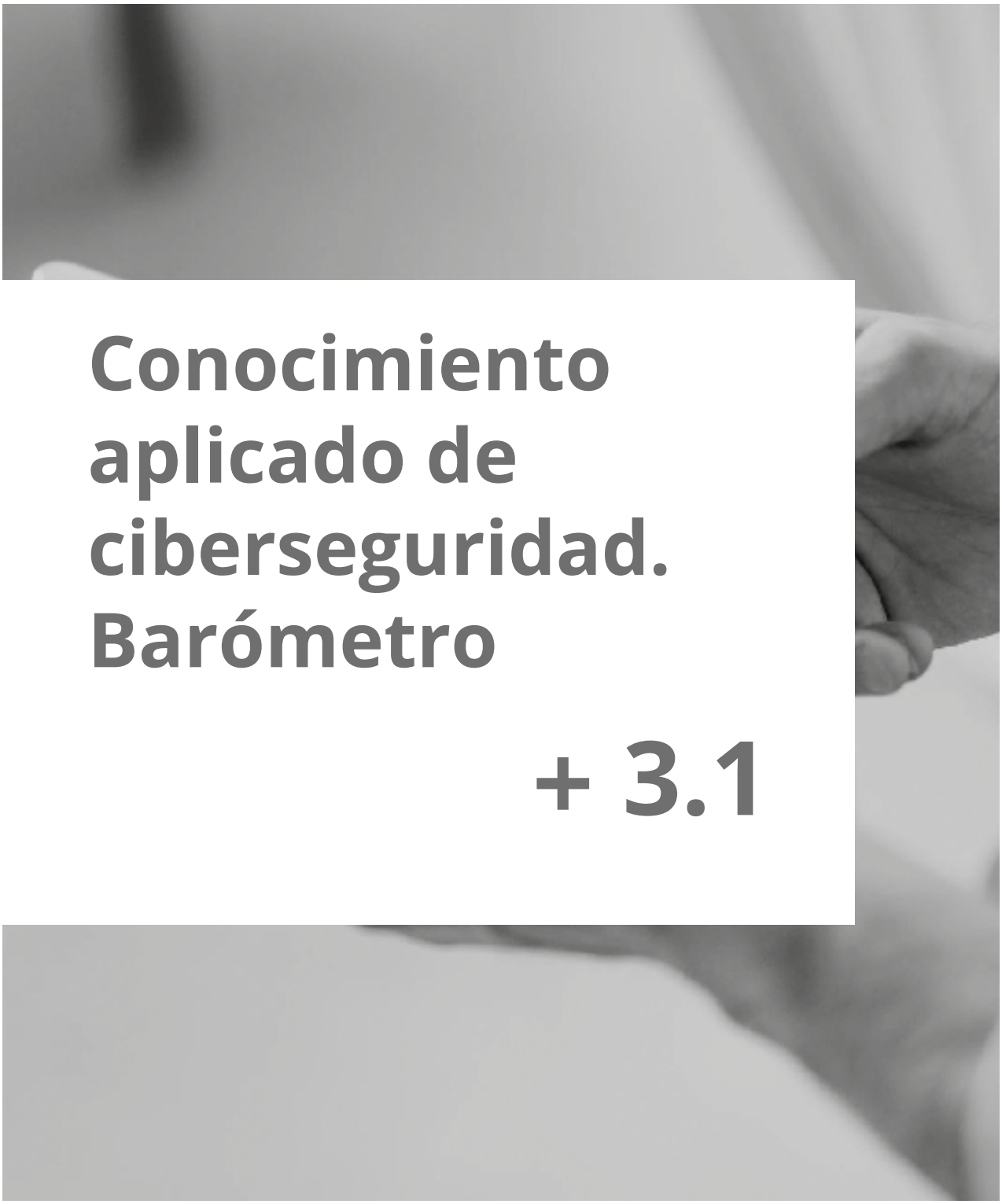
Por lo que respecta al Grupo de trabajo de Impulso a la industria y a la I+D+i, si se consigue una unificación de criterios y una lista priorizada de acciones comunes, la madurez del ecosistema de ciberseguridad aumentará significativamente para situar a España en uno de los tres principales polos de ciberseguridad en Europa.

La problemática de la I+D+i y del desarrollo industrial no es exclusiva de la ciberseguridad, si bien el sector presenta aspectos particulares por sus implicaciones sobre la seguridad nacional. El impulso a este ecosistema innovador deberá apoyarse tanto en acciones específicas como en reformas más transversales.

Análisis y recomendaciones para impulsar la Industria y la I+D+i

+ 03.

Los siguientes epígrafes recogen los análisis y propuestas de acción para alcanzar los objetivos de la ENCS, con el fin de que se desarrollen a nivel práctico las medidas de la Estrategia Nacional de Ciberseguridad referentes a la cooperación público-privada, impulso de la oferta y demanda nacionales en ciberseguridad, y refuerzo de la I+D+i.



Conocimiento aplicado de ciberseguridad. Barómetro

+ 3.1

La base de la mejora se encuentra en una adecuada medición. Por ello, el objetivo de este capítulo es plantear las líneas que definan el contenido y funcionamiento de un barómetro que permita medir la situación actual de la industria y la investigación de ciberseguridad en España y su evolución en el tiempo.

La creación del barómetro impacta directamente con lo que se expone en la línea de acción 5 de la ENCS [80]: «Potenciar la industria española de ciberseguridad y la generación y retención de talento, para el fortalecimiento de la autonomía digital».

En concreto, el barómetro debe contener la información necesaria para el desarrollo de algunas medidas incluidas en esta línea de acción:

· Impulsar los programas de apoyo a la I+D+i en seguridad digital y ciberseguridad (medida 1).

· Dinamizar el sector industrial y de servicios de ciberseguridad (medida 2).

· Incrementar las actividades nacionales para el desarrollo de productos, servicios y sistemas de ciberseguridad (medida 3).

· Promover las actividades de normalización y la exigencia de requisitos de ciberseguridad en los productos y servicios (medida 4).

· Detectar el talento en el campo de la investigación (medida 8).

· Impulsar programas específicos de I+D+i en ciberseguridad (medida 9).

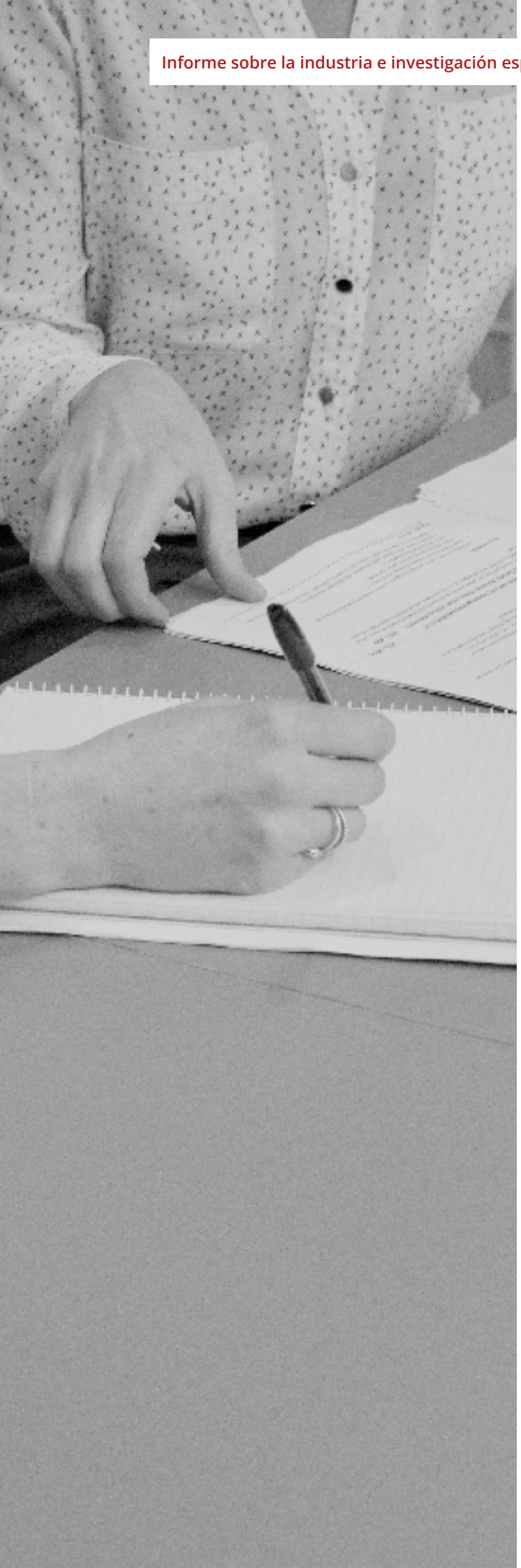
El barómetro también tiene su relevancia en medidas de otras líneas de actuación:

· El barómetro facilitará la colaboración de los centros de excelencia e investigación en la lucha contra las ciberamenazas; ayudará a potenciar y apoyar los desarrollos realizados en la red de CSIRT española y a desarrollar instrumentos de prevención, detección y respuesta. Todas ellas son medidas dentro de la línea de acción 1: «Reforzar las capacidades ante amenazas provenientes del ciberespacio».

· El conjunto de indicadores (Key Performance Indicators - KPI) incluidos en el barómetro podrán formar parte del sistema de métricas para las principales variables de ciberseguridad. También podrán servir de base para desarrollar catálogos de productos certificados y cualificados. Ambas son medidas incluidas en la línea de acción 2: «Garantizar la seguridad y resiliencia de los activos estratégicos para España».

· El barómetro puede ser también una herramienta que proporcione una información relevante para el impulso de la ciberseguridad en empresas (pymes, micropymes y autónomos), tal y como se establece en la línea 4: «Impulsar la ciberseguridad de ciudadanos y empresas».

· Por último, debido a que el barómetro pretende estar alineado con los sistemas de métricas y taxonomías definidos en el ámbito internacional, puede facilitar la participación de las empresas españolas en el ámbito de la Unión Europea en el desarrollo de un entorno europeo seguro, como viene recogido en la medida 4 de la línea de acción 6: «Contribuir a la seguridad del ciberespacio en el ámbito internacional».



3.1.1. Barómetro Integral de la Ciberseguridad

Elaborar un Barómetro Integral de la Ciberseguridad para evaluar el progreso hacia todos los objetivos de la ENCS.

El subsistema de industria e investigación necesita asegurarse su papel específico y diferenciado a través de la inclusión en el barómetro de indicadores de evaluación de su desempeño. De esta forma, la industria y la investigación tendrían dentro del conjunto de la ciberseguridad una visibilidad que en la actualidad no tienen.

El barómetro debe medir los fines establecidos en las políticas de ciberseguridad. En el caso español, los objetivos en industria e investigación se fijan en las líneas de acción de la Estrategia Nacional de Ciberseguridad, si bien en el futuro se podrían fijar otros derivados de políticas nacionales afines o de la estandarización de los barómetros para su comparación internacional, tal y como apunta el NCSS de ENISA.

En consecuencia, se propone que INCIBE elabore un barómetro de madurez específico para la industria y la investigación que se pueda integrar como componente del barómetro general de la ciberseguridad.

Dentro de un ambiente de buena colaboración público-privada como el español, potenciado con los trabajos del FNCS, el sector privado debería participar en la determinación de objetivos.

El Anexo VII desarrolla una propuesta de metodología de elaboración y modelo de cuestionarios, que pueden constituir un punto de partida para el desarrollo del futuro barómetro.

3.1.1.1. Indicadores de madurez del Barómetro Integral de la Ciberseguridad

Incluir dentro de ese Barómetro indicadores específicos de industria e investigación (KPI) para medir la madurez de la industria y la investigación y que cualifiquen (CÓMO) y cuantifiquen (CUÁNTO) su estado comparado con otros.

El barómetro de la industria e investigación en ciberseguridad debe identificar los indicadores necesarios para medir la madurez de los componentes identificados en la taxonomía anterior (sectores, dominios y tecnologías).

Para ello, se ha realizado un estudio de los indicadores y modelos de medición de madurez de la ciberseguridad utilizados internacionalmente. Una descripción detallada se encuentra en el Anexo VI.

Tras el análisis de los modelos de indicadores mencionados, y en ausencia de uno que pueda importarse directamente, una de las propuestas es la elaboración de una batería de indicadores ad hoc para medir la madurez, ya sea de forma aislada (Barómetro de industria e investigación) o como componente de un barómetro más amplio (Barómetro de la ciberseguridad).

Su elaboración es imprescindible para conocer el estado actual y evolución de la industria y la investigación de la ciberseguridad (madurez), así como su comparación con indicadores afines europeos e internacionales (*benchmarking*).

Fruto del análisis documental, se ha identificado la siguiente batería de 24 indicadores que pueden constituir la base para medir la madurez del subsistema español de la industria y la investigación en ciberseguridad:

Indicador	Descripción	Organismos / Modelos de medición que lo utilizan
1. Mercado de la ciberseguridad	Valor anual del sector. Permite comparativas temporales y desagregación por países, tamaños, especialización, oferta y otros	INCIBE ONTSI [76] UKCSA [89] CIMA [25] DESI [24] ICEX
2. Contribución al PIB	Permite agregar y desagregar las distintas contribuciones por sectores, especialización, tamaño, empleados y otros	DESI [24] UKCSA [89] CIMA [25]
3. Cuota de mercado	Porcentaje de servicios, software o hardware nacionales sobre el conjunto del mercado	ICEX
4. Exportaciones e importaciones de bienes de ciberseguridad	Cantidades y porcentajes en el balance de empresas y origen / destino	DATACOMEX [69] UKCSA [89] CIMA [25]
5. Mercado interno	Consumo interno = ventas - exportaciones + importaciones.	CIMA [25]
6. Inversiones	Inversión total o por sectores (I+D+i o seguridad), según su procedencia pública o privada, ubicación y tamaño de los destinatarios, entre otros	DESI [24] UKCSA [89] CIMA [25] RVCTI [83] NCPI [5] ECSO [35] NCSS [20]
7. Número de empresas		INCIBE ONTSI [76] RVCTI [83] UKCSA [89] ECSO [35] CIMA [25]
8. Número de empleos	Total y segmentado por ubicación, especialización, tamaño, productos / servicios y otros	DESI [24] UKCSA [89] CIMA [25] INCIBE ECSO [35]
9. Tamaño de empresas		DESI [24] CIMA [25] ECSO [35] UKCSA [89]

Indicador	Descripción	Organismos / Modelos de medición que lo utilizan
10. Distribución regional e internacional de sedes (presencia)	Ubicación de los centros de investigación e innovación regional	CIMA [25] UKCSA [89] ATLAS [26] RIS [27]
11. Nivel de especialización empresarial (total o parcial)		ECSO [35] UKCSA [89]
12. Códigos de Clasificación Industrial Uniforme		
13. Productos y servicios según taxonomías de oferta y demanda	Especialización de proveedores, segmentación y especialización de clientes finales	
14. Intangibles	Indicadores indirectos o globales que condicionan la maduración[1]	EIS [28]
15. Transferencias entre investigación e industria	Número de patentes, incentivos, programas o centros de trasferencia, entre otros	NCPI [5] RVCTI [83] DESI [24] NCSS [20]
16. Conectividad entre actores	Presencia de actores nacionales en redes regionales (clústeres) o europeas (EDIHs) de industria e investigación	RVCTI [83] NCSS [20]
17. Fondos dedicados a la I+D+i	Estimación de los fondos y los programas dedicados a la investigación, desarrollo e innovación[2]	RVCTI [83] NCPI [5] ECSO [35] DESI [24] NCSS [20]
18. Formación específica en ciberseguridad	Formación de talento digital. Se deberían explorar niveles de formación específicos en ciberseguridad.	DESI [24] NCSS [20] CMM [77] GCI [53] NCPI [5] RVCTI [83]

[1] European Innovation Scoreboard (EIS) [28] ofrece 37 indicadores genéricos que afectan a la capacidad de innovación general de los Estados como el porcentaje del PIB público invertido en I+D+i, el número de doctores, la penetración del ancho de banda, las publicaciones científicas o las iniciativas de emprendimiento entre muchos otros. Algunos de sus indicadores podrían particularizarse para medir la madurez de la ciberseguridad en general o la de la industria y la investigación en particular

[2] La diferenciación de las inversiones por su procedencia (pública, privada, europea y otras) arrojaría nuevos indicadores de madurez

Indicador	Descripción	Organismos / Modelos de medición que lo utilizan
19. Intangibles	Indicadores indirectos, por ejemplo, para la medir el grado de digitalización, la capacidad de innovación o la investigación digital de los países.	EIS [28] DESI [24]
20. Emprendimiento	Indicadores del observatorio *Global Entrepreneurship Monitor* – GEM [40] sobre emprendimiento industrial y tecnológico, financiación y *benchmarking*.	GEM [40]
21. Obstáculos al crecimiento	Factores que dificultan el crecimiento de las actividades industriales y de investigación	UKCSA [89] NCSS [20]
22. Prioridades	Prioridades críticas. Métricas que permitan medir el avance en las tecnologías y sectores de futuro.	
23. Volumen de concursos públicos de ciberseguridad		
24. Volumen de inversión extranjera en ciberseguridad en España		

Tabla 3: Batería de indicadores de madurez de la industria e investigación en ciberseguridad

3.1.1.2. Cadena de valor de la ciberseguridad

Elaborar un catálogo de los actores que participan en la cadena de valor de la industria e investigación (QUIÉN).

La cadena de valor en el ámbito de la industria y la investigación debe servir para enlazar oferta y demanda, siguiendo las reglas del libre mercado.

La ENCS y los trabajos del FNCS persiguen ejercer una influencia positiva sobre la oferta y la demanda de productos y servicios de ciberseguridad nacionales, al objeto de incrementar la autonomía estratégica.

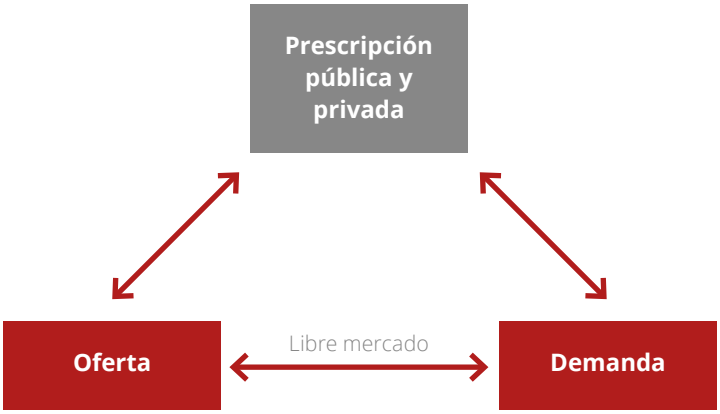


Figura 3: Mercado de la ciberseguridad

Por ello, se considera que la cadena incluye no solo a los actores tradicionales de industria e investigación, sino también a otros actores y roles que añaden valor a los anteriores según refleja la figura adjunta.

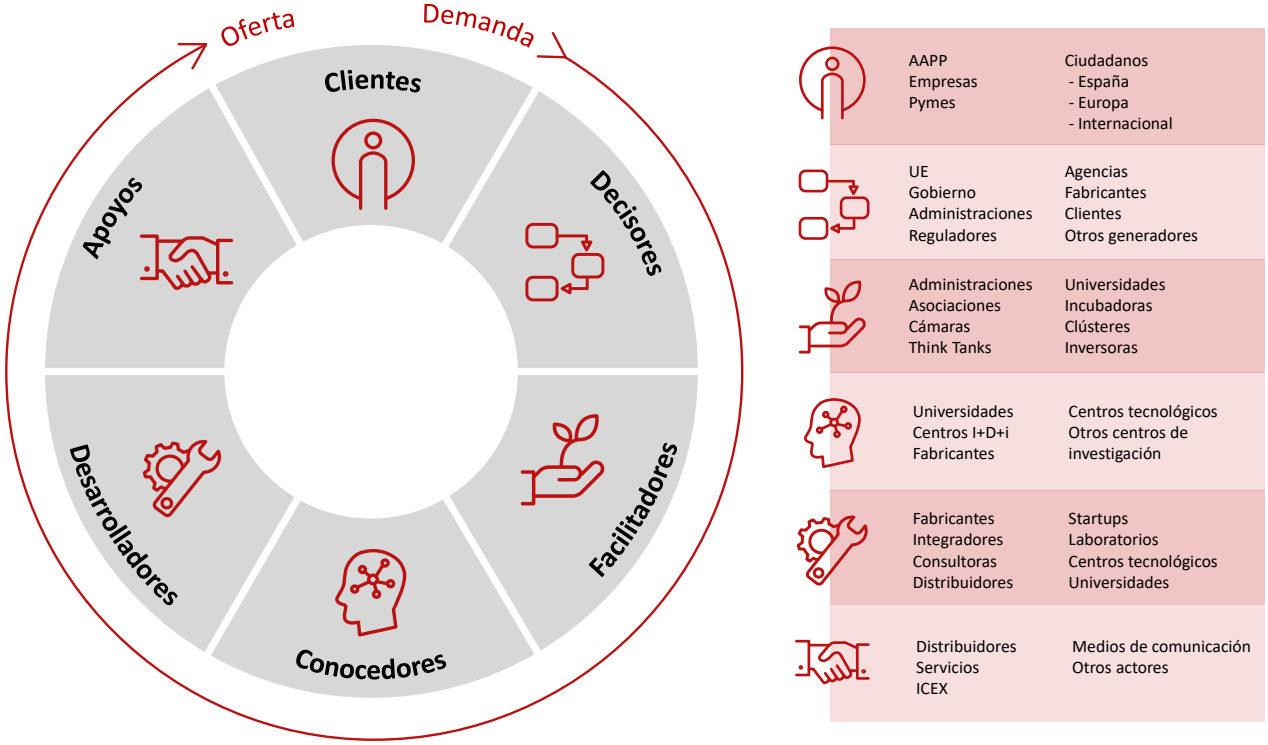
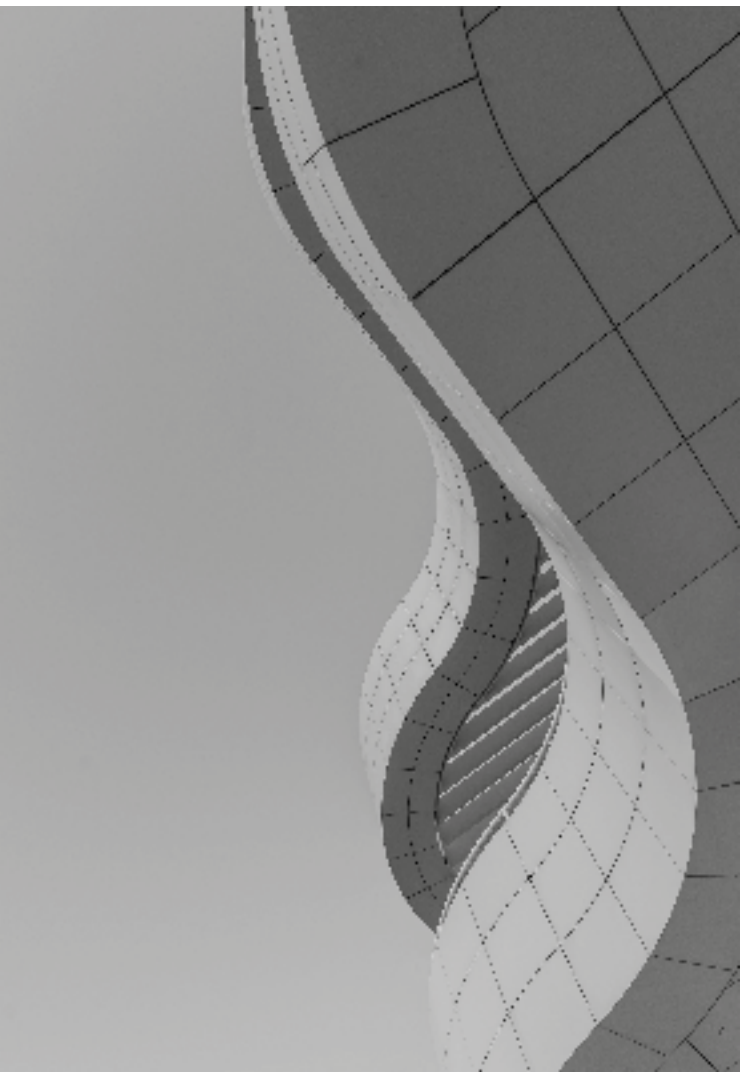


Figura 4: Roles de la cadena de valor de la ciberseguridad

La mayoría de las cadenas de valor analizadas [46] se centran en la parte industrial: parten de la fabricación, continúan por la distribución y terminan en los clientes usuarios de ciberseguridad. La investigación, por su parte, dispone de su propia cadena de valor, muy poco enlazada con la cadena industrial.

Esta desconexión entre industria e investigación constituye el eslabón más débil entre los dos grandes ámbitos de la cadena de valor global. Por tanto, la propuesta es continuar profundizando en la construcción de una cadena de valor global de la ciberseguridad en la que se detallen los roles, actividades e interacciones entre los diferentes actores: decisores, facilitadores, conocedores, desarrolladores y apoyos.



La inclusión de nuevos actores y la posibilidad de que desarrollen diferentes roles permitirá un mayor conocimiento del ecosistema, de las capacidades disponibles y de los indicadores de madurez y contribuirá a la eliminación de las barreras entre los diferentes actores en la cadena de valor global. Además de oferta y demanda, se identifican los siguientes roles:

· **Decisores**. La demanda de productos y servicios de ciberseguridad se inicia por la solicitud de administraciones públicas, industrias o clientes, para satisfacer las necesidades de sus servicios públicos o privados, agendas y planes de investigación o de mercado.

· **Facilitadores**. La demanda precisa la intervención de intermediarios que conviertan la demanda en programas industriales y de investigación.

· **Conocedores**. Los proyectos se ponen en marcha por quienes tienen capacidades de investigación y desarrollo en todas sus vertientes de investigación básica, aplicada e innovadora.

· **Desarrolladores**. Para continuar la actuación de los anteriores actores hacia los niveles de madurez tecnológica más elevados de la demanda (TRL – *Technological Readiness Level*), se precisa contar con capacidades tecnológicas para el desarrollo de prototipos y capacidades industriales para la obtención de productos, servicios o sistemas.

· **Apoyos**. Finalmente, tras la fabricación, intervienen los distribuidores de productos y prestadores de servicios, así como los medios de comunicación especializados para transferir dicha oferta hacia los clientes y usuarios finales.

En la Figura 5 se proporciona una visión integrada de los diferentes actores de la cadena de valor descritos anteriormente, así como las interacciones actuales entre los mismos.

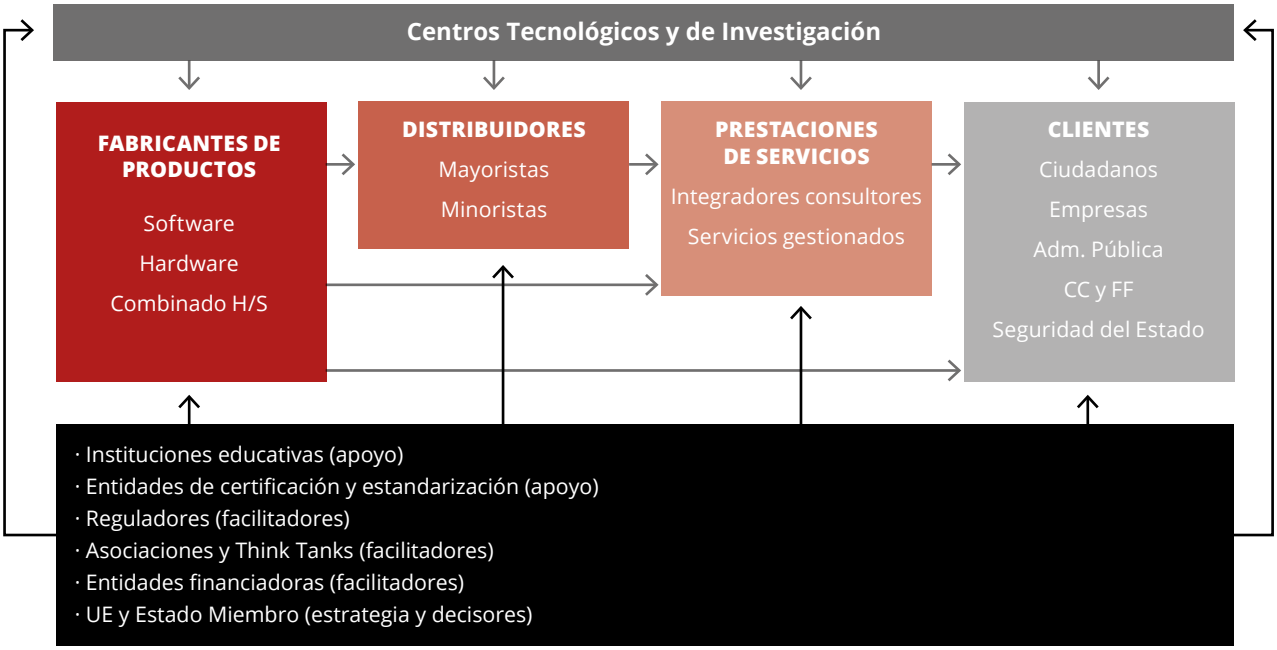


Figura 5. Visión integrada de los diferentes actores de la cadena de valor

En la Tabla 4 se proporciona una visión integrada de las categorías y subcategorías de los actores de la cadena de valor descritos anteriormente, junto con algunas dimensiones adicionales sobre su tipología y ámbito de actuación.

ACTORES - QUIÉN			
Rol	**Categoría - Tipología**	**Ámbito**	**Tipo**
Decisor	Administración Pública	Mundial	Público
Facilitador	Entidad de estandarización y certificación	Europeo	Privado
Conocedor	Think Tank	Nacional	Público- Privado
Desarrollador	Asociación / Cluster / Hub de Ciberseguridad	Autonómico	Otro
Apoyo	European Digital Innovation Hub	Local	
Cliente	Universidad	Otro	
Otro	Centro de Investigación I+D+i		
	Empresa fabricante		
	Empresa Integradora		
	Empresa Consultora		
	Empresa Prestadora de Servicios		
	Empresa Mayoristas/Distribuidoras		
	Startup		
	Incubadora		
	Entidad financiadora de proyectos		
	Medio de comunicación		
	CSIRTs		
	Ciudadano		
	Otro		

Tabla 4. Categorización y dimensiones añadidas de los actores de la cadena de valor

Una de las principales propuestas aborda la necesidad de acordar y desarrollar una caracterización de la cadena de valor y de los diferentes actores de la industria y la investigación en ciberseguridad.

3.1.1.3. Taxonomía de las competencias en ciberseguridad

Elaborar una taxonomía integrada de capacidades de la industria y la investigación (QUÉ)

Una taxonomía permite la categorización de los productos existentes en el mercado y de los dominios de aplicación, investigación y conocimiento, y al mismo tiempo el mapeado de las diferentes entidades que investigan y trabajan en el mundo de la ciberseguridad.

La taxonomía debe ir evolucionando con el tiempo, especialmente, en un ámbito tecnológicamente tan amplio en su desarrollo y tan transversal en su aplicación como es la ciberseguridad.

En la actualidad, no se ha encontrado una taxonomía única que permita la clasificación y ordenación de los productos y servicios del sector de la ciberseguridad. Esta circunstancia dificulta la conexión entre oferta y demanda, y entre industria e investigación. El primer paso, por tanto, es hacer un recorrido por las taxonomías en ciberseguridad existentes.

En el Anexo II se detallan las taxonomías que han sido tenidas en cuenta para el análisis, del que se obtienen las siguientes conclusiones:

· Desde el punto de vista de la investigación, se considera oportuno trabajar con la taxonomía JRC [54] ya que es muy probable que, al tratarse de una taxonomía creada en el seno de la Comisión Europea y contrastada ampliamente, sea considerada en los trabajos de la Red y el Centro de Competencias de Ciberseguridad. Es de esperar que la comunidad de I+D+I nacional deba mapearse contra esta taxonomía JRC.

· Desde el punto de vista de la industria, que ofrece productos y servicios de ciberseguridad, es mucho más natural y sencillo mapearse en la taxonomía de ECSO [34], que se ha convertido en referencia a nivel europeo.

· Por este motivo, se considera conveniente trabajar con ambas taxonomías, ECSO (ver Anexo III) y JRC (ver Anexo IV), generando una taxonomía híbrida (ver Anexo V) que permita mapear cada una de las 60 categorías de ECSO con varias de las 149 del JRC.

A efectos prácticos, cada entidad podría mapearse en función de sus características contra las categorías de ECSO (si se trata de un actor de la industria) o contra las categorías de JRC (si se trata de un actor de la investigación), actuando como una tabla de conversión de categorías que permitiría realizar análisis cuantitativos y cualitativos en el barómetro de la ciberseguridad que se propone.

Para facilitar el análisis cuantitativo y minimizar el error derivado de la conversión, se ha asumido que una categoría de JRC sólo puede estar en una categoría de ECSO.

Dado que este criterio dificulta los análisis más cualitativos, se ha decidido realizar la conversión ECSO-JRC mediante dos columnas correspondientes al JRC, una primaria, sobre la que se realizarán los análisis cuantitativos, y otra secundaria, sobre la que se realizarán los análisis más cualitativos y en la que una categoría del JRC podría estar en varias de ECSO.

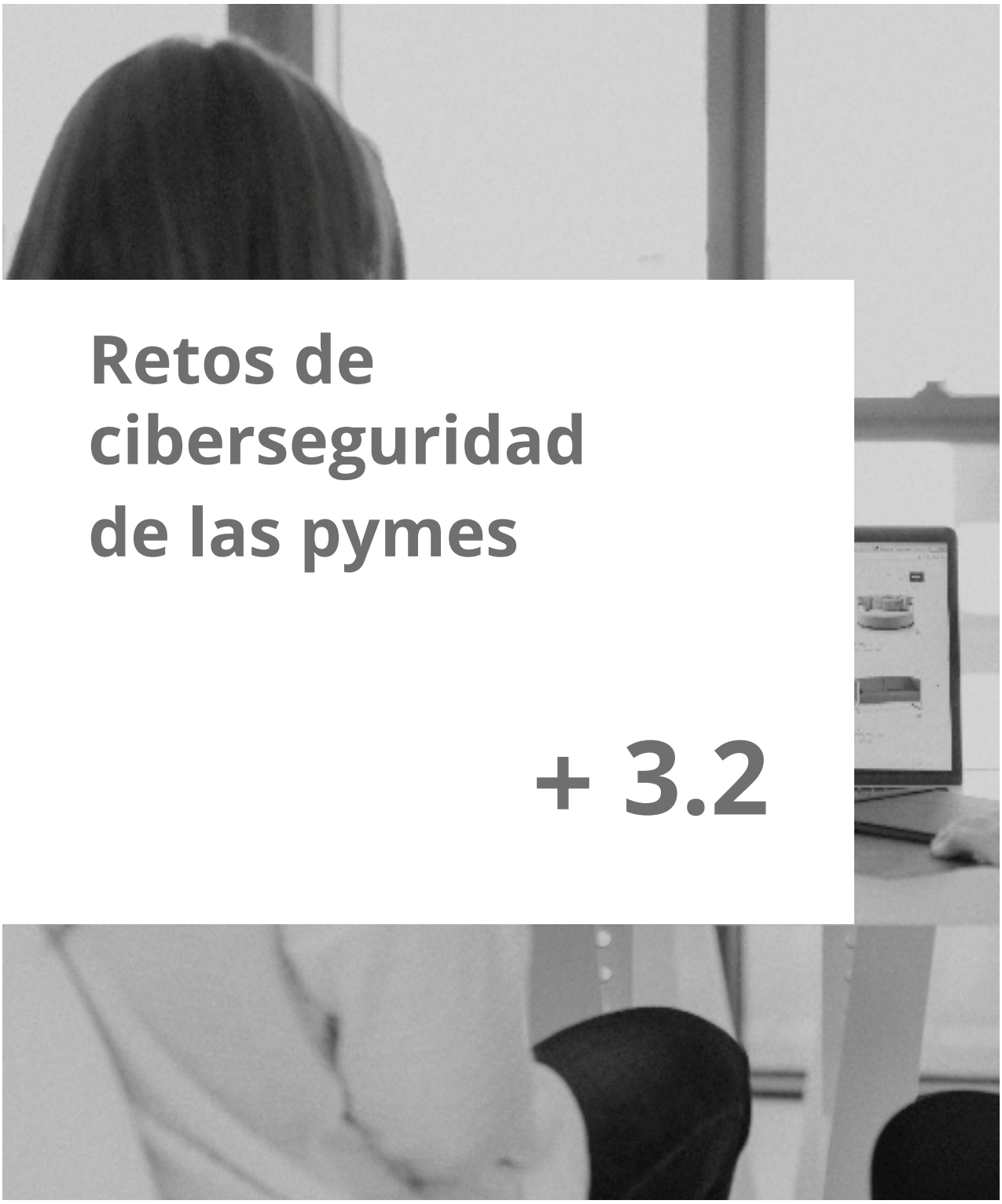
Esta taxonomía se complementa con los Casos de Uso del JRC, tanto si se mapean contra las categorías de ECSO o contra las del JRC.

Estas aproximaciones han sido contrastadas por los representantes de la industria y la investigación en ciberseguridad que participan en el FNCS.

Por ello, una propuesta fundamental es la necesidad de consensuar una taxonomía aplicable a I+D+i e industria, que podría basarse en la planteada en este Informe. Se propone continuar los trabajos de detalle para la definición de una taxonomía integrada, y realizar un piloto de la misma con los actores de investigación e industria que forman parte del FNCS, junto con los que voluntariamente deseen adscribirse.

3.1.1.4. Observatorio para la elaboración y seguimiento del Barómetro Integral de Ciberseguridad

Crear un Observatorio para la elaboración y seguimiento del Barómetro Integral de Ciberseguridad en la que participe el ecosistema de industria e investigación (DÓNDE).



Retos de ciberseguridad de las pymes

+ 3.2

Este capítulo analiza los retos de ciberseguridad a los que se enfrentan las pymes españolas en su papel de consumidoras y demandantes de productos y servicios de ciberseguridad.

El punto de partida para conocer los retos de las empresas españolas en materia de ciberseguridad es el contexto demográfico del país. La primera idea a destacar es que España es un país de pymes y, en especial, de microempresas. Los datos de la Secretaría General de Industria y de la Pequeña y Mediana empresa para marzo de 2020 indican que las pymes de hasta 250 empleados suponen el 99,83% del tejido empresarial español formado por cerca de 2,9 millones de empresas.

Dentro de las pymes, destaca especialmente el peso de aquellas que no emplean a ningún asalariado (más de 1,6 millones) y de las microempresas con hasta nueve empleados (1,1 millones).

Empresas por tamaño	Número de empresas	Tasa anual de variación %
Pyme (0-249 asalariados)	2.919.456	1,71
Pyme sin asalariados	1.614.765	1,66
Pyme con asalariados	1.304.691	1,78
Microempresas (1-9 asalariados)	1.123.936	1,36
Pequeñas (10-49 asalariados)	155.502	4,57
Medianas (50-249 asalariados)	25.253	3,82
Grandes (250 o más asalariados)	4.878	3,19
Total empresas	**2.924.334**	**1,71**

Tabla 5: Empresas por tamaño en España [70]

El Plan de digitalización de pymes 2021-2025 [41] reconoce que «la digitalización de las pymes adquiere una especial urgencia ante las circunstancias derivadas de la pandemia COVID-19». Las pymes españolas deberán adaptar sus modelos de negocio y sus procesos para poder sobrevivir.

Aunque el impacto de la pandemia ha acelerado el cambio tecnológico de las empresas hacia modelos más digitales, no se puede obviar el reto extraordinario que ello supone: la digitalización exprés y forzada del tejido empresarial español puede tener consecuencias, entre otras, la debilidad en materia de seguridad digital.

La ciberseguridad es clave en el reto de transformación digital de la empresa y debe ser considerada en cualquier iniciativa de digitalización empresarial.

En este contexto, la ciberseguridad (considerada como un elemento implícito a la transformación digital) es absolutamente transversal a todos los sectores. El reducido tamaño medio de las empresas españolas puede suponer un importante reto a la hora de su adopción, por lo que la adaptación y personalización a las circunstancias concretas de la pyme debe estar en la base de todas las acciones.

El colectivo de pymes no es ajeno al aumento en frecuencia y gravedad de los incidentes de seguridad. Así, el centro de respuesta a incidentes de ciudadanos y pymes INCIBE-CERT gestionó en 2020 un total de 106.466 incidentes reportados por ciudadanos y empresas [48].

Por tanto, es clave sensibilizar a la población en general y al conjunto del tejido empresarial acerca de los riesgos de la falta de seguridad digital y de sus consecuencias tanto individuales como colectivas, así como proporcionar formación y herramientas que permitan empoderar y hacer responsable al usuario final acerca de su seguridad digital y de la organización.

Es urgente que las pymes aborden la digitalización y, por ende, todas las medidas necesarias respecto a la ciberseguridad. Para ello, los fondos Next Generation EU suponen una extraordinaria oportunidad para la implementación en un breve espacio de tiempo de las medidas que se proponen, por lo es necesario que estas se incorporen a los proyectos asociados a su ejecución a través del Plan de Recuperación, Transformación y Resiliencia.

Las propuestas identificadas para dar respuesta a los retos de ciberseguridad de las pymes españolas y que, a su vez, pueden constituir un impulso para la industria e investigación españolas en ciberseguridad son las siguientes:

3.2.1. Elevar el nivel de sensibilización

- Impulsar jornadas de sensibilización, talleres de capacitación y sesiones en centros demostradores de ciberseguridad. Se pueden utilizar infraestructuras ya existentes, tales como la red de Oficinas Acelera Pyme de las Cámaras de Comercio, asociaciones empresariales sectoriales y territoriales, clusters o Digital Innovation Hubs, por mencionar algunos ejemplos.

- Adaptar el lenguaje de la ciberseguridad al perfil y nivel de comprensión del destinatario (personal no técnico de las pymes), agrupando y simplificando las categorías de riesgos y servicios de ciberseguridad. Se propone el uso de diferentes estándares de categorización de ciber amenazas.

- Impulsar la compartición de ejemplos reales de incidentes y casos de buenas prácticas de administraciones públicas y empresas para sensibilizar a las pymes sobre el desarrollo de mecanismos de prevención y respuesta a ciberataques.

- Lanzar una campaña de comunicación de ámbito nacional dirigido específicamente a pymes, micropymes y autónomos sobre la importancia de reforzar la ciberseguridad de manera paralela al proceso de digitalización. El público objetivo está formado principalmente por propietarios y directores generales de las empresas, personas con capacidad de decisión y, normalmente, bajo conocimiento técnico.

3.2.2. Reforzar las competencias digitales en ciberseguridad: capacitación, certificación y herramientas

- Bajo un modelo de colaboración público-privado, diseñar e implementar contenidos formativos específicos en ciberseguridad adaptados a los distintos segmentos de empresas (micro, pequeñas y medianas), autónomos y trabajadores en activo.

- Proporcionar a las pymes un servicio de asesoría personalizada en ciberseguridad, que les facilite un diagnóstico de su situación y exposición al riesgo junto con una propuesta de soluciones y herramientas.

- Bajo un modelo de colaboración público-privado, diseñar e implementar contenidos formativos específicos en ciberseguridad adaptados a los distintos segmentos de empresas (micro, pequeñas y medianas), autónomos y trabajadores en activo.

- Establecer un programa de ayudas para la implantación, renovación y modernización de herramientas e infraestructuras de ciberseguridad, con participación público-privado, que incluya una apuesta por el *cloud computing.*

- Creación de un sello en materia de ciberseguridad para las pymes que cumplan determinados requisitos.

- Establecer un modelo de suscripción a un hub tecnológico de ciberseguridad o Centro de Servicios Compartidos que provea a las compañías suscriptoras un entorno compartido, dedicado y especializado en servicios avanzados de ciberseguridad que aporte soluciones efectivas a riesgos de ciberseguridad.

  Esto tendría importantes beneficios de economía de escala y especialización para las pymes.

  Todo ello tendría lugar en tecnología cloud, con los esfuerzos que esto supone de migración para muchas pymes, por lo que se hace necesario un plan de adaptación específico a autónomos y micro pymes, quizás con financiación pública o condiciones preferentes.

  Para la prestación de este servicio, igual que el resto de recomendaciones incluidas en este capítulo, se debe tener en cuenta que el objetivo es el desarrollo de la industria española de ciberseguridad, por lo que la Administración debe contar con el sector privado.

3.2.3. *Benchmark* internacional

Realizar una prospectiva de programas internacionales de apoyo a la ciberseguridad en las Pymes. Asegurar las oportunidades para las compañías españolas a través del hub del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad.

3.2.4. Medición del riesgo de pymes

Definir un sistema de métricas comunes, estandarizadas y centralizadas para la medición del nivel agregado de ciberriesgo sobre las pymes en España.

Este modelo de supervisión debe permitir identificar tendencias, supervisar el nivel de efectividad de la ciberseguridad en la pyme y adoptar medidas para la mejora global. Los indicadores podrían ser parte de un barómetro sectorial y territorial que implicara a todas las entidades y agentes con periodicidad semestral o anual.

A modo de ejemplo de métricas a considerar, se mencionan los siguientes:

· Tipología de ciberincidentes con mayor afectación en frecuencia e impacto sobre los diferentes sectores de pyme en España

· Tiempo medio de detección de ciberincidentes

· Tiempo medio de resolución de ciberincidentes

· Coste medio por cada brecha de ciberseguridad

· Nivel de demanda de las pymes

3.2.5. Adaptación y personalización de contenidos de ciberseguridad a las características concretas de pymes

Construir una matriz que permita categorizar las pymes en función de características como tamaño, sector, nivel de alfabetización del capital humano, criticidad de la información y situación económica de la pyme. Esta matriz constituirá la base para adaptar y personalizar las actuaciones, contenidos y herramientas de ciberseguridad a las circunstancias concretas de la empresa.

Colaboración público - privada

+ 3.3

La colaboración público-privada, que se ha institucionalizado en algunos ámbitos de la ciberseguridad española, todavía no se ha articulado en el ámbito de la investigación y la industria. Por ello, en este capítulo, se proponen instrumentos y modelos de colaboración público-privada (CPP) que permitan desarrollar las líneas de acción previstas en la Estrategia Nacional de Ciberseguridad para impulsar la industria y la investigación, tanto pública como privada (ver Tabla 2: Medidas asociadas a la Línea de Acción 5 de la Estrategia Nacional de Ciberseguridad).

Con este objetivo, se plantea la articulación de un ecosistema de ciberseguridad especializado y competente en industria e investigación sostenible a largo plazo. Este ecosistema de industria e investigación en ciberseguridad (EI2C) incrementará la autonomía estratégica nacional en productos y servicios que satisfagan las necesidades públicas y las oportunidades de negocio privadas.

3.3.1. El ecosistema en construcción: el EI2C

Implantar un ecosistema de ciberseguridad público-privado a nivel nacional especializado en industria e investigación (EI2C) para potenciar la autonomía estratégica en ese ámbito. Su implantación debe coincidir con la operatividad de la Red y Comunidad de Centros Nacionales de Coordinación.

Se emplea en este capítulo el término ecosistema para denominar al subsistema formado por la industria y la investigación en ciberseguridad de España. El EI2C es una parte del ecosistema más amplio de ciberseguridad que, a su vez, forma parte del ecosistema digital, por lo que su especialización debe ser compatible y estar conectada con ellos. Esta conexión es imprescindible para asegurar el impacto positivo de las propuestas sobre la ciencia y la industria españolas.

La construcción del EI2C parte de una evaluación del estado de la colaboración público-privada (CPP), sus antecedentes, elementos y cultura existente hasta el momento. El Anexo VIII ofrece una visión sobre el contexto de la colaboración público-privada en ciberseguridad.

Lo específico del EI2C es impulsar la aplicación de la investigación (conocimiento) a las políticas públicas (servicios) y a la economía digital (industria) a escala nacional. Para que funcione y sea atractivo, es necesario dotar al EI2C de un conjunto de instrumentos y de un buen sistema de gobernanza.

Tratándose de un modelo abierto de innovación e industria, debe ser inclusivo y con unas condiciones de participación que faciliten la gobernabilidad y eficacia. La participación colectiva podría resolverse mediante agrupaciones tipo foro en una asamblea periódica de control. El derecho a decisión, según el modelo europeo, corresponde a quienes invierten en los programas.

Bajo este criterio, podrían participar en el Consejo de Administración los órganos de la Administración General del Estado y de las CCAA que aportaran fondos públicos al CNC, así como los actores privados que hicieran lo propio.

Dentro del EI2C, y como refleja la Figura 6, los órganos rectores propuestos (Director y Consejo Consultivo) contribuirán a definir las prioridades nacionales (en colaboración con los Ministerios y Agencias implicados) y las propias (en coherencia con aquellas o por cuenta propia si no se alinean los planeamientos estratégicos de la industria y la investigación en el plano nacional)[3].

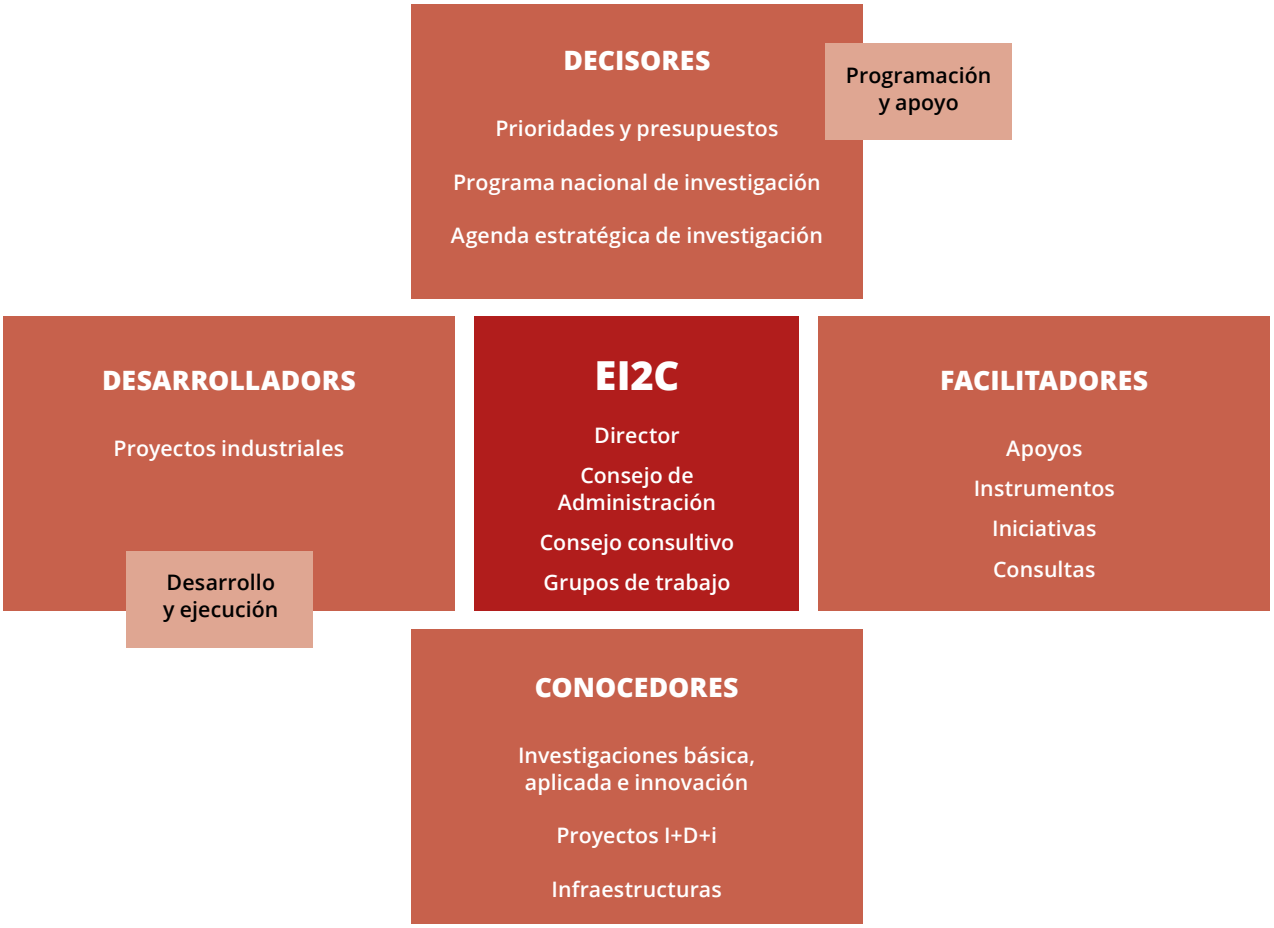


Figura 6: Programación y ejecución de los proyectos

Una vez aprobados, la gestión de cada proyecto industrial, tecnológico o mixto se coordinaría con el CNC a efectos de seguimiento y apoyo hasta su ejecución final. Cada responsable de proyecto rendiría cuentas a la dirección del CNC y, a su vez, esta lo haría respecto a las autoridades o demandantes que hayan solicitado el proyecto. Finalmente, el CNC informaría a la comunidad del estado y desarrollo de los proyectos para fomentar la distribución de sus resultados.

[3] Dos posibles aplicaciones de integración son:

• Elaboración de las prioridades ECSO para el programa Horizonte Europa 2021-2027 [15]

• Desarrollo de la línea estratégica sobre seguridad civil en materia de ciberseguridad establecida en la Estrategia Española de Ciencia y Tecnología (EECTI 2021-2027) [26]

El EI2C debería especializarse competencialmente en la investigación aplicada a la industria de ciberseguridad para facilitar la escala y la distribución y transferencia de conocimientos, infraestructuras y financiación entre toda la comunidad de investigación e industria.

Esto apunta a un modelo propio con autonomía funcional y conectable a otros ecosistemas y subsistemas, sea cual sea su nivel o ámbito. A efectos prácticos, se diferencia entre el ecosistema o subsistema en sentido amplio (la comunidad) y el núcleo de la gobernanza (el hub) encargado de dinamizar su actividad.

Para coordinar el EI2C hacia adentro y conectarlo hacia afuera se necesita, por un lado, un centro de coordinación (hub) en el que se inserten los distintos actores y, por otro, unos instrumentos tractores y de gestión atractivos. La carencia de mecanismos de coordinación e instrumentos de incentivos explica el limitado desarrollo de las líneas y medidas de acción de la Estrategia Nacional de Ciberseguridad. Al mismo tiempo, cabe destacar que algunas de las propuestas formarían parte de políticas más transversales que impulsarían la investigación y la industria en otros sectores también.

El hub es el corazón del EI2C y su elemento de impulso e interacción con toda la comunidad industrial y tecnológica. Debe conectar la comunidad nacional con la europea y su organización, pendiente de aprobación reglamentaria, debería ser compatible con la del Centro Europeo de Competencia en Ciberseguridad (CEC) y la Red de Centros Nacionales de Coordinación (CNC) y la Comunidad de Competencias de la UE [31].

En la Tabla 6 se desdobla la estructura del CEC y la posible del CNC, su espejo nacional.

	Centro Europeo de Competencia en Ciberseguridad (CEC)	Centro Nacional de Coordinación (CNC)
Participantes	Estados Miembros Comisión Europea	Comunidad
Ejecución	Consejo de Administración Director ejecutivo	Consejo de Administración Director ejecutivo
Asesoramiento	Consejo Consultivo Industrial y Científico (CCIC)	Órgano Consultivo
Participación	Comunidad de Competencias de Ciberseguridad (CCC)	Órgano abierto tipo Foro
Recursos	Presupuestos propios o comunes (Europa Digital, Horizonte Europa, Fondo Europeo de Defensa)	Presupuestos públicos y privados
Financiación de proyectos	Cofinanciación a partes iguales (todos opinan, pero deciden los que invierten)	Cofinanciación a definir
Conectividad	Abierta (con todos los actores afines dentro y fuera del ecosistema)	

Tabla 6: Estructura funcional comparada entre CEC y CNC

Si se pretende equiparar el modelo español con el europeo, la CPP debería contar con un Centro Nacional de Coordinación, Centro Espejo o *hub* que sea el interlocutor nacional con el Centro Europeo de Competencia en Ciberseguridad de Bucarest. El centro debería organizarse en una estructura como la establecida en la propuesta de Reglamento de la Comisión (Figura 6).

Figura 7: Estructura de gobierno del EI2C

El CNC podría desarrollar algunas de las tareas que se llevan a cabo en el modelo CPP de la Comisión y ECSO que se enumeran a continuación, bajo un esquema de grupos de trabajo (ver Figura 8):

· **Coordinación científico-técnica**: evaluar la situación, identificar tecnologías y la agenda estratégica de investigación e innovación (coordinación científico-técnica, academia y centros tecnológicos).

· **Coordinación de las políticas de industria e innovación**: coordinar las distintas áreas de gestión.

· **Definición de áreas de aplicación para la industria y la Administración**. Identificar tecnologías y servicios (encriptación, gestión de riesgo, privacidad, seguridad) y validación de aplicaciones (industria, energía, sanidad, transporte, IoT).

· **Desarrollo de mercado**. Instrumentos de inversión y explotación, certificación, estandarización, regulación.

· **Formación, educación, simulación, *re-skilling*, gestión de talento**.

· **Apoyo estratégico a sectores críticos** de la cadena de suministro, pymes, clústeres.

· **Evaluación y difusión**.

Las áreas de trabajo pueden gestionarse según la complejidad mediante grupos de trabajo o comités ejecutivos en los que participarían los miembros de la comunidad implicados en una estructura similar a la CPP de ECSO y la Comisión Europea, tal y como refleja la Figura 8.

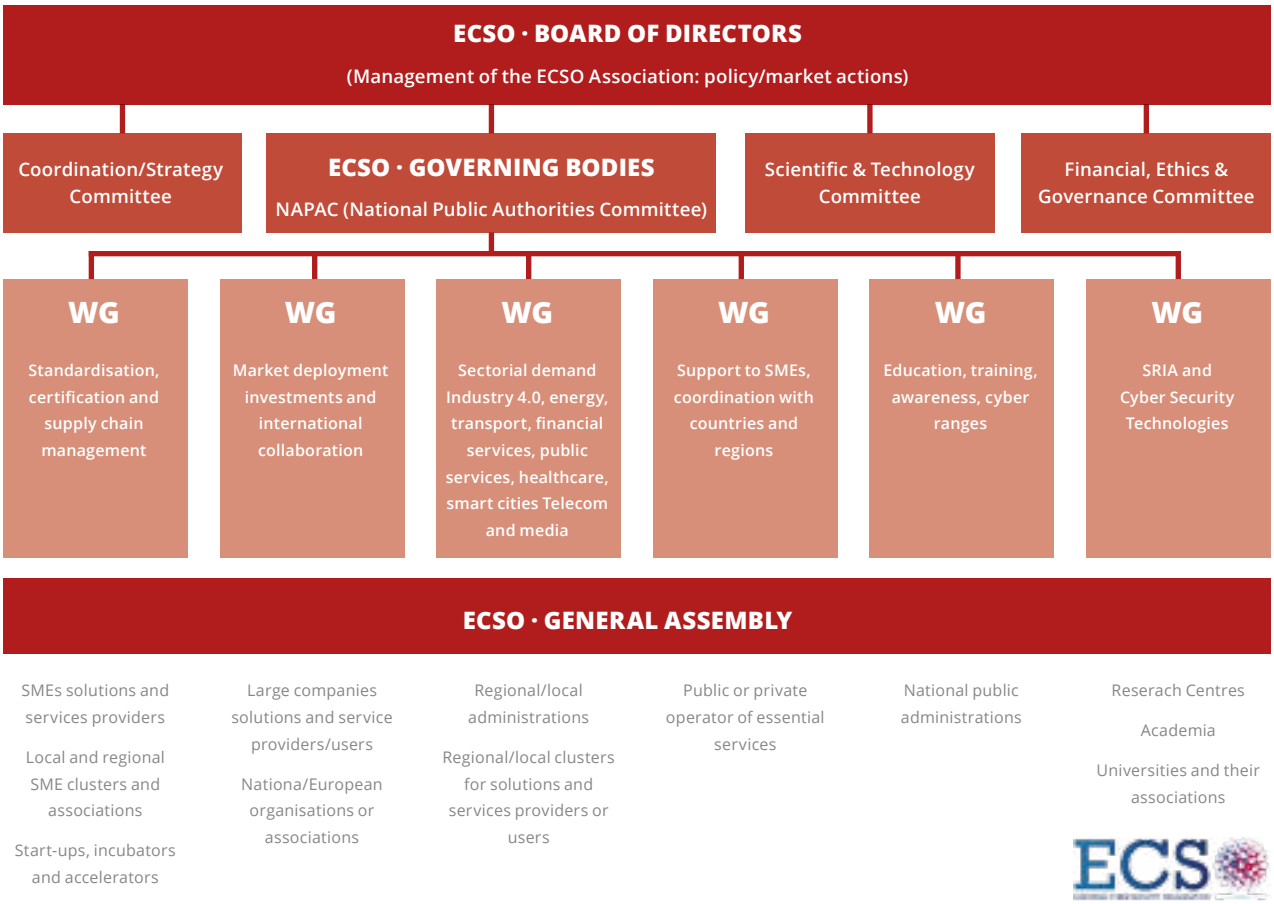


Figura 8: Estructura de CPP entre ECSO y Comisión Europea

3.3.2. Instrumentos de colaboración

Los instrumentos aplicables a la industria y la investigación de ciberseguridad son similares a los de otros sectores, con la particularidad de su posible impacto sobre la seguridad nacional y la necesidad de que los instrumentos del EI2C sean atractivos para incentivar la participación de los miembros.

3.3.2.1. Instrumentos financieros

Crear un presupuesto nacional de ciberseguridad con la designación expresa de los fondos disponibles para desarrollar la línea de acción 5 de la ENCS. Su creación, cuantía y finalidad deben figurar en el Plan Nacional de Ciberseguridad.

Entre otras medidas, se propone evolucionar la cultura de inversión en empresas de base tecnológica frente al modelo inversor en activos materiales y la realización de un estudio comparado de prácticas de financiación en ecosistemas nacionales, así como identificar los modelos y prácticas de financiación vigentes.

3.3.2.2. Agenda estratégica de investigación.

Definir las capacidades tecnológicas e industriales de ciberseguridad críticas para la seguridad nacional y los instrumentos para desarrollarlas. Su elaboración debe figurar en el Plan Nacional de Ciberseguridad.

Definir una agenda estratégica de investigación e innovación para incrementar la autonomía tecnológica e industrial y coordinar las prioridades y programas públicos y privados. Al ser una primera experiencia, el INCIBE debería conformar un grupo informal para elaborarla antes de la operatividad del Centro Nacional de Coordinación.

Junto a una agenda, necesaria para la programación a medio y largo plazo, se sugiere la necesidad de facilitar la programación de prioridades no contempladas previamente. En este sentido, se recomienda emular la práctica de CPP del Departamento de Seguridad Nacional de Estados Unidos (DHS) que solicita a las pequeñas empresas innovadoras que colaboren en la definición de un programa anual de licitación a través del Small Business Innovation Research (SBIR) [15].

Otra buena práctica es la de los temas abiertos (open topics) del programa Horizonte Europa, que sirven para resolver problemas concretos y urgentes de seguridad en los que se definen necesidad, fondos y condiciones de licitación[4].

Corresponde al EI2C elaborar una Agenda Estratégica de Investigación alineada con las prioridades generales y con las suyas propias y, sobre ella elaborar un Programa de Investigación en ciberseguridad.

3.3.2.3. Otros instrumentos de colaboración

Articular los instrumentos de inversión, gestión y apoyo necesarios para que el Centro Nacional de Coordinación pueda centralizar la demanda y la oferta nacional. Los incentivos para la colaboración público-privada deben coincidir con su disponibilidad operativa.

En un sistema de innovación abierta como el que se propone, el funcionamiento eficaz del EI2C depende de la capacidad de observación del mercado y las tecnologías, su conexión con las prioridades industriales y de investigación, la consulta a las bases de datos de capacidades nacionales y la identificación de los instrumentos de apoyo, entre otros, en un punto de contacto único.

[4] Open Topic (Horizon-CL3-2022-BM-01-04), presupuesto (€ 3,5 millones), tipo (I+D), condiciones (participantes, países, requisitos...), nivel tecnológico (TRL 5-7).

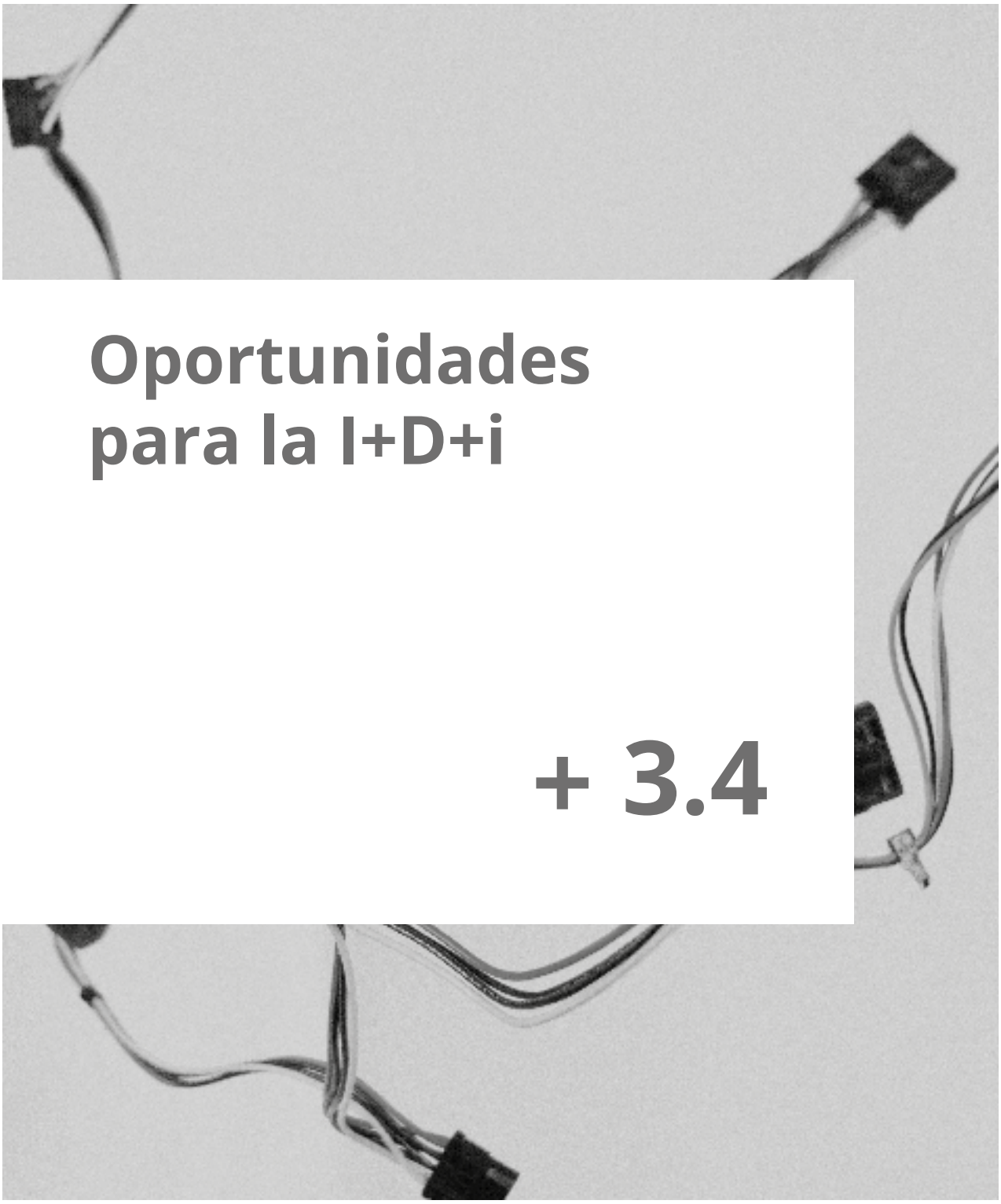
La centralización se refiere a delegar en el *hub* la articulación de los instrumentos de gestión necesarios para asegurar la coordinación del EI2C, especialmente en su Dirección y Consejo de Administración. El *hub* es un facilitador en beneficio del conjunto, sin perjuicio de los mecanismos de colaboración que se establezcan para cada proyecto.

El *hub* tendrá que asumir la coordinación del EI2C hacia el exterior y hacia el interior, mediante su conexión con los nodos y redes que desarrollen funciones similares (conectividad) para identificar oportunidades y retos al conjunto del EI2C[5].

Entre los instrumentos más importantes, están las bases de datos en elaboración por el Subgrupo de Trabajo 2, que deben permitir contrastar en tiempo real las necesidades con la oferta disponible según se ha explicado. Las bases de datos deben facilitar el emprendimiento y la asesoría, especialmente a las industrias y centros de investigación que no dispongan de capacidades autónomas. Estas ya disponen de servicios de asesoramiento diseñados por INCIBE para su seguridad, pero necesitan estar al tanto de las oportunidades de mercado, exportación, ayudas y prospectiva de mercado.

Potenciar la interconexión de los CERTs y CSIRTs ampliando la capacidad de servicios y apoyando que España pueda ser un *hub* Europeo y global de inteligencia de amenazas.

[5] En Francia, el proyecto Campus Cyber [2] aspira a crear un ecosistema de excelencia público-privado en cibeseguridad gestionada mediante una sociedad anónima simplificada (SAS).



Oportunidades para la I+D+i

+ 3.4

Los aspectos ligados a la ciberseguridad están impactando todos los sistemas modernos, desde las infraestructuras críticas hasta los derechos fundamentales del ciudadano. El reto no consiste solo en la defensa contra las ciberamenazas actuales, sino también en el desarrollo de capacidades futuras.

En este contexto, las oportunidades para la I+D+i deben orientarse a desarrollar capacidades esenciales para asegurar la economía digital, las infraestructuras, sociedad y democracia, protegiendo a los negocios y a los ciudadanos de ciberamenazas, reforzando la excelencia de los centros de I+D+i y aumentando la competitividad de la industria de ciberseguridad, y todo ello alineado con la ENCS (Estrategia Nacional de Ciberseguridad).

Este capítulo ofrece un análisis del estado de la I+D+i en ciberseguridad a nivel nacional y formula propuestas de acción para alcanzar los objetivos de la ENCS, con el objetivo de alcanzar una posición de liderazgo de la I+D+i española en ciberseguridad a nivel internacional.

Figura 9: Agentes de la investigación

Fruto del diagnóstico, se ha elaborado un análisis DAFO, donde se identifica un listado de debilidades, amenazas, fortalezas y oportunidades alrededor de cada uno de los cuatro ejes anteriores, que a su vez ha dado lugar a un análisis CAME, donde se recoge una primera relación no estructurada de acciones que podrían contribuir a corregir, afrontar, mantener y explotar las conclusiones del DAFO. Tanto el DAFO como el CAME se presentan en el Anexo XI.

Tomando como partida los objetivos establecidos por la Estrategia Nacional de Ciberseguridad, las actividades que se identifican para reforzar el ámbito de la I+D+i centran su prioridad en alcanzar las siguientes metas:

· Conocer la situación actual de las capacidades de I+D+i en España.

· Identificar oportunidades viables de posicionamiento en nichos con baja madurez y alto potencial.

· Mejorar el reconocimiento exterior de España como lugar donde se produce I+D+i de vanguardia en ciberseguridad.

· Reducir la dependencia tecnológica, así como mejorar la protección del tejido empresarial e institucional.

· Mejorar los modelos de inversión en I+D+i de ciberseguridad en todos los ámbitos donde tiene lugar.

· Aumentar la eficiencia de las inversiones relacionadas con I+D+i y emprendimiento en ciberseguridad.

· Dinamizar la transferencia de personas y tecnología entre la Red de Ciencia, Tecnología e Innovación (Universidades y Centros Tecnológicos) y las empresas.

· Paliar el déficit de talento en I+D+i.

Con el propósito de alcanzar los objetivos marcados, se identifican las siguientes actividades a nivel general que condensan todas acciones identificadas en el análisis CAME. Cada una de las actividades se fundamenta en la respuesta a las necesidades planteadas por la Estrategia Nacional de Ciberseguridad en sus objetivos III y IV y líneas de acción 4 y 5 (ver Figura 2: Líneas de acción de la Estrategia Nacional de Ciberseguridad).

Actividad	Medidas de la Estrategia Nacional
Definir una agenda estratégica de investigación (SRIA) en ciberseguridad a nivel nacional.	LA_5: M_1, M_2, M_3, M_5 y M_8
Realizar un estudio comparativo de las capacidades I+D+i y la financiación pública y privada.	LA_5: M_1
Definir un modelo de financiación de la I+D+i orientado a las prioridades de la SRIA.	LA_5: M_1, M_2, M_3 y M_9
Impulsar la creación a nivel nacional de un proyecto a imagen de los 4 pilotos europeos (SPARTA, CyberSec4Europe, ECHO y CONCORDIA), que permita articular una red de competencia en ciberseguridad a nivel español.	LA_5: M_3, M_5 y M_8
Crear un mapa exhaustivo de capacidades en I+D+i de ciberseguridad más completo y detallado que el actual, que contemple la I+D+i empresarial y las disciplinas de especialización surgidas en cada nodo.	LA_5: M_1, M_2, M_3, M_8 y M_9
Lanzar una campaña de promoción de la calidad de la tecnología nacional de ciberseguridad que inculque confianza y dé a conocer el intenso trabajo que se está realizando.	LA_5: M_2 y M_8
Asegurar que las acciones identificadas para paliar el déficit de talento existente en el sector de ciberseguridad contengan medidas específicas orientadas a las necesidades de personal investigador y de innovación.	LA_5: M_6, M_7 y M_8
Evolucionar la cultura de inversión en empresas de base tecnológica relacionadas con la ciberseguridad.	LA_4: M_2, M_5 y M_8 LA_5: M_1, M_2, M_3, M_4 y M_9
Fomentar el consumo de la industria nacional.	LA_5: M_1, M_2, M_3 y M_9

Tabla 7: Relación entre actividades y medidas de la ENCS

3.4.1. Agenda estratégica de investigación (SRIA) en ciberseguridad

Definir una agenda estratégica de investigación e innovación para España en el ámbito de la ciberseguridad con su hoja de ruta asociada, de forma que se prioricen de forma clara los ámbitos de I+D+i de apuesta a nivel nacional y en donde deben centrarse los esfuerzos investigadores y de financiación.

La ambición de alcanzar una posición de liderazgo internacional será más viable si se orienta el trabajo con una perspectiva de especialización, seleccionando nichos con alto potencial de crecimiento, baja madurez de la competencia y que responda a retos de la industria nacional más internacionalizada.

En la elaboración de la SRIA se han de tener en cuenta a diferentes agentes públicos como las agencias de innovación (CDTI y organismos autonómicos semejantes) y/o emprendimiento, así como a los organismos cuya actividad esté directamente relacionada con la ciberseguridad.

Del mismo modo, tendrán un papel protagonista en el desarrollo de la agenda las universidades, centros tecnológicos y empresas de ciberseguridad especializadas. Por su parte, el valor de organizaciones como las infraestructuras críticas y esenciales, las empresas consumidoras y las asociaciones o clústeres de ciberseguridad residirá en su conocimiento de las necesidades actuales y de los retos futuros de la industria.

Para racionalizar los esfuerzos y sacar un mayor partido de los recursos que se asignen, conviene tener en cuenta que existen en Europa diferentes iniciativas que pueden servir de modelo para el desarrollo de la SRIA. Es destacable el esfuerzo llevado a cabo por la European Cyber Security Organisation (ECSO) en su grupo de trabajo WG6 y también los trabajos de cuatro pilotos europeos: SPARTA, ECHO, CONCORDIA y CyberSec4Europe.

En los cinco anteriores, hay destacada presencia de empresas y centros tecnológicos españoles o con sedes permanentes en España. En este sentido, cabe mencionar el taller realizado en el SGT2.5 en el que los cuatro pilotos y ECSO han presentado las SRIAs con sus correspondientes hojas de ruta.

La investigación y la innovación encontrarán mejores oportunidades de desarrollo si se orientan a las necesidades actuales y futuras de la industria, y teniendo en cuenta el carácter transversal de la protección la vinculación con tecnologías emergentes como redes 5G, computación cuántica, IA y otras.

Por ello, cobra especial importancia el establecimiento de espacios de diálogo con los agentes de la demanda y el aseguramiento de que la permanencia del subgrupo de trabajo de «Oportunidades para la I+D+i» se oriente con un enfoque de largo plazo.

Mientras se define la SRIA completa, se adelantan a continuación cinco líneas de investigación que seguro estarán incluidas y que, por tanto, se podrían iniciar antes incluso de formalizar la SRIA, que muy probablemente añadirá otras líneas.

3.4.2. Línea de investigación: Identidad digital

En esta línea de investigación de identidad digital, se plantea un piloto a nivel nacional, en colaboración público-privada, que permita diseñar y desarrollar un sistema global de gestión de la identidad digital descentralizado, auto soberano y portable, que ofrezca garantías de seguridad y privacidad, y que complemente al sistema actual de certificación digital (como los basados en DNIe) en aquellos escenarios para los que este no está concebido.

Para ello, previamente se investigarán las tecnologías más prometedoras en el ámbito de la identificación electrónica y la gestión de la identidad digital, como son las técnicas de inteligencia artificial aplicada a procesos biométricos y validación documental (fundamentales en los procesos de *onboarding* digital y alta de usuarios), las redes de comunicación basadas en registros distribuidos (o cadenas de bloques) junto con credenciales verificables (tal y como las define el W3C) y/o los contratos inteligentes (para los procesos de autenticación mediante el uso de identidades derivadas y/o los procesos de gestión del consentimiento informado).

Promover la protección de la identidad digital es una de las medidas definidas en la Estrategia Nacional de Ciberseguridad para impulsar la ciberseguridad de ciudadanos y empresas. Para ello, la gestión de la identidad digital debe ser una propiedad fundamental en la seguridad de los sistemas de información, así como la base de cualquier servicio o modelo de negocio proporcionado sobre redes de comunicaciones.

Históricamente, la verificación de la identidad se ha basado en tecnologías y modelos centralizados que se han ido quedando obsoletos. Los sistemas basados en usuario y contraseña han ocasionado problemas de usabilidad e innumerables incidentes de seguridad y privacidad. La aplicación de este modelo sobre los servicios descentralizados proporcionados en Internet implica que los usuarios deban crear identificadores separados y difíciles de recordar por cada servicio online que deseen consumir.

Además, la identidad digital se encuentra fragmentada y almacenada en los distintos proveedores de servicio y por ello controlada por múltiples terceras partes. Esto implica, en la mayoría de las ocasiones, asumir niveles de riesgo que no deberían ser aceptados ni por los usuarios ni por los propios proveedores de servicio.

Por otro lado, los mecanismos basados en identidad federada, donde la gestión de la identidad se delega totalmente a una tercera parte, denominada Proveedor de Identidad, solucionan algunos de los problemas vistos anteriormente. Sin embargo, esta aproximación presenta graves riesgos a la privacidad, especialmente en el caso de Proveedores de Identidad privados, ya que este tendrá la capacidad de aprender sobre los hábitos, costumbres y accesos en internet de los ciudadanos.

Otros mecanismos disponibles para la protección de la identidad digital son aquellos basados en el uso de certificados digitales. Aunque son una solución con un alto nivel de seguridad y funcionan muy bien en

escenarios como, por ejemplo, los relacionados con Administraciones Públicas (como es el caso del DNIe español), tienen algunas limitaciones importantes cuando se hace uso de ellos en Proveedores de Servicios privados (por ejemplo, una plataforma de e-commerce o una red social) o cuando se emplean para identificar objetos con capacidad computacional limitada. No en vano, por un lado, pueden ser una solución invasiva con la privacidad, ya que no es posible revelar exclusivamente los atributos de la identidad necesarios para utilizar un determinado servicio, sino que es necesario revelar la identidad en su totalidad (todo el contenido del certificado). Por otro lado, el modelo actual de certificados está concebido para ser utilizado por entidades (personas, procesos o dispositivos) durante un tiempo relativamente largo y que pueden ser identificados de manera unívoca por una Entidad de Registro y no tanto para dispositivos con baja capacidad de cómputo (como algunos dispositivos IoT) o máquinas virtuales creadas bajo demanda en un sistema cloud, edge o 5G, por ejemplo.

Por tanto, es necesario evolucionar los sistemas existentes y que funcionan bien en ciertos escenarios para hacerlos en primer lugar más usables (lo que ayudaría en su adopción masiva), al tiempo que se complementan con sistemas de identidad digital adaptados a nuevos escenarios de comunicaciones, donde que al mismo tiempo que se maximiza la privacidad de los ciudadanos y los objetos de computación, se proporcionan garantías a los proveedores de servicios, ya sean estos públicos o privados. Un sistema de identidad digital que potencie su adopción, tanto por parte de los usuarios como las organizaciones públicas y privadas. Para ello, deberá contar con las siguientes características fundamentales:

· universal, portable, usable y escalable
· autosoberano
· garante con la privacidad y
· seguro

3.4.3. Línea de investigación: Red de laboratorios 5G y Beyond 5G

Se plantea una red de laboratorios (testbeds) 5G a nivel nacional, en colaboración público-privada, que fomente sinergias entre operadoras, universidades, centros tecnológicos y empresas en aquellos sectores donde la adopción del 5G tenga mayor impacto.

Esta red dispondrá de infraestructuras descentralizadas por el territorio nacional en formato de laboratorios, interconectados para facilitar el desarrollo de pruebas sobre los diferentes dispositivos, casos de uso y servicios. Para maximizar el impacto los laboratorios se especializarán en distintos segmentos y verticales (automoción, energía, salud, industria 4.0, *smart buildings & smart cities*, etc.).

Esta misma red de laboratorios servirá de base para las tareas de investigación e innovación en las nuevas características que se esperan en escenarios que vayan más allá del actual 5G (Beyond 5G o B5G), prestando en las mismas, y desde su diseño, una especial atención a las funcionalidades relativas a la ciberseguridad y a la preservación de la privacidad de los actores que hacen uso de la misma.

En el prólogo de la Estrategia Nacional de Ciberseguridad se destaca la influencia de la implantación del 5G, que aumentará exponencialmente el uso de tecnologías de la conectividad, potenciando paradigmas como el internet de las cosas o el edge computing. Sin duda, la aplicación de esta tecnología a múltiples sectores y casos de uso proporcionará grandes beneficios, pero también nos hará más vulnerables a acciones hostiles contra (y desde) estas nuevas infraestructuras.

Por ello, es fundamental el impulso de la ciberseguridad en el diseño, despliegue y operación de las infraestructuras 5G y en las nuevas arquitecturas mejoradas B5G (Beyond 5G) en las que ya se está trabajando a nivel de investigación. En la actualidad, el despliegue de la red 5G se está centrando en la capa de acceso, en convivencia con la generación anterior, por lo que su impacto es limitado, tanto en nuevas funcionalidades como en ciberseguridad.

Será en el futuro despliegue de 5G en el núcleo de las redes y su adopción masiva para proporcionar nuevos servicios sobre ellas cuando las consideraciones de ciberseguridad sean críticas.

Esta red de laboratorios de 5G y B5G servirá como entorno abierto de experimentación a diferentes actores del tejido productivo como empresas y otros organismos públicos y privados, para la ciberseguridad de:

· Nuevas tecnologías que formen parte de las futuras redes de comunicaciones celulares 5G y posteriores generaciones (equipos y componentes hardware de infraestructura, dispositivos inteligentes, funciones virtualizadas de red y radio, herramientas de gestión de las redes celulares, etc.).

· Nuevas tecnologías que formen parte de las futuras redes de comunicaciones celulares 5G y posteriores generaciones (equipos y componentes hardware de infraestructura, dispositivos inteligentes, funciones virtualizadas de red y radio, herramientas de gestión de las redes celulares, etc.).

· Nuevos productos, aplicaciones y servicios que hagan uso de la red celular para diferentes sectores verticales.

Desde el punto de vista tecnológico, los laboratorios se especializarán en la protección, detección de ataques y recuperación en distintas capas de los protocolos.

Se investigarán nuevos mecanismos de seguridad radio que puedan ser integrados en la infraestructura de las redes 5G y posteriores generaciones. Dichos mecanismos están orientados a proteger las redes celulares frente a ataques de radiofrecuencia que supongan una amenaza, tanto desde un punto de vista de la confidencialidad de los datos como de su propia disponibilidad (estaciones base falsas, uso ilegal de recursos espectrales, *jamming*, *spoofing*, etc.).

Otro de los elementos cruciales dentro del 5G, y también fuera de él, es el paradigma del Edge Computing. Este permite optimizar servicios del cloud, como la virtualización de recursos, mediante su despliegue en entornos cercanos a los usuarios finales. Aunque estándares como el ETSI MEC han

considerado la ciberseguridad como un elemento crucial en el diseño de sus arquitecturas, existen aún numerosos retos de seguridad y privacidad que deben considerarse.

Uno de ellos es el uso y aplicación de elementos seguros (SE) y módulos de plataforma de confianza (TPM / TEE) para integrar servicios de seguridad básicos (autenticación de servidores) y avanzados (atestación de servicios). Otros retos incluyen el estudio de la seguridad en la integración de mecanismos de virtualización ligeros como contenedores, la integración de mecanismos que permitan detectar y reaccionar ante la presencia de anomalías y ataques dentro de la infraestructura, y herramientas para preservar la privacidad de los usuarios que utilicen o accedan a servicios del Edge.

Además, debe analizarse la problemática de la seguridad y privacidad en la migración de servicios entre distintos proveedores y la movilidad de los dispositivos del usuario, aspectos cuyo desarrollo actual es muy limitado.

Más allá de la protección de las propias infraestructuras Edge, también es necesario explorar los retos y oportunidades que nos ofrece el uso del Edge para desplegar servicios de seguridad, conocido como SecaaS en inglés. El principal desafío en este campo es la integración de mecanismos que permitan no sólo administrar el ciclo de vida de los diversos SecaaS, sino facilitar la interacción y cooperación entre los diversos servicios.

Otros desafíos están relacionados con el desarrollo de servicios de gestión de credenciales (incluyendo seudónimos y revocación) en escenarios de alta movilidad, servicios de confianza para la interacción de múltiples usuarios, aplicaciones y recursos, y servicios orientados a la difusión de información de inteligencia (*threat intelligence*) o gestión de evidencias electrónicas.

Asimismo, es necesario prestar especial atención a los retos de seguridad y privacidad de uno de los principales casos de uso del 5G y el paradigma Edge: internet de las cosas, o IoT. Esto es debido a que aún existen muchos desafíos por resolver, como la integración de soluciones basadas en HW como los elementos seguros y los physical unclonable functions (PUF), la existencia de modelos de confianza y reputación, el uso de esquemas de identidad para dispositivos IoT, la disponibilidad de herramientas de análisis forense, y la incorporación de mecanismos de detección temprana de vulnerabilidades.

Dichos desafíos son aún más relevantes en el ámbito de la internet de las cosas Industriales, o IIoT. La aplicación de la IIoT permite aumentar las ventajas competitivas en el entorno industrial, proporcionando un mayor control del contexto en términos operativos, funcionales y de servicios. Sin embargo, este acoplamiento implica una mayor exposición a amenazas y vulnerabilidades, lo que puede afectar la disponibilidad e integridad de recursos esenciales.

Es por ello necesario hacer énfasis en mecanismos de seguridad tales como la prevención y la detección de anomalías con soporte en inteligencia artificial, la trazabilidad y la respuesta a ataques, y la restauración de servicios en tiempo real, y todo ello midiendo el impacto que tiene la inclusión de servicios complejos de seguridad en estos contextos. Adicionalmente, se pondrá el foco en la aplicación de criptografía ligera en la protección de la información en dispositivos donde, por sus limitaciones de cómputo o de consumo de energía, no es posible el uso de criptosistemas de mayor complejidad. Finalmente, también hay que prestar atención a la certificación de los dispositivos IoT e IIoT, incluyendo los mecanismos que permitan acelerar dicho proceso.

3.4.4. Línea de investigación: seguridad e inteligencia artificial

Abrir una línea estratégica de investigación en Seguridad e Inteligencia Artificial con su hoja de ruta asociada, que sirva como marco de actuación de apuesta a nivel nacional para lograr estar a la vanguardia científico-tecnológica en esta área de especialización y poder transferirla a la industria.

Se ha escogido esta línea de investigación porque responde a retos de la industria nacional actual y se ha identificado como una de las 10 líneas de investigación más relevantes a nivel nacional, tal y como aparece en el documento Catálogo y Mapa del Conocimiento de la I+D+i en Ciberseguridad en España (abril 2021).

Por otra parte, esta línea de investigación está alineada con la línea de acción 1: Reforzar las capacidades ante las amenazas provenientes del ciberespacio definida en la Estrategia Nacional de Ciberseguridad, y más concretamente con las medidas 1, 6 y 11.

Esta línea de investigación abarca desde la investigación en la utilización de la Inteligencia Artificial para reforzar la ciberseguridad a la investigación en la ciberseguridad y privacidad de la propia IA:

· Explorar la utilización de la Inteligencia Artificial para reforzar la ciberseguridad durante las fases de Identificación, Protección, Detección, Respuesta y Recuperación.

· Crear técnicas y métodos que faciliten el diseño, desarrollo, validación y despliegue de sistemas prácticos basados en Inteligencia Artificial, con un enfoque multicriterio 3S: seguridad del dato, seguridad del modelo y seguridad del resultado que garanticen la privacidad, equidad, trazabilidad, robustez, confiabilidad, causalidad, explicabilidad y transparencia, así como desplegabilidad y gobernanza del dato.

3.4.5. Línea de investigación: seguridad y comunicaciones cuánticas

Abrir una línea estratégica de investigación en tecnologías cuánticas aplicadas a los desafíos de ciberseguridad existentes y emergentes, con su hoja de ruta asociada, que sirva como marco de actuación de apuesta a nivel nacional para lograr estar a la vanguardia científico-tecnológica en este área de especialización y poder transferirla a la industria.

Se ha escogido esta línea de investigación porque responde a retos de la industria nacional actual y se ha identificado como una de las 10 líneas de investigación más relevantes a nivel nacional tal y como aparece reflejado en la Estrategia Europea de Ciberseguridad para la Década Digital en donde se habla de la creación de una infraestructura de comunicación cuántica segura para Europa.

Esta línea de investigación implica las tecnologías cuánticas aplicadas a los desafíos de ciberseguridad existentes y emergentes afectados por el volumen, la sofisticación y la complejidad de las metodologías de ataque modernas:

· Investigación en criptografía cuántica: desarrollo de criptografía adaptada a la computación cuántica.

· Investigación en criptografía post cuántica: cómo hacer que la criptografía actual sea resistente a la computación cuántica.

· Comunicaciones cuánticas seguras basadas en Quantum Key Distribution.

· Creación de una infraestructura cuántica de experimentación mediante la creación/extensión de una red de nodos de comunicaciones cuánticas.

3.4.6. Línea de investigación: seguridad por diseño, gestión de ciberseguridad y cadena de suministro

Abrir una línea estratégica de investigación en seguridad por diseño, gestión de ciberseguridad y cadena de suministro, con su hoja de ruta asociada, que sirva como marco de actuación de apuesta a nivel nacional para lograr estar a la vanguardia científico-tecnológica en esta área de especialización y poder transferirla a la industria.

Se ha escogido esta línea de investigación porque responde a retos de la industria nacional actual y se ha identificado como una de las 10 líneas de investigación más relevantes a nivel nacional tal y como aparece en el documento Catálogo y Mapa del Conocimiento de la I+D+i en Ciberseguridad en España (Abril 2021).

Esta línea de investigación está alineada con la línea de acción 5 definida en la Estrategia Nacional de Ciberseguridad, concretamente con la medida 3 que establece: incrementar las actividades nacionales para el desarrollo de productos, servicios y sistemas de seguridad, y la seguridad desde el diseño, apoyando específicamente aquellas que sustenten necesidades de interés nacional para fortalecer la autonomía digital, y la propiedad intelectual e industrial.

Finalmente, esta línea también responde a las necesidades establecidas en el reglamento europeo de la Ciberseguridad (Cybersecurity Act) que establece un marco de certificación europeo que aumente la confianza en los productos, servicios y procesos de TIC que hayan sido certificados con arreglo a los distintos esquemas europeos de certificación que se diseñen. Estos esquemas deberán incorporar entre sus objetivos que los

productos, servicios y procesos de TIC sean seguros por defecto y desde el diseño.

Esta línea de investigación es una línea transversal que puede incorporar las siguientes actividades (no excluyentes):

· Metodologías o procedimientos que permitan lograr seguridad y privacidad por diseño.

· Metodologías o herramientas que garanticen la construcción de *hardware* y *software* seguro.

· Métodos o herramientas que garanticen que los componentes de terceros y de código abierto estén libres de vulnerabilidades, debilidades y/o *malware*.

· Métodos y entornos para la codificación segura por diseño.

· Metodologías y entornos que permitan una evaluación integral y eficaz de la seguridad, incluyendo aspectos del marco de certificación de la UE.

· Metodologías para una gestión ágil de la ciberseguridad en todo el ciclo de vida

· Monitorización de seguridad.

· Gestión de incidencias o protección frente amenazas.

· Gestión de actualizaciones.

· Métodos o procedimientos para hacer seguras las cadenas de suministro.

· Realidad aumentada aplicada a la ciberseguridad en ámbitos IT, OT e IoT.

3.4.7. Estudio comparativo de las capacidades de I+D+i y modelo de financiación

Llevar a cabo un estudio comparativo de las capacidades I+D+i y de los modelos de financiación. Tomar como referencia modelos de financiación pública y privada diferentes al español y que puedan considerarse casos de éxito.

Actualmente se carece de información contrastada sobre el posicionamiento internacional del subsistema investigador español en relación con la ciberseguridad. Sin ese conocimiento, se corre el riesgo de tomar decisiones incorrectas para mejorar el posicionamiento frente a posibles competidores que busquen ubicarse en los nichos de oportunidad a los que aspire España.

Es necesario identificar un número manejable, pero suficientemente diverso, de referentes (no más de 10) que puedan servir como modelos de mejores prácticas en I+D+i de ciberseguridad o de disciplinas digitales en general. Preferiblemente, deberían elegirse una mayoría de entornos (7 u 8) con modelos legislativos susceptibles de encajar con la estructura de Estado que caracteriza a España, dejando también espacio a unos pocos ejemplos menos afines (Israel, Singapur), pero de los que se pudiera extraer buenas prácticas interesantes.

Dentro del estudio, entre otras cosas, debería identificarse la cantidad de universidades, centros tecnológicos y unidades I+D+i empresariales en otros países competidores y su posicionamiento en rankings globales porque supondrán una amenaza en términos de competir por talento, ideas y financiación de proyectos y *startups*.

Las conclusiones del estudio deberían estar orientadas a seleccionar y priorizar la puesta en marcha de los instrumentos más adecuados que sirvan específicamente para financiar las líneas de investigación que formen parte de la SRIA. A corto plazo sería más ágil integrarlos en programas existentes y a medio-largo plazo convendría definir futuros programas.

Se espera que la evolución de los modelos de financiación traiga beneficios tangibles porque creará las condiciones para que el talento investigador pueda mejorar su desempeño.

Es esencial enriquecer con los programas nacionales de financiación de la I+D+i a universidades y centros tecnológicos para que se convierta en un instrumento de carácter competitivo, que fomente la colaboración y cohesión, y basado en la excelencia e indicadores, más dirigido a aquellas prioridades relacionadas con la Estrategia Nacional y con la SRIA que se defina.

Las tecnologías digitales, campo en el que se enmarcan las de ciberseguridad, son un campo de juego donde la competencia ha de entenderse en clave global y, por ello, para el estudio, es necesario tener en cuenta cómo están avanzando en otras áreas geográficas.

En términos generales, aspirar hoy en día a ejercer un liderazgo internacional parece un reto difícil de alcanzar si tenemos en cuenta que la inversión de España en I+D+i (1,25% del PIB) se encuentra muy lejos de la media actual de la UE (2,18%), destacando por proximidad Suecia (3,3%) o Alemania (3,1%). También merecen mención los Estados Unidos de América (2,8%) o ciertos países de Asia como Israel (4,9%), Corea del Sur (4,5%) o Japón (3,2%).

3.4.8. Cyber Competence Community: piloto español

Creación a nivel nacional de un proyecto a imagen de los cuatro pilotos europeos (SPARTA, CyberSec4Europe, ECHO y CONCORDIA), que permitan articular una red de competencia en ciberseguridad a nivel español que desarrolle e implemente acciones colaborativas de investigación, innovación y capacitación de primer nivel, en diferentes ámbitos y experiencia, desde la investigación básica a la aplicada y tanto en el entorno académico como en el industrial, para dar forma a una comunidad de ciberseguridad española alrededor del centro espejo de competencias en ciberseguridad, desde donde se gobernaría una estructura de nodos.

El objetivo es crear una comunidad duradera capaz de colaborar para definir, desarrollar, compartir y desarrollar soluciones que ayuden a los profesionales a prevenir el cibercrimen y mejorar la ciberseguridad para proteger a la industria, a las instituciones públicas y a la ciudadanía.

Actividades que se podrán articular en el ámbito de este proyecto:

· Definición y articulación de la gobernanza de la comunidad.

· Elaboración de una agenda estratégica de investigación con su roadmap asociado.

· Identificación de comunidades de alta concentración para arrancar con masa crítica de proyectos, empresas y talento, así como generar casos de éxito de manera temprana.

· Proyectos específicos de I+D que permitan articular la investigación.

· Actividades de capacitación y de sensibilización.

· Actividades de apoyo a la certificación en varias vertientes: personas, organizaciones y productos.

· Actividades de diseminación y comunicación.

· Coordinación de infraestructuras de investigación.

Entre los participantes, se contaría tanto con entidades públicas como privadas de investigación, empresas y startups, CERTs, clústeres y todas aquellas entidades que formen parte de la cadena de valor de la ciberseguridad y de su I+D+i.

3.4.9. Campaña de promoción de la tecnología nacional

La acción que se propone es una campaña institucional a todos los niveles en España y Europa para dar a conocer la tecnología propia y construir confianza alrededor del uso de esa tecnología. Una acción desarrollada, desde 2021 hasta 2023, haciendo uso de medios de comunicación masivos como radio y televisión, diseñando una campaña muy fuerte en medios digitales, haciendo uso de las palancas que garanticen el éxito de la campaña.

Es una campaña orientada a personas de instituciones europeas, empresas europeas y españolas, organismos nacionales y ciudadanos en general. Una campaña masiva para prestigiar la tecnología propia que fomente su consumo y, por tanto, la apuesta por su desarrollo. Debería incluir, incluso, la posibilidad de montar centros móviles demostradores de las tecnologías nacionales seleccionadas y también la posibilidad del desarrollo de pilotos para poder poner a prueba la calidad de las soluciones presentadas.

Uno de los objetivos clave de la estrategia europea para los próximos años es el desarrollo de un mercado único digital fuerte, tal y como se recoge en *Making Europe's businesses future-ready: A new industrial strategy for a globally competitive, green and digital Europe*.

En este sentido, Europa necesita tener cierto grado de independencia tecnológica en aspectos clave como son la inteligencia artificial, *big data*, cloud, Internet de las cosas o ciberseguridad, entre otros. Así se recoge en las estrategias de inversión en I+D+i de Europa para los próximos años y en las declaraciones que personas relevantes de la UE hacen de forma continua.

The role of R&I investments in building a better future for Europeans[6]:

Horizon Europe, the next EU research and innovation programme, will drive the systemic changes needed to ensure a green, healthy and resilient Europe. Its instruments such as the European Innovation Council, EU missions and European Partnerships are important investments to accelerate the achievement of the green and digital goals, while strengthening Europe's global leadership and technological sovereignty.

Observaciones del presidente Michel tras el Consejo Europeo extraordinario del 2 de octubre de 2020:

Nos fijamos una alta aspiración: la soberanía digital. Entendemos por tal un mercado único verdaderamente digital, en el que definimos nuestras propias normas, tomamos decisiones tecnológicas autónomas y desarrollamos nuestras propias soluciones digitales.

Por tanto, la soberanía digital entendida como la autonomía estratégica en el ámbito digital es uno de los objetivos perseguidos por todos los programas de la UE.

[6] https://ec.europa.eu/info/news/role-ri-investments-building-better-future-europeans-2020-nov-27_en

La ciberseguridad es una de las tecnologías habilitadoras clave para el desarrollo de ese mercado digital europeo y, como tal, la UE también se marca como objetivo el desarrollo de una industria de ciberseguridad fuerte y la independencia tecnológica frente a otras potencias extranjeras. De hecho, la nueva estrategia de ciberseguridad de la UE[7] incide en cómo puede aprovechar y fortalecer todas sus herramientas y recursos para ser tecnológicamente soberana, estableciendo tres áreas de acción siendo la primera de ellas *resilience*, *technological sovereignty and leadership*.

Si Europa quiere fomentar el desarrollo de tecnología propia para avanzar en el camino de la independencia tecnológica, necesita que el sector privado especializado en ciberseguridad se involucre en el proceso. Hasta ahora, el sector privado ha optado por el uso de tecnología de otros países al no encontrar un incentivo claro para el desarrollo de tecnología propia que apuntale su desarrollo empresarial y España no ha sido una excepción.

Las grandes compañías europeas y españolas se encuentran cómodas utilizando tecnologías anglosajonas, israelíes e incluso rusas y chinas.

Tanto a nivel nacional como europeo, no se han acometido acciones coordinadas para fomentar el consumo de tecnologías autóctonas que faciliten el desarrollo de cierto grado de independencia tecnológica europea en detrimento de tecnologías foráneas.

Las universidades y los centros de investigación han desarrollado programas de I+D+i en materia de ciberseguridad al amparo de los programas de apoyo europeos, pero este desarrollo tecnológico no ha estado alineado con el desarrollo empresarial, por lo que los avances que se han conseguido en I+D+i en ciberseguridad no han sido utilizados por compañías nacionales o europeas, han quedado en el olvido, o han acabado en manos de capital no nacional o europeo.

Para revertir esta situación a nivel nacional, entre otras cosas, es necesario poner en valor de forma pública y masiva la alta calidad de los desarrollos tecnológicos españoles y la capacidad que tienen, trabajando en equipo, los sistemas universitarios, los centros de investigación y las empresas tecnológicas.

Es necesario trabajar la confianza de las empresas españolas en las tecnologías nacionales en materia de ciberseguridad, promocionando el uso de las mismas en igual o mayor medida que otras tecnologías de países terceros y mostrando las ventajas, en todos los sentidos, que tiene el apoyo al desarrollo de una industria española potente.

Para conseguirlo se propone el desarrollo de una Campaña de Promoción de la Calidad de las Tecnologías de Ciberseguridad Españolas que inculque confianza en el nuestro tejido empresarial y que ponga en valor el intenso trabajo que se está realizando en este campo.

Solo fomentando el uso de tecnologías propias por parte de organizaciones y empresas europeas, a través de darlas a conocer de forma masiva y transmitiendo la confianza necesaria, seremos capaces de construir un equilibrio entre los esfuerzos que ya está haciendo en I+D+i, con el desarrollo comercial dentro y fuera de nuestras fronteras de tecnología de ciberseguridad marca España.

Fomentemos pues, en primer lugar, el conocimiento y la confianza de nuestras instituciones, empresas y ciudadanos en los desarrollos tecnológicos nacionales y luego promocionemos esa tecnología incluso fuera de nuestras fronteras.

[7] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

Es una campaña que en definitiva trabajaría la marca España en tecnología de ciberseguridad y que podría diseñarse atendiendo a un esquema de fases:

Fase 0:

· Debe partir de formalizar el subsistema de pymes nacionales de soluciones de ciberseguridad a través de un estudio independiente alineado a la taxonomía ECSO para España.

· Identificar la demanda nacional dispuesta a participar de esta iniciativa, agrupada en sectores que permita trabajar la especialización de las pymes nacionales y realizar encuestas que permitan conocer el nivel de ciberseguridad que tienen y cómo la resuelven.

Fase 1:

· Diseñar un Plan de Comunicación para divulgar hacia la demanda la existencia de estas pymes nacionales de soluciones de ciberseguridad.

· Diseñar programas de subvenciones que incentiven el consumo de tecnología de ciberseguridad y que también actúen sobre inversiones o gastos que las empresas de ciberseguridad incurran para reforzar su oferta y promocionarse (por ejemplo, la construcción de demostradores o la participación activa en determinados eventos).

· Promover la realización de pruebas de valor entre oferta (pymes) y demanda (sectores).

· Incentivar en mayor medida la colaboración entre pymes de ciberseguridad para unir capacidades que permitan ofrecer soluciones más completas/complementarias.

· Involucrar a los centros de investigación nacionales en ciberseguridad.

Fase 2:

· Realización de las pruebas de valor.

· Divulgar los casos de éxito a nivel nacional, EU y LATAM.

Fase 3:

· Fomentar la internacionalización (hacia EU y LATAM) de las pymes nacionales mediante subvenciones que les permitan redimensionar sus estructuras y la realización de nuevas pruebas de valor con la nueva demanda internacional.

Generación, transformación retención y atracción de talento

+ 3.5

El talento en ciberseguridad es hoy un bien escaso. La competencia en un mercado global por este talento está produciendo un reajuste al alza del precio en el factor humano.

El impacto para la empresa no solo se cifra en el encarecimiento de los servicios de seguridad TI, sino en la sobreexplotación del personal a cargo, y una excesiva rotación en posiciones organizativas que manejan información sensible.

Falta un marco que defina y armonice roles a nivel europeo, catalogando las competencias y habilidades profesionales, que oriente a las empresas y trabajadores sobre el diseño de carreras profesionales, retribuciones equilibradas, etc.

Con el paso del tiempo se observa la aceleración de la divergencia entre las necesidades reales de las empresas fruto de su transformación digital y la capacidad del sistema educativo y productivo para generar profesionales cualificados y experimentados en todos los niveles del desempeño de tareas de seguridad de la información.

La institucionalización del I+D+i del sector público y su fragmentación regional no permiten a los organismos y centros de investigación adaptarse a la flexibilidad y tamaños necesarios para competir con propuestas comerciales extranjeras[8]. Resulta especialmente difícil para el sector público atraer y retener el talento en ciberseguridad.

En el sector privado el I+D+i en ciberseguridad tampoco se desvía mucho del tono general marcado por un bajo interés de las empresas [65]. Resulta paradójica la alta valoración social y empresarial de los investigadores e ingenieros españoles, tanto dentro como fuera de nuestras fronteras, que sin embargo no se ve recompensada en la práctica por la adquisición en España de los productos que estos desarrollan.

[8] A pesar de ello, excepcionalmente, las AA.PP. pueden contar con una excelente gama de productos y desarrollos propios en ciberseguridad, respaldados por el CCN.

3.5.1. Marco de habilidades y competencias profesionales

3.5.1.1. Taxonomía de roles en seguridad de la información

Definir un marco de perfiles profesionales que homologue a nivel europeo las competencias, habilidades y certificaciones profesionales. Se requieren profesionales con perfiles diferentes para los distintos niveles de desempeño en la empresa: gerenciales, arquitectura y diseño, operacionales, supervisores, etc. Estos perfiles y acreditaciones profesionales deben definirse con la mayor claridad posible y ser reconocidos a nivel europeo.

Elaborar planes de carrera profesional en ciberseguridad. Las empresas deberían disponer de una guía para diseñar itinerarios profesionales en los distintos niveles del desempeño: gerencia, tareas de apoyo y soporte, operacionales, supervisión, etc.

Las taxonomías estáticas resultan efímeras para este fin, debido a la dinámica de las tecnologías y de las empresas. Se hace necesario definir un proceso continuo y una organización que lo gestione en el tiempo. El resultado esperado de tal proceso debe ser la evolución en el tiempo del marco que define los roles, competencias, habilidades, itinerarios profesionales, certificaciones, etc., para que la fuerza de trabajo en ciberseguridad esté siempre alineada con las necesidades de la empresa privada y de las organizaciones públicas.

Los esfuerzos deben centrarse en adherirse a una iniciativa madura a nivel internacional que incorpore estas aspiraciones y no en promover un estudio local limitado. En un mundo globalizado resulta conveniente que exista una homologación o armonización de perfiles a nivel global, tanto para la empresa (sobre todo las multinacionales) como para los profesionales.

Uno de los paquetes de trabajo del proyecto piloto SPARTA dentro del programa H2020 tiene como objetivo el desarrollo del *Cybersecurity Skill Framework* (CSF) [79]. Además de presentar un enfoque dinámico, SPARTA está alineada con la iniciativa previa NICE [74], auspiciada por el NIST norteamericano.

Se ha creado un grupo de trabajo *ad hoc* [19] para impulsar la convergencia de este diseño organizativo y competencial en ciberseguridad promovido en el seno de SPARTA con la iniciativa NICE anteriormente mencionada y el marco general EN16234 e-CF (EU) [9] de competencias digitales. Este esfuerzo integrador podría suponer un freno al desarrollo de SPARTA, por lo que la propuesta es:

Adoptar el modelo SPARTA CSF y liderar de manera decidida su adopción en Europa, lo que implica que:

- **España adopte decididamente SPARTA CSF como marco de referencia para el desarrollo del diseño organizativo de la ciberseguridad en las empresas.**
- **Las AAPP adopten igualmente SPARTA CSF como «modelo de llegada» en la definición de itinerarios formativos y de certificación de profesionales en todos los niveles de desempeño definidos en el diseño organizativo citado anteriormente.**
- **España se postule para una presencia decidida y activa en los órganos de dirección de SPARTA CSF.**
- **Si los organismos europeos concernidos retrasaran excesivamente la adopción de esta iniciativa, España promueva un acuerdo de reconocimiento mutuo entre países interesados.**

La reciente publicación del RD 43/2021 [71] es un buen principio en el reconocimiento de la figura del Responsable de Seguridad de la Información (*Chief Information Security Officer*) tanto en el sector público como privado. No obstante, por similitud con lo que ocurre en el sector de la seguridad privada, deben reglamentarse y respaldarse oficialmente otras figuras organizativas.

Respaldar otras posiciones organizativas y perfiles profesionales de la ciberseguridad, además del Responsable de Seguridad de la Información.

Promover la armonización de la figura del Responsable de Seguridad de la Información a nivel europeo.

El desempeño en los puestos clave de las AAPP, tanto operacionales como de gestión de la seguridad de la información, debe quedar al margen de tensiones políticas o de presiones del mercado.

El objetivo es que dichos puestos sean ocupados por personal estatutario, independiente de poderes contingentes, remunerados de acuerdo al mercado, con movilidad geográfica y con las debidas garantías para su permanente actualización en conocimientos, habilidades y competencias.

Definición y creación de un Cuerpo Superior de Técnicos de Gestión de Riesgos de Ciberseguridad de la AGE y/o nuevas categorías profesionales para el personal de ciberseguridad al servicio de las AAPP.

Promover la colaboración entre centros de investigación de organismos públicos y empresas, con rotación del personal, comisiones de servicio, etc.

3.5.1.2. Cuantificación de las necesidades en España

INCIBE informará sobre la marcha y los resultados del servicio «Análisis y diagnóstico del talento en ciberseguridad en España» a los miembros del Foro Nacional de Ciberseguridad y al Consejo Nacional de Ciberseguridad.

Recientemente, INCIBE ha contratado [47] un servicio de análisis y diagnóstico del talento en ciberseguridad en España, entre cuyos objetivos se encuentran los siguientes:

· Cuantificar y segmentar la fuerza laboral actual de profesionales de la ciberseguridad en España y la demanda existente; así como sus características, conocimientos y habilidades en materia de ciberseguridad necesarias en cada uno de los segmentos (perfiles) identificados.

· Caracterizar la fuerza laboral requerida proporcionando detalles sobre estimaciones de brechas.

· Estimar la brecha actual de la fuerza laboral de ciberseguridad en España.

· Identificar las mejores prácticas en Gestión del Talento (GT) en las ocho economías globales con mayor madurez en el campo de la ciberseguridad (por ejemplo, EEUU, Israel, Rusia, Canadá, Reino Unido, Malasia, China y Francia).

· Definir los escenarios de intervención para cada tipología de profesionales de la ciberseguridad identificados, revisando los pasos clave en la carrera profesional de ciberseguridad en función de la demanda identificada.

· Identificar y consensuar, con los principales actores involucrados, recomendaciones a corto, medio y largo plazo para la creación y consolidación de equipos y profesionales de ciberseguridad cualificados ahora y en el futuro.

Además, en base a los resultados del informe de diagnóstico, el prestador de este servicio elaborará un plan de acción que justifique la adopción de un conjunto de acciones prácticas.

Los resultados de este servicio, junto con los obtenidos de otros informes similares o complementarios [44], recientemente contratados también por otras AAPP, serán cruciales para corroborar el diagnóstico y establecer los indicadores que midan las magnitudes involucradas, así como para formular recomendaciones accionables para la atracción, rendimiento y retención del talento en seguridad de la información.

3.5.2. Generación, atracción, rendimiento y retención del talento en ciberseguridad (GARRTC)

3.5.2.1. Propuesta de acciones estructurales

3.5.2.1.1. Sensibilización social y fomento de vocaciones tempranas

- **Los planes de concienciación social en ciberseguridad, además de alertar sobre las amenazas, incluirán mensajes nítidos relativos a las oportunidades de desarrollo profesional para los jóvenes, en la protección frente a dichas amenazas.**

- **Acciones de fomento vocacional en colegios y centros de enseñanza secundaria, mediante gamificación, concursos, actividades extraescolares, etc. Por ejemplo, competiciones del tipo CTF (Capture the flag) entre colegios, Red Team vs. Blue Teams, visitas a SOCs de empresas. Visibilidad en medios de comunicación social.**

- **Programa de becas y ayudas directas a alumnos destacados, así como financiación para la dotación de infraestructuras de laboratorio en colegios y centros de enseñanza secundaria. Visibilidad en medios de comunicación social.**

- **Incorporación de la materia Ciberseguridad dentro de los planes de formación académicos de enseñanza básica y media e, incluso, como una opción de especialización universitaria (la demanda de «ingeniero de ciberseguridad»).**

3.5.2.1.2. Plan integral

Las organizaciones públicas y privadas, especialmente aquellas de gran tamaño y con una fuerte componente en I+D+i, deben disponer de un Plan Integral GARRTC. Dicho Plan debe contemplar lo siguiente:

- **Definición del Valor de Marca que desea tener, o tiene, la organización (*Employer branding*).**
- **En función del Valor de Marca, establecer el conjunto de competencias deseadas y su priorización.**
- **En función del conjunto de competencias deseadas, definir los perfiles (habilidades) deseados en los trabajadores y su priorización.**
- **Elaboración de las matrices de rendimiento y potencial deseado en la organización, en cada competencia y para cada perfil, transmitiéndolo de forma clara a los empleados, en todos los niveles de la organización.**
- **Búsqueda del talento necesario para cada perfil definido, promoviendo políticas que permitan localizar el talento allí donde se encuentre, abiertos a encontrarlo incluso donde menos se pudiera pensar.**
- **Promover políticas que generen talento diverso, entendiendo la diversidad en el más amplio sentido de la palabra y sin fronteras de ningún tipo, buscando equipos multi-talento y multi-disciplinares de alto rendimiento.**
- **Elaborar planes de carrera profesional para el desarrollo del talento, tanto a nivel individual como colectivo.**
- **Fidelización del talento elaborando una Propuesta de Incentivos de la empresa hacia el empleado de forma individualizada en los máximos y colectiva a nivel de mínimos.**
- **Elaborar un plan de renovación de personal coherente y no disruptivo en función del cumplimiento o no de la matriz de rendimiento y potencial establecido.**
- **Confluencia de la Gestión del Talento (GT) con la gestión del conocimiento buscando como objetivo final la consecución de la Gestión del Talento Inteligente (*Smart talent management*).**

Disponer de una plantilla estable en el tiempo ayuda a las empresas a afrontar proyectos a largo plazo con mayores garantías de éxito. La retención de empleados puede suponer una ganancia de competitividad, productividad y seguridad, en comparación con las empresas que presentan altos niveles de rotación de personal. La Propuesta de Incentivos constará de componentes salariales y no salariales, que se detallan en el Anexo XII a título de ejemplo.

3.5.2.2. Propuesta de acciones inmediatas

Para apoyar la I+D+i en seguridad de la información en pymes, empresas, universidades y centros de investigación, mediante programas de compra pública innovadora:

- **Estudiar fórmulas para dar continuidad, más allá del fin del estado de alarma, a lo establecido en el Real Decreto-ley 34/2020, de 17 de noviembre, de medidas urgentes de apoyo a la solvencia empresarial y al sector energético y en materia tributaria.**

- **Apoyar el emprendimiento dentro de las empresas, estableciendo incentivos para que los trabajadores desarrollen sus ideas. Una posible opción, entre otras alternativas, puede ser a través de la participación del empleado en el capital de startups que desarrollen sus ideas, bien sea en incubadora de la propia empresa o externa a la misma.**

- **Ofrecer bolsas de trabajo en ciberseguridad en las empresas para que los egresados de la Universidad puedan incorporarse fácilmente a la empresa.**

Las siguientes propuestas persiguen incrementar las actividades nacionales para el desarrollo de productos, servicios y sistemas de ciberseguridad, y la seguridad desde el diseño, apoyando específicamente aquellas que sustenten necesidades de interés nacional para fortalecer la autonomía digital, y la propiedad intelectual e industrial:

- **Promover concursos abiertos de ideas para resolver desafíos no resueltos en empresas u organismos de la Administración pública, de interés nacional.**

- **Establecer canales alternativos a los departamentos de I+D de las empresas para evitar que dichos departamentos desestimen ideas de empleados que podrían desarrollarse exitosamente.**

- **Simplificar el proceso de petitorio de patentes, financiar el proceso y ofrecer una ventanilla de ayuda a los solicitantes durante todo el proceso. Es necesario estudiar el proceso actual, y habilitar una oficina específica para la gestión.**

Para promover las actividades de normalización y la exigencia de requisitos de ciberseguridad en los productos y servicios de Tecnologías de la Información y de las Comunicaciones.

+ **Facilitar la publicación de artículos científico-técnicos en publicaciones nacionales e internacionales. Es necesario estudiar el panorama internacional de las publicaciones científico técnicas y habilitar una oficina específica para la gestión.**

+ **Ayudas directas para sufragar costes por dedicación y gastos por asistencia a foros profesionales de estandarización en representación institucional de la empresa, del organismo público correspondiente o de España.**

3.5.2.3. Ideas clave a fin de poder iniciar el proceso de implantación de la Gestión del Talento en la Función Pública y por extensión en las FAS

Adopción por las empresas de las siguientes claves prácticas:

/// Clave 1. La organización tiene que permitir que el talento aflore, incluso debe regarlo y después cuidarlo.

/// Clave 2. Crear nuestro propio camino hacia la Gestión del Talento basándonos en nuestros propios valores, experiencias y recursos.

/// Clave 3. Para atraer el talento lo primero que necesitamos es saber qué es lo que queremos.

/// Clave 4. Salir a buscar el talento allá donde esté, pero no nos olvidemos de buscar primero en casa.

/// Clave 5. Establecer procesos de atracción de candidatos, de selección e inserción en la organización.

/// Clave 6. Empleo de métricas que analicen la relación rendimiento/potencial de nuestro personal con el que establecer programas de formación específicos asociados.

/// Clave 7. Creación de un departamento encargado tanto del Aula Virtual como de la página web así como del desarrollo y distribución de productos en formatos web, audiovisuales y texto impreso.

/// Clave 8. Conocer la opinión de nuestro personal.

/// Clave 9. Trabajar orientado a proyectos con pequeños equipos altamente especializados y muy motivados.

/// Clave 10. El liderazgo de los equipos de alto rendimiento.

/// Clave 11. Medir para mejorar.

/// Clave 12. Dar un giro al concepto del horario, buscamos eficiencia no permanencia en el puesto de trabajo.

/// Clave 13. Fomentar la motivación, el compromiso y el *engagement* de nuestro personal.

/// Clave 14. Establecer la Propuesta de Valor del Empleado (PVE) de nuestra organización/departamento.

/// Clave 15. Establecer nuestra propia Responsabilidad Social Corporativa (RSC).

/// Clave 16. Elaborar el Plan de Mejora Digital de nuestra organización/departamento.

Las FAS y por extensión las AAPP son organizaciones fuertemente estructuradas y jerarquizadas, cuyos procedimientos, tanto operativos como de gestión de personal, funcionan adecuadamente para la generalidad de sus unidades y organismos, aunque resulta mucho más costoso para ellas girar su modus operandi hacia la Gestión de Talento, que en el entorno privado.

Dentro de la AAPP, las organizaciones cuya actividad se centra específicamente en el empleo de las TIC para el desarrollo de sus actividades, como por ejemplo el caso del MCCE que las emplea para la realización de operaciones militares en el ciberespacio, las convierte de pleno en organizaciones donde la Gestión del Talento puede ofrecer sus mejores resultados.

Este tipo de organizaciones pueden ser pequeñas islas dentro de la Administración a la que pertenecen a fin de no morir antes siquiera de empezar el proceso del giro a la Gestión del Talento que pudiera darse el caso de no ser de interés para la totalidad de su organización.

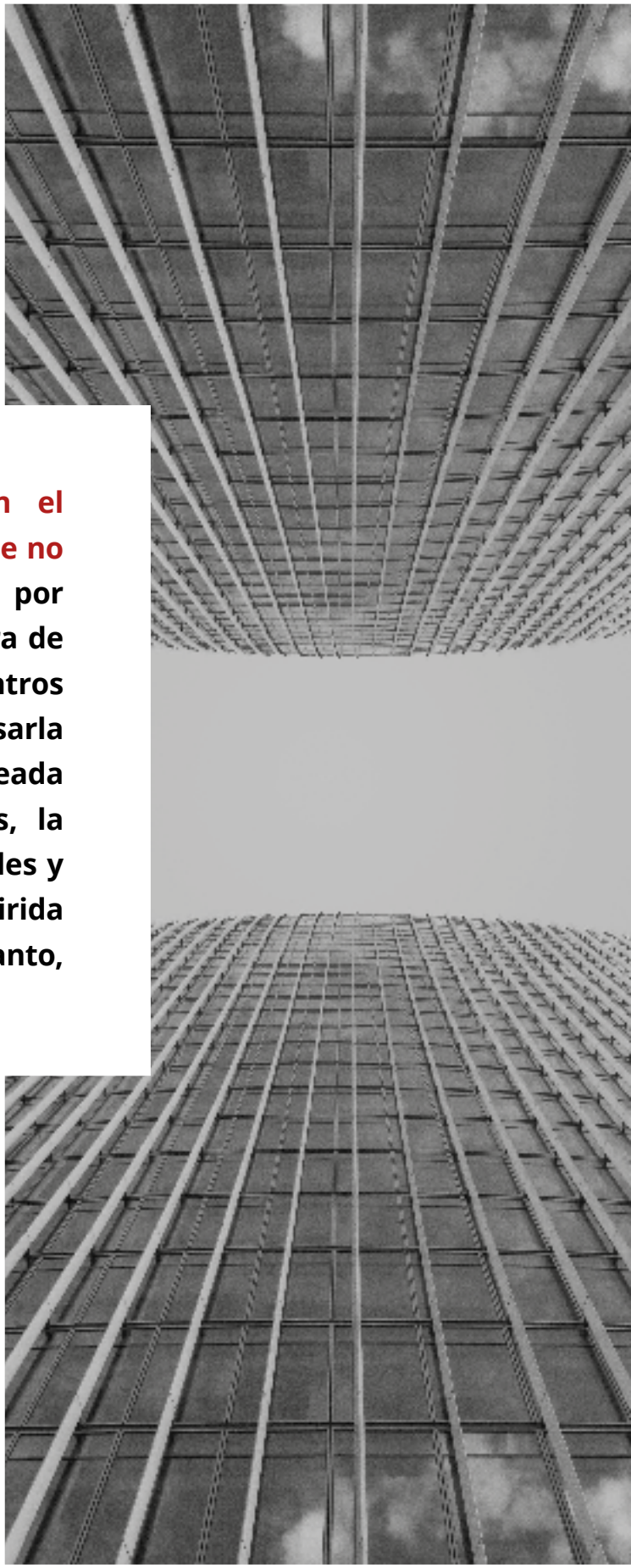
Buscando un acercamiento eminentemente práctico y realista [78], se plantean un conjunto de 16 claves, independientes unas de otras, que pueden ser evaluadas y en su caso aplicadas por las empresas de forma parcial, adaptándose a las peculiaridades de cada empresa en un modelo de adopción conservador e incremental.

Acciones transversales

+ 3.6

Este apartado recoge las acciones transversales que condicionan de manera esencial el éxito de las propuestas relacionadas con el impulso de las oportunidades en I+D+i de ciberseguridad.

Se refieren a ámbitos de diversa naturaleza como fomentar el consumo de tecnología nacional, financiación de proyectos de I+D+i, paliar el déficit de talento investigador y emprendedor, y dinamizar la inversión en empresas de base tecnológica.



La empresa privada no invierte en el desarrollo de tecnología nacional porque no encuentra incentivos para realizarlo y, por tanto, no usa la capacidad investigadora de nuestras universidades y nuestros centros tecnológicos, que es muy alta. Al no usarla está, en muchas ocasiones, desalineada con las necesidades de las empresas, la tecnología desarrollada por universidades y centros tecnológicos. Acaba siendo adquirida por empresas extranjeras y, por tanto, enriqueciendo a otros países.

Las acciones transversales propuestas van orientadas a los siguientes objetivos:

· fomento del consumo de tecnología nacional,

· financiación de proyectos I+D+i,

· paliación del déficit de talento investigador y emprendedor, e

· inversión en empresas de base tecnológica.

Los siguientes epígrafes detallan las propuestas concretas.

3.6.1. Fomento del consumo de tecnología nacional

· Diseñar y activar programas de ayuda específicos, basados en los requisitos de la regulación europea, destinados a sectores de demanda que se consideren esenciales para la economía española.

· Identificar ámbito público competente para poder valorar las propuestas que salgan de las siguientes fases.

· Se identificarán para su valoración y extensión acciones modelo como el "Programa de Ayudas a la Ciberseguridad Industrial" del Gobierno Vasco.

· Diseñar y activar modelos para flexibilizar las condiciones y tratar de mejorar la situación actual en cuanto a la exigencia de avales.

· En España existen iniciativas de *start-ups*, EBTs, micropymes y pymes que están desarrollando tecnología propia en el ámbito de la ciberseguridad.

· El desarrollo de nuevas soluciones en este campo para empresas de este tipo requiere de proyectos de inversión (capital) o de apoyo institucional a través de subvenciones o financiación con instrumentos públicos que les permitan desarrollar la tecnología y crecer sin tener que acudir a los mercados de capital en los momentos iniciales de la creación o el desarrollo de la empresa.

· Es necesario revisar los instrumentos públicos de apoyo a este tipo de proyectos de desarrollo de tecnologías nacionales para que resulten ágiles y ventajosos para sus promotores, aun a costa de asumir un mayor nivel de riesgo. Disponer de empresas capaces de desarrollar una tecnología nacional competitiva dependerá de nuestra capacidad como país para diseñar y aplicar estos instrumentos.

· Diseñar y activar modelos que faciliten la adopción temprana de soluciones nacionales de ciberseguridad por las administraciones públicas y las infraestructuras críticas.

· Identificar las situaciones en las que es necesario el uso de tecnología española o europea para la prestación de determinados servicios y analizar la forma de usar mecanismos de compra basados en criterios de "Seguridad Nacional".

· Fomentar la confianza en el uso de tecnología europea (nacional) diseñando herramientas de garantía en las que el Estado pueda actuar como "garante" o como actor de confianza.

3.6.2. Financiación de proyectos I+D+i

· Evolucionar los programas nacionales de financiación de la I+D+i.

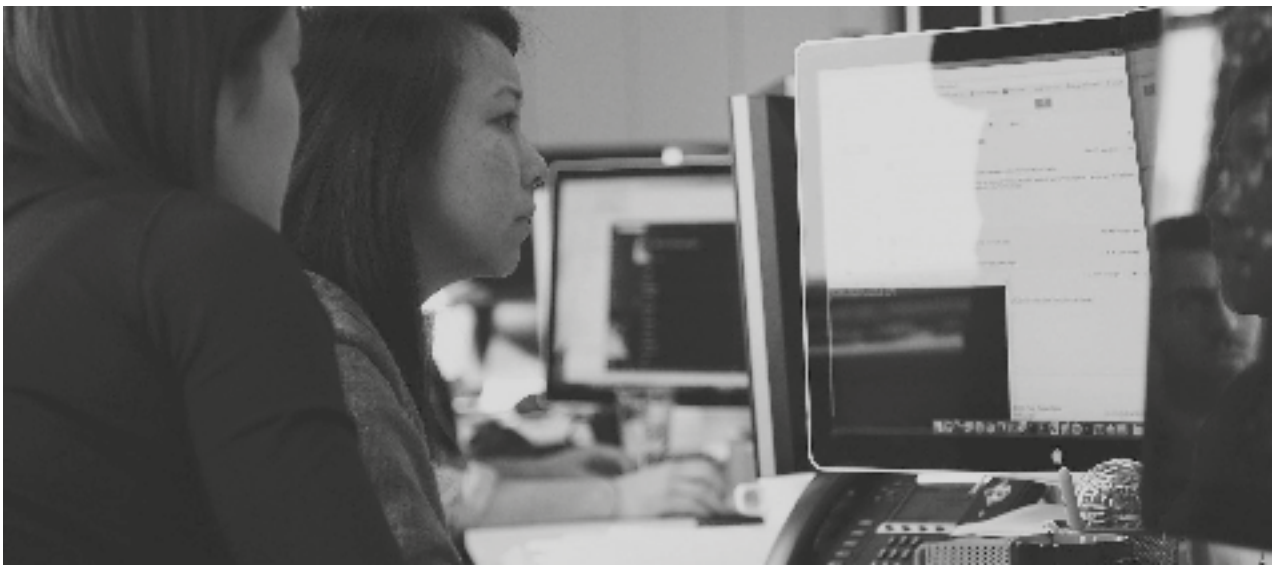
· Identificar ámbito público competente para poder evolucionar los programas para universidades y CCTT, convertirlos en instrumentos de carácter competitivo, basarlos en la excelencia y dotarlos de cuadros de mando compuestos por indicadores dirigidos a aquellas prioridades relacionadas con la Estrategia Nacional.

· Crear mecanismos de permanencia de las acciones estratégicas de I+D+i para que no queden vinculados a ciclos de legislatura.

· Identificar ámbito público competente para poder definir el modelo y garantizarlo.

· Incluir la ciberseguridad en otros programas de financiación de I+D+i.

· Identificar ámbito público competente para poder incluir la ciberseguridad en los programas de palancas tecnológicas como 5G, inteligencia artificial, computación cuántica, IoT, etc.



3.6.3. Paliación del déficit de talento investigador y emprendedor de tecnología nacional

· Crear incentivos para el personal investigador que desarrolle otras funciones (ejemplo, el profesorado universitario).

· Identificar ámbito público competente para poder valorar las propuestas que salgan de las siguientes fases, incluyendo aspectos como la retribución económica o la reducción de la carga docente.

· Actuar sobre el sistema educativo desde edades tempranas y con perspectiva de género.

· Identificar ámbito público competente para poder valorar las propuestas que salgan de las siguientes fases, incluyendo:

· Evolucionar los programas curriculares incorporando competencias de ciberseguridad en grados TIC (materias sobre tecnología) pero también en todos los relacionados con sectores digitalizados (materias sobre buenas prácticas).

· Visibilizar la I+D+i y la ciberseguridad como una opción profesional, con especial atención al alumnado femenino.

· Evolucionar los programas orientados a la contratación laboral de personas doctoradas.

· Identificar ámbito público competente para poder valorar las propuestas que salgan de las siguientes fases, incluyendo:

· Evoluciones a los doctorados industriales para que incluyan retos y contenidos de ciberseguridad.

· Evoluciones a los programas que actualmente sirven para la transferencia de doctores hacia las empresas y a los centros tecnológicos (por ejemplo, Torres Quevedo o similares).

· Potenciar el desarrollo del pensamiento computacional en la sociedad

· Identificar ámbito público competente para poder valorar las propuestas que salgan de las siguientes fases.

· Se identificarán para su valoración y extensión acciones modelo como, por ejemplo, “TXAC Planet" y “TXACkathon”, una serie infantil de TV, que acerca la lógica del pensamiento computacional y la alfabetización en tecnología informática a niñas y niños. Promovida por EITB, Canal Sur, el clúster vasco de empresas tecnológicas GAIA y las empresas Azaroa Films y DIGITOMICA.

3.6.4. Inversión en empresas de base tecnológica

· Diseñar y activar programas de fomento a la innovación empresarial.

· Desarrollar acciones de promoción de la tecnología desarrollada por empresas nacionales.

· Fomento del uso por parte de la administración pública de la CPI (Compra Pública Innovadora). Mediante el uso de este instrumento se pueden lanzar pruebas de concepto y retos industriales que activen la capacidad de desarrollo de soluciones de las empresas del sector.

· Establecer programas de apoyo a la innovación con condiciones flexibles y ágiles acordes con el tipo de tejido empresarial nacional formado principalmente por PYMES.

· Diseñar y activar mecanismos para generar y escalar EBTs y *start-ups* "*born-digital*" y "*Big Bang disruptor*".

· Fomentar el espíritu emprendedor en las universidades y CCTT españoles.

· Diseñar programas en los que se exponga los retos a los que se enfrenta la sociedad en materia de ciberseguridad y el tipo de problemas que es necesario resolver a corto y medio plazo.

· Activar programas públicos de financiación de empresas de producto en su fase inicial: capital semilla.

· Diseñar y activar modelos que valoren adecuadamente los activos intangibles (propiedad intelectual).

· La economía digital se caracteriza por la aparición de compañías de producto con una inversión masiva en activos intangibles. La valoración que se hace habitualmente de los activos intangibles no es proporcional a la valoración que se hace de los activos tangibles, por lo que resulta complicado defender el valor de aquellas compañías españolas que han decidido el camino de la inversión en el desarrollo de tecnología propia.

· A diferencia de lo que sucede en España y en Europa, en EEUU los instrumentos financieros valoran muy positivamente los activos intangibles por lo que resulta más sencillo valorar las compañías que invierten en este tipo de activos.

· Se propone, en el mercado de la ciberseguridad, analizar los activos intangibles de las compañías españolas e identificar instrumentos que permitan valorar de forma adecuada este tipo de activos.

· Diseñar y activar modelos de incubación y aceleración de ideas/propuestas, potenciando los ya existentes y fomentando la creación de nuevos.

· Identificar el ámbito público competente para poner en marcha un servicio de las siguientes características:

· Validación de oportunidades de negocio con alta probabilidad de éxito apoyada en la figura de *Venture Builder* que pueda convertir las ideas en empresas.

· Esquema de escalado/aceleración de ideas mediante la priorización de aquellas con potencial crecimiento exponencial.

· Autosostenibilidad mediante la participación de redes de inversores, emprendedores en serie y empresas tractoras.

· Programas de incubación / aceleración o espacios físicos de emprendimiento de referencia que actúen como palancas de visibilidad y con ello, de atracción de ideas, talento e inversión.

· Favorecer el crecimiento de las empresas de base tecnológica de alto valor.

· Aunque no es un problema específico de las empresas de ciberseguridad, sin duda les afecta también.

· Para competir en un mercado global como el actual, las empresas de ciberseguridad españolas necesitan ganar tamaño y para ganar tamaño se debe fomentar la fusión de empresas, crear herramientas para favorecer el crecimiento inorgánico de algunas de ellas o fomentar las colaboraciones en aventuras tipo *Joint Venture*.

· Se propone:

· Realizar un estudio comparativo del tamaño de las empresas de ciberseguridad españolas en un contexto internacional analizando su productividad como un factor de competitividad.

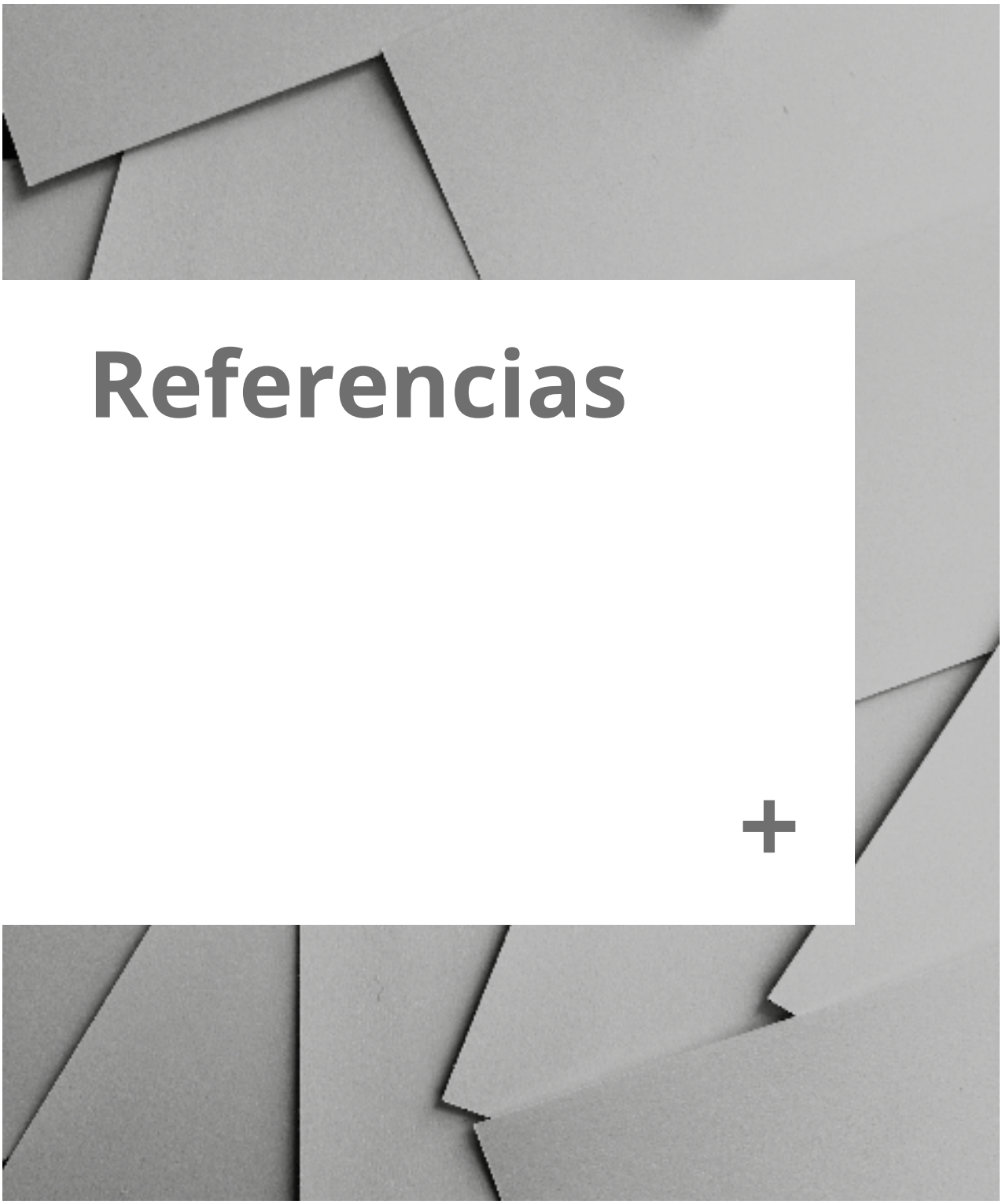
· Diseñar programas formativos para los emprendedores y equipos directivos orientados a exponer la importancia del tamaño de las empresas y las posibilidades de crecimiento.

· Desarrollar herramientas públicas que fomenten el crecimiento de las empresas españolas dentro y fuera de nuestras fronteras.

· Desarrollar la regulación específica para la protección de empresas estratégicas de Ciberseguridad Nacional:

· Identificar ámbito público competente para poder profundizar en la reforma iniciada por el Real Decreto-ley 34/2020, de 17 de noviembre, de medidas urgentes de apoyo a la solvencia empresarial y al sector energético, y en materia tributaria que en su Disposición final cuarta deja suspendido el régimen de liberalización de las inversiones extranjeras directas en España, que se realicen en los sectores que se citan a continuación y que afectan al orden público, la seguridad pública y a la salud pública, incluyendo:

· «b)Tecnologías críticas y de doble uso, tecnologías clave para el liderazgo y la capacitación industrial, y tecnologías desarrolladas al amparo de programas y proyectos de particular interés para España, incluidas las telecomunicaciones, la inteligencia artificial, la robótica, los semiconductores, la ciberseguridad, las tecnologías aeroespaciales, de defensa, de almacenamiento de energía, cuántica y nuclear, las nanotecnologías, las biotecnologías, los materiales avanzados y los sistemas de fabricación avanzados.»



Referencias

Referencias

/// 1 (ISC)2. (2020). Cybersecurity Workforce Study. Recuperado de https://www.isc2.org/Research/Workforce-Study

/// 2 Agence Nationale de la sécurité des systèmes d'information. Campus Cyber. Un campus dédié à la cybersécurité. Recuperado de: https://www.ssi.gouv.fr/agence/cybersecurite/un-campus-dedie-a-la-cybersecurite/

/// 3 Agence Nationale de la sécurité des systèmes d'information. Cybersécurité: faire face à la menace. La stratégie française. Recuperado de: https://www.ssi.gouv.fr/actualite/cybersecurite-faire-face-a-la-menace-la-strategie-francaise/

/// 4 Asociación Española para la Digitalización. (2019). El desafío de las vocaciones STEM. Recuperado de: https://www.digitales.es/wp-content/uploads/2019/09/Informe-EL-DESAFIO-DE-LAS-VOCACIONES-STEM-DIGITAL-AF-1.pdf

/// 5 Belfer Center, Harvard Kennedy School (2020). National Cyber Power Index – NCPI. Recuperado de: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

/// 6 Cabinet Office (2020). National Cyber Security Strategy 2016 – 2021. Progress Report. Recuperado de: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/937702/6.6788_CO_National-Cyber-Security-Strategy-2016-2021_WEB3.pdf

/// 7 Carnevalli, J., Paulo Cauchick Miguel (2008). Review, analysis and classification of the literature on QFD—Types of research, difficulties and benefits. International Journal of Production Economics, Volume 114, Issue 2, DOI. Recuperado de: https://doi.org/10.1016/j.ijpe.2008.03.006

/// 8 CCN-CERT. Herramienta INES para Informe Estado de la Seguridad del ENS. Recuperado de: https://www.ccn-cert.cni.es/soluciones-seguridad/ines.html

/// 9 CEN/TC 428. (2019). EN 16234-1. e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all sectors - Part 1: Framework.

/// 10 Cybasque. Libro blanco de la Ciberseguridad. Recuperado de: https://www.basquecybersecurity.eus/es/actualidad-bcsc/segunda-edicion-libro-blanco-ciberseguridad-euskadi.html

/// 11 Código de Derecho de la Ciberseguridad (2020). Recuperado de: https://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho__de_la_Ciberseguridad

/// 12 Cyber Security Competence for Research and Innovation (CONCORDIA). https://www.concordia-h2020.eu/

/// 13 Cyber Security for Europe (CyberSec4Europe). https://cybersec4europe.eu/

/// 14 Delgado, V. (2019). Quiero dedicarme a la ciberseguridad ¿Y ahora qué? Recuperado de: https://cybercamp.es/sites/default/files/contenidos/videos/adjuntos/cybercamp19_vd_quiero_dedicarme_ciberseguridad.pdf

/// 15 Department of Homeland Security. Small Business Innovation Research Program. Recuperado de: https://www.dhs.gov/science-and-technology/sbir

/// 16 Directiva 2016/1148 del Parlamento y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Recuperada de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148

/// **17** Economist. Cyber Power Index CPI. Recuperado de: https://www.economist.com/science-and-technology/2020/09/17/a-new-global-ranking-of-cyber-power-throws-up-some-surprises

/// **18** ENISA. (2019). Cybersecurity Skills Development in the EU. DOI: 10.2824/525144

/// **19** ENISA. (2020). Ad-Hoc Working Group on the European Cybersecurity Skills Framework. Recuperado de: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

/// **20** ENISA (2020). National Capabilities Assessment Framework – NCAF. Pp. 16 y 78. Recuperado de: https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

/// **21** ENISA. CSIRTs inventory map. Recuperado de: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

/// **22** European Commission. Contractual public-private partnerships. Recuperado de: https://ec.europa.eu/programmes/horizon2020/en/contractual-public-private-partnerships

/// **23** European Commission. EU-funded projects on Digital security. Recuperado de: https://ec.europa.eu/digital-single-market/en/programme-and-projects/eu-funded-projects-digital-security

/// **24** European Commission. EU Digital Society. Recuperado de: https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi

/// **25** European Commission, Directorate-General of Communications Networks, Content & Technology (2019). Cybersecurity Industry Market Analysis (CIMA). Recuperado de: https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Cibersecurity_Market_Analysis_CIMA_2019.pdf

/// **26** European Commission. EU Atlas. Recuperado de: https://cybersecurity-atlas.ec.europa.eu/centres-in-europe

/// **27** European Commission. EU Regional Innovation Scoreboard - RIS (2019). Recuperado de: https://ec.europa.eu/growth/industry/policy/innovation/regional_en

/// **28** European Commission. European Innovation Scoreboard – EIS (2020). Recuperado de: https://ec.europa.eu/growth/industry/policy/innovation/scoreboards_en

/// **29** European Commission (2017). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. 450 final.

/// **30** European Commission. Four EU pilot projects launched to prepare the European Cybersecurity Competence Network. Recuperado de: https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

/// **31** European Council (2020). Propuesta 13856/20. Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Recuperado de: https://www.consilium.europa.eu/media/47665/st13856-en20.pdf

/// **32** European Cyber Security Organization (2020). Input to the Horizon Europe Programme 2021-2027 Priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity. Recuperado de: https://ecs-org.eu/documents/publications/5fdc4c5deb6f9.pdf

/// 33 European Cyber Security Organization (2020). Nota de prensa. ECSO initiates dialogue with the European Commission for the creation of a €1 billion cybersecurity investment platform. Recuperado de: https://ecs-org.eu/newsroom/ecso-initiates-dialogue-with-the-european-commission-for-the-creation-of-a-1-billion-cybersecurity-investment-platform

/// 34 European Cyber Security Organization. European Market Radar Taxonomy. Recuperado de: http://www.ecs-org.eu/initiatives/cybersecurity-market-radar y https://www.ecs-org.eu/documents/uploads/ecso-cybersecurity-market-radar-taxonomy-table.pdf

/// 35 European Cyber Security Organization. Colaboración Público Privada (cPPP). Recuperado de: https://ecs-org.eu/cppp

/// 36 European Investment Fund. InnovFin Equity. Recuperado de: https://www.eif.org/what_we_do/equity/single_eu_equity_instrument/innovfin-equity/index.htm

/// 37 European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO Network). https://echonetwork.eu/

/// 38 European Union. InvestEU. Recuperado de: https://europa.eu/investeu/home_en

/// 39 Global Cyber Security Capacity Center. Cybersecurity Capacity Review of the United Kingdom. Recuperado de: https://gcscc.ox.ac.uk/files/cybersecuritycapacityreviewoftheunitedkingdompdf

/// 40 Global Enterpreneuship Monitor – GEM, pp. 30-32. Recuperado de: https://www.gem-spain.com/wp-content/uploads/2020/06/Informe-GEM-Espa%C3%B1a-2019_20.pdf

/// 41 Gobierno de España. Plan de Digitalización de pymes 2021-2025. Recuperado de: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/270121-PlanDigitalizacionPYME01Optimizado.pdf

/// 42 Gobierno Vasco. Sistema integral de monitorización del Plan de Ciencia, Tecnología e Innovación Euskadi 2020. Recuperado de: https://www.euskadi.eus/informacion/monitorizacion-y-evaluacion-del-pcti-euskadi-2020/web01-a2lehpct/es/

/// 43 GRC Technical Reports. European Cybersecurity Centre of Expertise – Cybersecurity Competence Survey. ISBN 978-92-79-92954-0. 2018

/// 44 HAYS Executive. (2020). Análisis de talento en el sector ciberseguridad. Recuperado de: https://www.madridforoempresarial.es/wp-content/uploads/2020/11/194-Ana%CC%81lisisTalentoCiberseguridadMayo-Julio2020.pdf

/// 45 INCIBE (2016). Catálogo de empresas y soluciones de Ciberseguridad. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/catalogo_ciberseguridad.pdf

/// 46 INCIBE (2016). Tendencias en el mundo de la ciberseguridad, p. 34. Recuperado de: https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf

/// 47 INCIBE (4 Diciembre 2020). Exp. 030/20 Servicios de análisis y diagnóstico de Talento en ciberseguridad de España. Publicado en: https://contrataciondelestado.es/wps/wcm/connect/1d08b511-6854-4230-9bba-e1e068814d59/DOC_CAN_ADJ2020-430201.html?MOD=AJPERES

/// **48** INCIBE (2020). Balance de Ciberseguridad de INCIBE 2020. Recuperado de: https://www.incibe.es/que-es-incibe/que-hacemos#balances

/// **49** INCIBE. Catálogo de Ciberseguridad. Recuperado de: https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

/// **50** INCIBE (2021). Taxonomía de Ciberseguridad. Nota informativa. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/taxonomia_ciberseguridad.pdf

/// **51** INCIBE (2021). Catálogo de másteres en Ciberseguridad en España. Recuperado de: https://www.incibe.es/catalogos-formacion-ciberseguridad

/// **52** International Network for Natural Sciences (2009-2021). Types of scientific research. Recuperado de: https://innspub.net/types-of-scientific-research/. Último acceso: marzo de 2021

/// **53** International Telecommunications Union (ITU) (2018). Global Cybersecurity index (GCI). Recuperado de: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

/// **54** Joint Research Centre (2019). A proposal for a European Cybersecurity Taxonomy. Recuperado de: https://ec.europa.eu/jrc/en/publication/proposal-european-cybersecurity-taxonomy

/// **55** LOGITEC. Evaluación de la ciberseguridad entornos IT&OT. Recuperado de: https://www.ciberseguridadlogitek.com/wp-content/uploads/Evaluacion-ciberseguridad-de-entornos-industriales.pdf

/// **56** Lluch, A. (14 Febrero 2020). Addressing the Shortage of Cybersecurity Skills in Europe. Recuperado de: https://cybersec4europe.eu/addressing-the-shortage-of-cybersecurity-skills-in-europe/

/// **57** Ministère des Armées (2019). La DGA inaugure Aliénor, cluster d'innovation technique de défense dans le domaine aérospatial. Recuperado de: https://www.defense.gouv.fr/actualites/articles/la-dga-inaugure-alienor-cluster-d-innovation-technique-de-defense-dans-le-domaine-aerospatial

/// **58** Ministerio de Asuntos Económicos y Transformación Digital (2020). España Digital 2025. Recuperado de: https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx

/// **59** Ministerio de Asuntos Económicos y Transformación Digital. Red.es. Programa Acelera pyme. Recuperado de: https://acelerapyme.gob.es/programa-acelera-pyme#sobre-acelera-pyme

/// **60** Ministerio de Asuntos económicos y Transformación digital. Instituto de Crédito Oficial (2020). Nota de prensa: El ICO lanza la mayor convocatoria de Fond-ICO Global y anuncia la próxima ampliación del fondo. Recuperado de: https://www.ico.es/web/ico/notas-de-prensa/-/blogs/el-ico-lanza-la-mayor-convocatoria-de-fond-ico-global-y-anuncia-la-proxima-ampliacion-del-fondo

/// **61** Ministerio de Ciencia e Innovación (2020). Estrategia Española de Ciencia, Tecnología e Innovación 2021-2027. Recuperado de: https://www.ciencia.gob.es/stfls/MICINN/Ministerio/FICHEROS/EECTI-2021-2027.pdf

/// **62** Ministerio de Ciencia e Innovación (2021). Pacto por la Ciencia y la Innovación. Recuperado de: https://www.ciencia.gob.es/portal/site/MICINN/menuitem.edc7f2029a2be27d7010721001432ea0/?vgnextoid=d18d6fba75427710VgnVCM1000001d04140aRCRD

/// 63 Ministerio de Ciencia e Innovación (2017). Plan Estatal de Investigación Científica, Técnica y de Innovación 2017-2020. Recuperado de: https://www.ciencia.gob.es/portal/site/MICINN/menuitem.7eeac5cd345b4f34f09dfd1001432ea0/?vgnextoid=83b192b9036c2210VgnVCM1000001d04140aRCRD

/// 64 Ministerio de Ciencia e Innovación. Centro para el Desarrollo Tecnológico Industrial. Ayudas a la I+D+i. Recuperado de: http://www.cdti.es/index.asp?MP=100&MS=898&MN=1&r=1366*768

/// 65 Ministerio de Economía y Competitividad. (2016). Estrategia española de ciencia y tecnología y de innovación. Recuperado de: https://www.ciencia.gob.es/stfls/MICINN/Investigacion/FICHEROS/Estrategia_espanola_ciencia_tecnologia_Innovacion.pdf

/// 66 Ministerio de Educación y Formación Profesional. (2020). Nota de prensa. Recuperado de: http://www.educacionyfp.gob.es/prensa/actualidad/2020/04/20200407-titulosfp.html

/// 67 Ministerio de Industria, Comercio y Turismo (2019). Directrices generales de la nueva política industrial española. Recuperado de: https://www.mincotur.gob.es/es-es/gabineteprensa/notasprensa/2019/documents/docu%20directrices%20generales%20de%20la%20pol%C3%ADtica%20industrial%20espa%C3%B1ola.pdf

/// 68 Ministerio de Industria, Comercio y Turismo. Servicio Financia Industria. Recuperado de: https://plataformapyme.es/es-es/Financiacion/Paginas/ApoyoFinanInd.aspx

/// 69 Ministerio de Industria, Comercio y Turismo. Secretaría de Estado de Comercio. Datos del Comercio Exterior. Economía (dataComex), empresas (dataEmpresas) y UE (dataUE). Recuperado de: https://datacomex.comercio.es/

/// 70 Ministerio de Industria, Comercio y Turismo. Dirección general de Industria y de la pequeña y mediana empresa (2021). Cifras PYME. Datos marzo 2021. Recuperado de: https://industria.gob.es/es-es/estadisticas/Cifras_PYME/CifrasPYME-marzo2021.pdf

/// 71 Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática. (28 de enero de 2021). Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. BOE-A-2021-1192

/// 72 Ministerio del Interior. Personal de Seguridad Privada. Normativa básica reguladora. Recuperado de: http://www.interior.gob.es/web/servicios-al-ciudadano/personal-de-seguridad-privada/normativa-basica-reguladora

/// 73 National Audit Office (2019). Progress of the 2016–2021 National Cyber Security Programme. Recuperado de: https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme-Summary.pdf

/// 74 NIST SP 800-181 Rev. 1. (Noviembre 2020). Workforce Framework for Cybersecurity (NICE Framework). https://doi.org/10.6028/NIST.SP.800-181r1

/// 75 NIST Cyber Security Framework. Recuperado de: https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

/// **76** Observatorio Nacional de las Telcomunicaciones y Sociedad de la Información (2020). Informe del sector TIC 2020. Recuperado de: https://www.ontsi.red.es/es/estudios-e-informes/informe-anual-del-sector-tic-2020

/// **77** Oxford University. Global Cyber Security Capacity Centre. Cybersecurity Maturity Model for Nations (CMM). Recuperado de: https://gcscc.ox.ac.uk/files/cmmrevisededition090220171pdf

/// **78** Peñas, J. La Gestión del Talento TIC en el marco de las FAS. Una posible aplicación a la Ciber-Reserva (2018). TFM del Máster en Gestión y Dirección de Sistemas y Tecnologías de la Información y las Comunicaciones y de Seguridad de la Información de la Universidad de Vigo.

/// **79** Piesarskas, E. (31 Enero 2020). SPARTA D9.1 Cybersecurity skills framework. Recuperado de: https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf

/// **80** Presidencia del Gobierno. Departamento de Seguridad Nacional (2019). Estrategia Nacional de Ciberseguridad (2019). Recuperado de: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

/// **81** Raffino, M (2020). Tipos de Investigación. Recuperado de: https://concepto.de/tipos-de-investigacion/. Último acceso: marzo 2021

/// **82** Real Instituto Elcano (2021). Las cifras para España del Plan de Recuperación Europeo. Recuperado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari25-2021-feas-steinberg-cifras-para-espana-del-plan-de-recuperacion-europeo#:~:text=Para%20Espa%C3%B1a%2C%20la%20cifra%20rondar%C3%A1,explican%20en%20detalle%20estas%20cifras.

/// **83** Red Vasca de Ciencia y Tecnología e Innovación (RVCTI). Recuperado de: http://laadministracionaldia.inap.es/noticia.asp?id=1207752

/// **84** RENIC. Mapa de la I+D+i. Recuperado de: https://www.renic.es/es/mapa-idi-en-ciberseguridad

/// **85** RENIC. Miembros de la Red. Recuperado de: https://www.renic.es/es/miembros-y-colaboradores

/// **86** Revista Observatorio RH. (7 Septiembre 2020). Decae el temor de las empresas a una «fuga de talentos» por primera vez en seis años. Recuperado de: https://www.observatoriorh.com/orh-posts/decae-el-temor-de-las-empresas-a-una-fuga-de-talentos-por-primera-vez-en-seis-anos.html

/// **87** Seed Enterprise Investment Scheme. Recuperado de: https://www.seis.co.uk/

/// **88** SPARTA. https://sparta.eu/

/// **89** UK Cybersecurity Sectorial Analysis – UKCSA (2020) https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020

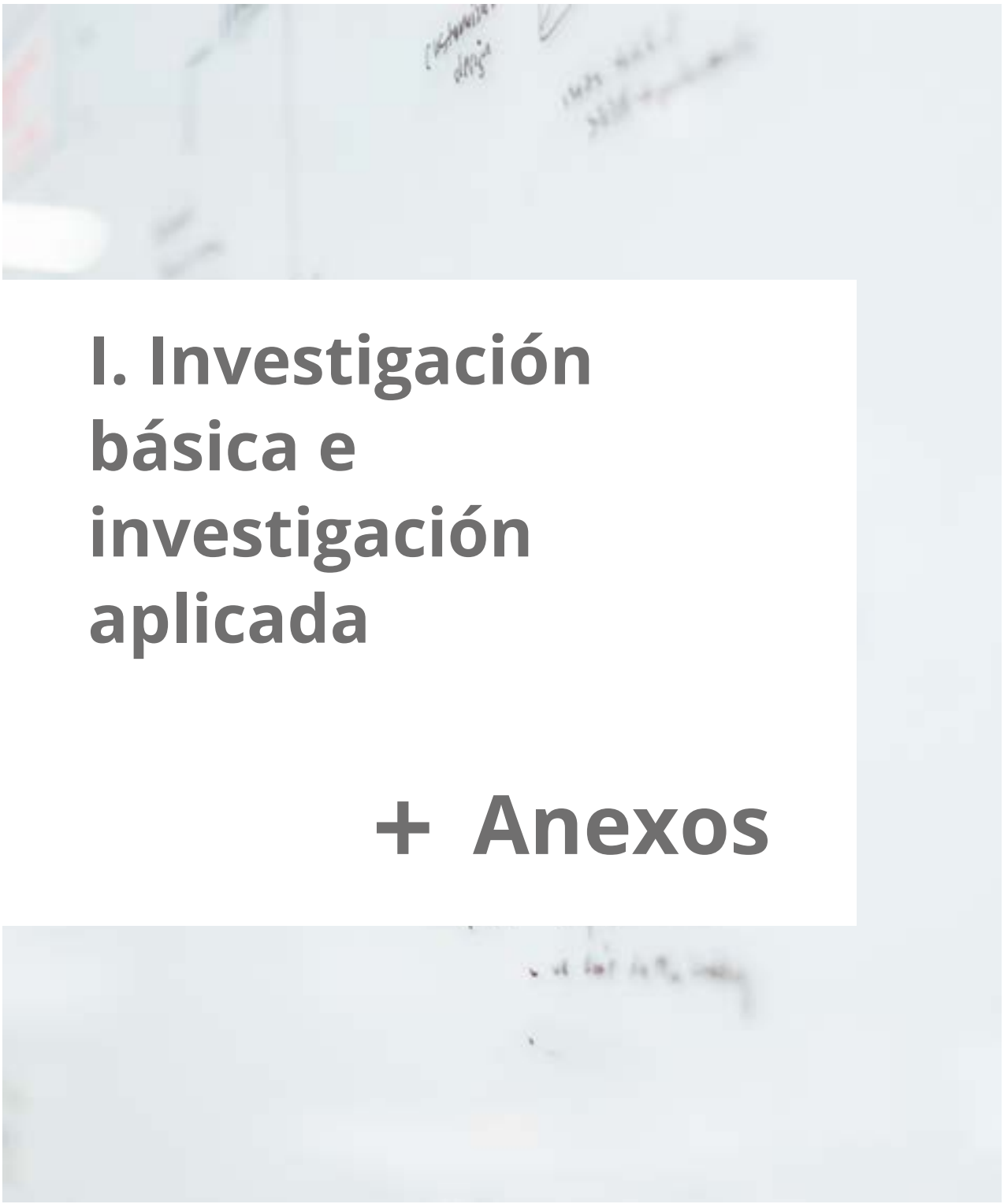
Acrónimos

Acrónimos

/// **(ISC)2**	Consorcio Internacional para la Certificación de la Seguridad de los Sistemas de Información
/// **AAPP**	Administraciones públicas
/// **B5G**	Beyond 5G
/// **BEI**	Banco Europeo de Inversión
/// **BCSC**	Basque Cybersecurity center
/// **BOE**	Boletín oficial del estado
/// **BTID**	Baste Tecnológica e Industrial de la Defensa
/// **CAPTECHS**	Capability Technology groups
/// **CARD**	Coordinación de Planeamientos
/// **CCAA**	Comunidades autónomas
/// **CCN**	Centro Criptológico Nacional
/// **CDTI**	Centro para el Desarrollo Tecnológico Industrial
/// **CEC**	Centro Europeo de Coordinación en ciberseguridad
/// **CEN/CT**	Comité europeo de estandarización/Comité técnico
/// **CERSA**	Compañía Española de Refinanciamiento
/// **CIMA**	EU Cybersecurity Industry Market Analysis
/// **CIRCE**	Centro de Información y Red de Creación de Empresas
/// **CMM**	Cybersecurity Capacity Maturity Model for Nations
/// **CNC**	Centro Nacional de Coordinación en ciberseguridad
/// **CNPIC**	Centro Nacional de Protección de Infraestructuras Críticas
/// **CPP**	Colaboración público-privada
/// **cPPP**	Public and Private Partnership Cooperation
/// **CSF**	Marco de perfiles profesionales de ciberseguridad
/// **CSIRT**	Computer Emergency Response Team
/// **CTF**	Capturar la bandera
/// **DESI**	Digital Economy and Society Index
/// **DGPYME**	Dirección General de Política de la PYME
/// **DHS**	Departamento de Seguridad Nacional de Estados Unidos
/// **EBT**	Empresa de Base Tecnológica
/// **e-CF**	Marco de competencias digitales
/// **ECSO**	European Cyber Security Organization

/// **EECTI**	Estrategia Española de Ciencia y Tecnología
/// **EI2C**	Ecosistema de Industria e Investigación en Ciberseguridad
/// **EIS**	European Innovation Scoreboard
/// **ENCS**	Estrategia Nacional de Ciberseguridad
/// **ENISA**	Agencia europea para la seguridad de la información y de las redes
/// **ENISA**	Empresa Nacional de Innovación, S.A.
/// **ESO**	Enseñanza Secundaria Obligatoria
/// **EDA**	Unión Europea de Defensa
/// **EDIH**	Centros Europeos de Innovación Digital
/// **FAS**	Fuerzas Armadas
/// **FNCS**	Foro Nacional de Ciberseguridad
/// **GARRTC**	Generación, atracción, rendimiento, retención de talento en ciberseguridad
/// **GCI**	Global Cybersecurity Index
/// **GEM**	Global Entrepreneurship Monitor
/// **GT**	Gestión del talento
/// **HPC**	Computación de alto rendimiento
/// **IA**	Inteligencia Artificial
/// **ICEX**	España Exportación e Inversiones
/// **ICO**	Instituto de Crédito Oficial
/// **ICT**	Tecnología de la Información y Comunicaciones
/// **I+D+i**	Investigación, desarrollo e innovación
/// **IoT**	Internet of Things
/// **INCIBE**	Instituto Nacional de Ciberseguridad
/// **JRC**	Joint Research Committee
/// **KPI**	Key Performance Indicator
/// **MCCE**	Mando conjunto del ciberespacio
/// **MD**	Ministerio de Defensa
/// **MINCOTUR**	Ministerio de Industria, Comercio y Turismo
/// **NCA**	National Capabilities Assessment Framework
/// **NCPI**	National Cyber Power Index
/// **NCSS**	National Cybersecurity Strategies

/// **NICE**	Iniciativa nacional para la educación en ciberseguridad
/// **NIST**	Instituto Norteamericano para los estándares y la tecnología
/// **OCC**	Oficina de Coordinación de Ciberseguridad
/// **ONTSI**	Observatorio Nacional de las Tecnologías y Sociedad de la Información
/// **PAE**	Punto de Atención al Emprendedor
/// **PESCO**	Cooperación Estructurada Permanente de la UE en materia de defensa
/// **PGE**	Presupuestos Generales del Estado
/// **PPP**	Public Private Partnership
/// **PVE**	Propuesta de valor del empleado
/// **RD**	Real Decreto
/// **RENIC**	Red de Excelencia Nacional de Investigación en Ciberseguridad
/// **RIE**	Real Instituto Elcano
/// **RIS**	EU Regional Innovation Scoreboard
/// **RSC**	Responsabilidad social corporativa
/// **RVCTI**	Red Vasca de Ciencia y Tecnología e Innovación
/// **SEPI**	Sociedad Estatal de Participaciones Industriales
/// **SGT1**	Subgrupo de Trabajo 1: Objetivos. Entregables
/// **SGT2**	Subgrupo de Trabajo 2: Conocimiento aplicado. Barómetro
/// **SGT3**	Subgrupo de Trabajo 3: Retos de pymes
/// **SGT4**	Subgrupo de Trabajo 4: Colaboración público – privada
/// **SGT5**	Subgrupo de Trabajo 5: Oportunidades para la I+D+i
/// **SGT6**	Subgrupo de Trabajo 6: Generación, transformación, retención y atracción del talento
/// **SGT7**	Subgrupo de Trabajo 7: Difusión y gestión de impacto
/// **SOAR**	Orquestación de la Seguridad, automatización y respuesta
/// **SOC**	Centro de operaciones de ciberseguridad
/// **SRIA**	Agenda Estratégica de Investigación e Innovación
/// **STEM**	Ciencias, Tecnología, Ingeniería y Matemáticas
/// **TIC**	Tecnología de la Información y Comunicaciones
/// **TRL**	Technological Readiness Level
/// **UE**	Unión europea
/// **UKCSA**	UK Cyber Sectorial Analysisi



I. Investigación básica e investigación aplicada

+ Anexos

Las tareas de investigación se pueden clasificar en dos grandes áreas de aplicación [81] [52]: investigación básica o fundamental e investigación aplicada:

· Investigación básica o fundamental. Se centra en liderar estudios y/o demostraciones teóricas para explicar la ocurrencia de un evento, proceso o fenómeno que, en el caso de la ciberseguridad, se asociaría a la temática en cuestión, a las tecnologías implicadas y en los verticales que esta aplica, según la taxonomía de capacidades que se analizará posteriormente.

· Investigación aplicada. Corresponde a aquellos estudios y métodos que intentan resolver ciertos problemas desde un punto de vista práctico y cercano a las necesidades actuales del mundo real, empleando teorías y principios conocidos y aceptados derivados, probablemente, de la propia investigación básica.

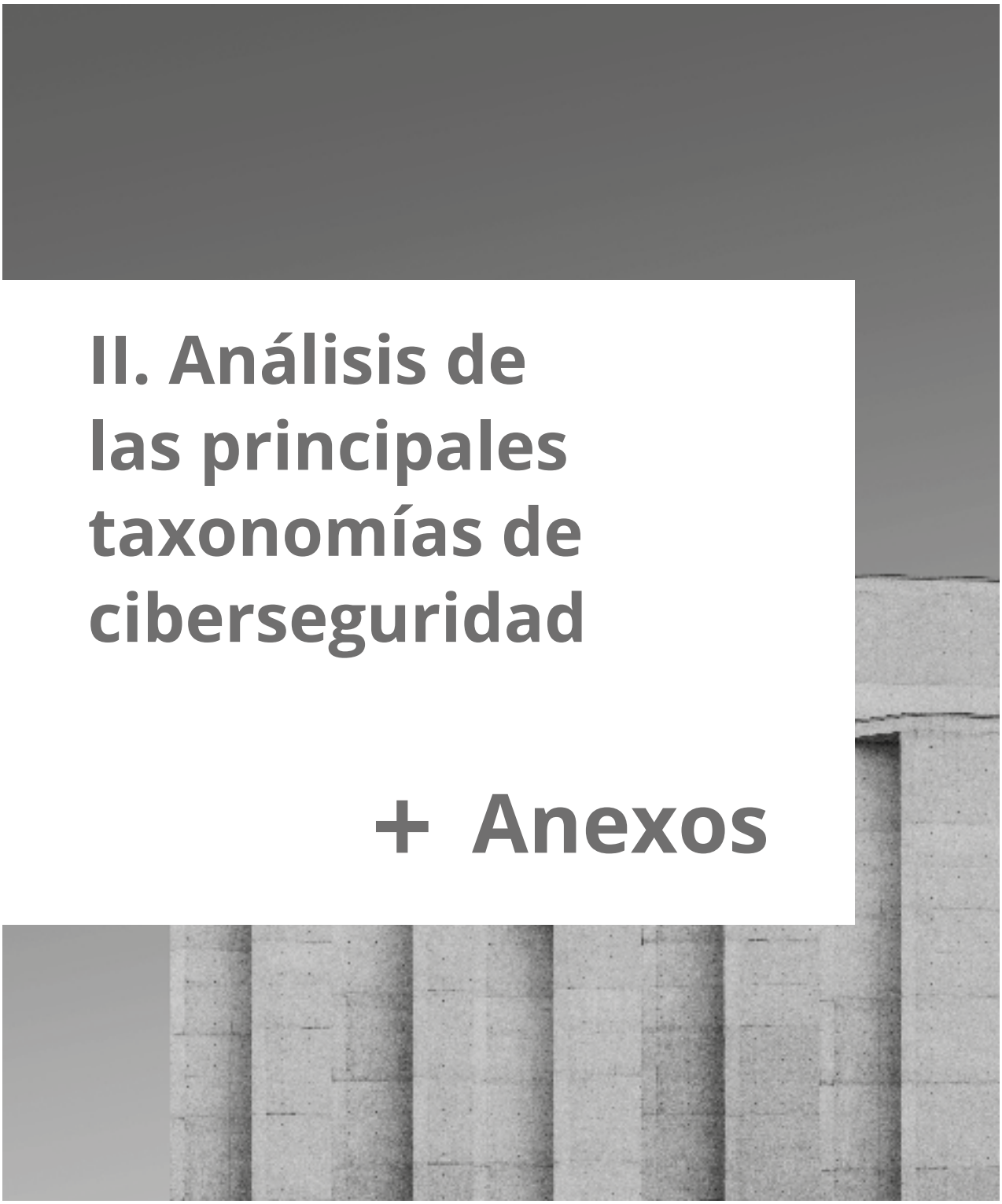
En la Tabla 8 se detallan las características de cada una de estas dos áreas de investigación, mientras que la Figura 12 ilustra las características comunes en términos de metodologías, fuentes de información y alcance, también descritos en [52].

Investigación fundamental o básica (I+D)	Investigación aplicada (I+D+i)
- Las hipótesis no necesariamente conducen a resultados inmediatos ni aplicaciones prácticas en el área de la ciberseguridad, tan solo a un análisis profundo y/o sistemático de un problema. -Puede ayudar a construir conocimiento y forma la base de muchas de las investigaciones aplicadas.	- El resultado de la investigación tiene una aplicación inmediata y práctica dentro del campo de la ciberseguridad. - Estudia casos específicos sin generalizar en un determinado problema.
Actores de investigación	
- Universidades - Institutos de investigación - Centros tecnológicos	- Universidades - Institutos de investigación - Centros tecnológicos - Centros de I+D+i - Empresas o fabricantes con departamento de I+D+i

Tabla 8. Diferencias conceptuales entre investigación fundamental y aplicada

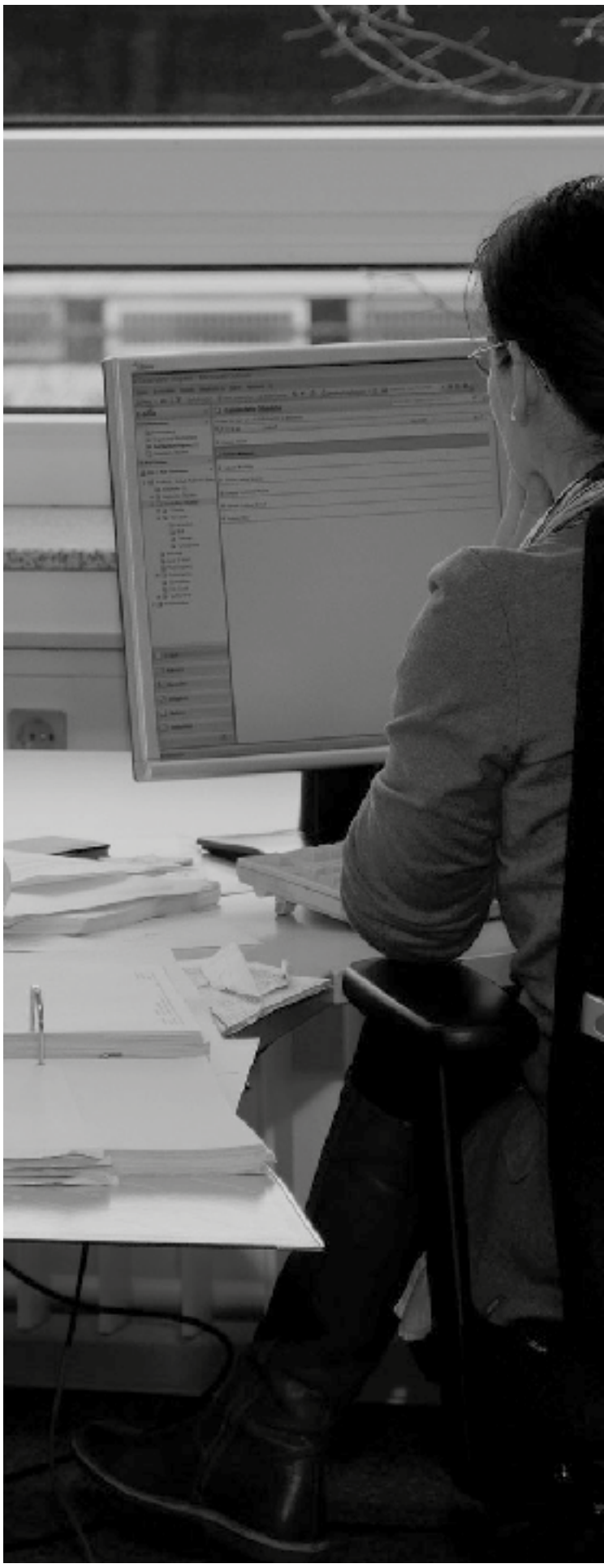
En la figura adjunta se resumen las metodologías, fuentes, áreas de estudio y alcance de la investigación en toda su amplitud.

Figura 10: Tipos de metodologías, fuentes, áreas de estudio y alcance



II. Análisis de las principales taxonomías de ciberseguridad

+ Anexos



A nivel nacional destaca la taxonomía utilizada por INCIBE en su Catálogo de empresas y soluciones de Ciberseguridad [49], también utilizada por RENIC en su Mapa de I+D+i en Ciberseguridad [84] y por la AEI de Ciberseguridad.

A principios del 2021, INCIBE realizó un estudio [50] repasando otras taxonomías de ciberseguridad que se utilizan internacionalmente:

· **ECSO**: su taxonomía se refleja en el Radar del Mercado europeo de proveedores de ciberseguridad [34] y también ha sido utilizada por el BCSC en su Informe de la Ciberseguridad en Euskadi [10].

· **Gartner**: su taxonomía se utiliza para mostrar la demanda de ciberseguridad a nivel mundial, por países y soluciones.

· **Momentum**: su taxonomía se utiliza para mostrar el panorama de la ciberseguridad de las principales empresas del sector.

· ***First Global Cybersecurity Observatory***: su taxonomía se utiliza para mostrar el panorama de la ciberseguridad de cualquier país.

· **Taxonomías de países como Países Bajos e Israel**.

A las anteriores debe añadirse la taxonomía realizada por el Joint Research Centre (JRC) [54], servicio científico interno de la Comisión Europea, que en su primera versión permitió el mapeo de más de 600 centros europeos de I+D+i en ciberseguridad.

Posteriormente, los cuatro pilotos europeos para ayudar a la Comisión Europea al establecimiento de una Red de Competencia en Ciberseguridad (CONCORDIA, ECHO, SPARTA y CyberSec4Europe) revisaron la taxonomía JRC, proporcionando recomendaciones para desarrollar una segunda versión de la misma.

III. Taxonomía de competencias en la industria (ECSO)

+ Anexos

La taxonomía de capacidades definida por ECSO [34] se utiliza principalmente por los actores de la Industria. Está constituida por 5 funciones, 21 categorías y 60 subcategorías.

Seguidamente se proporciona la lista de las 60 subcategorías agrupadas por las cinco funciones principales: **Identify, Protect, Detect, Respond & Recover**.

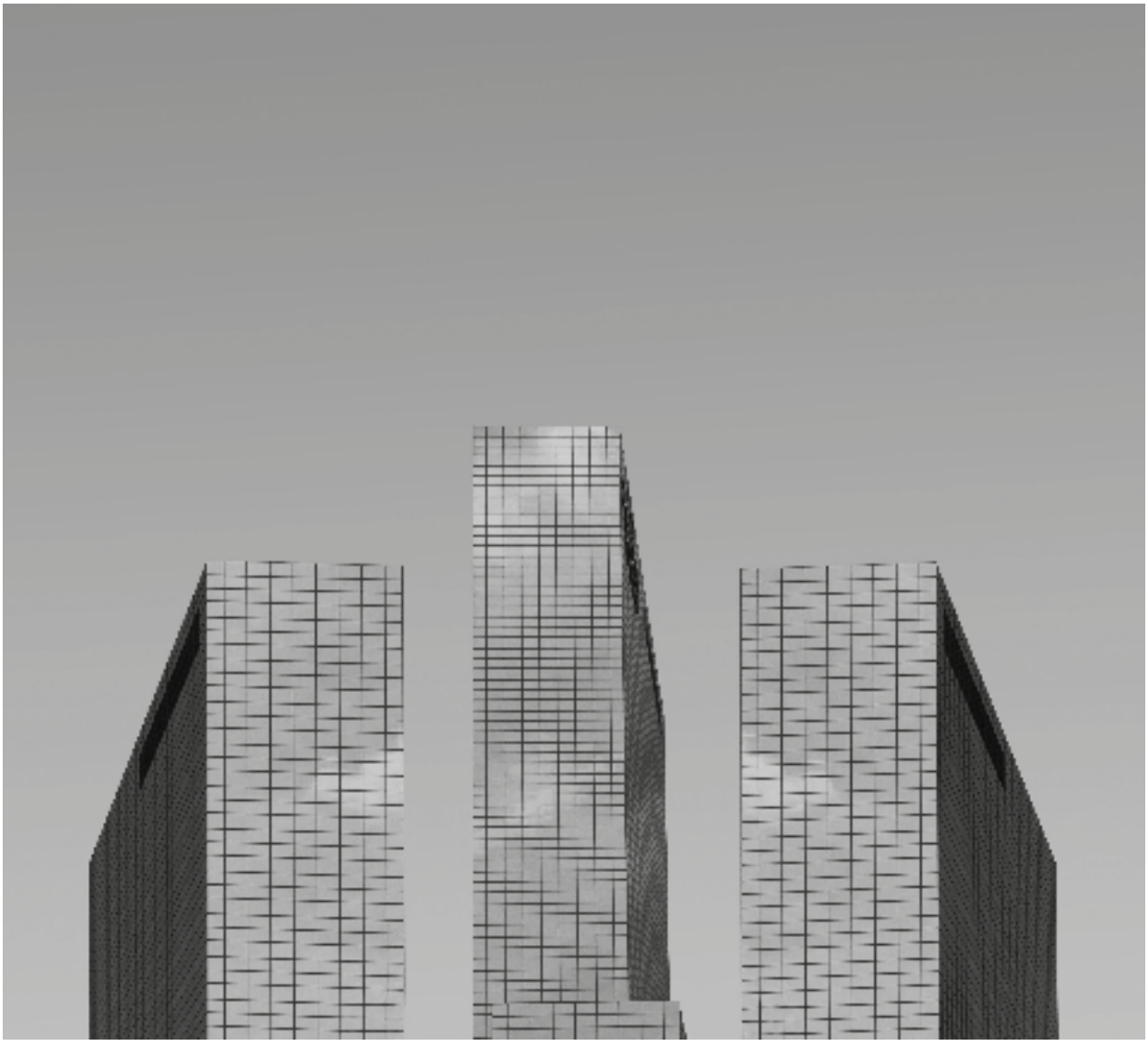
INDUSTRIA - TAXONOMIA ECSO - QUÉ			
ID	Función	Categoría	Subcategoría
1	Identify	Asset Management	Software & Security Lifecycle Management
2	Identify	Asset Management	IT Service Management
3	Identify	Business Environment	Business Impact Analysis
4	Identify	Governance & Risk Management	Governance, Risk & Compliance (GRC)
5	Identify	Governance & Risk Management	Governance, Risk & Compliance (GRC)
6	Identify	Risk Assessment	Risk Management solutions & services
7	Identify	Risk Management Strategy	Risk Management Strategy Development & Consulting
8	Identify	Supply Chain Risk Management	Supply chain risk monitoring solutions & services

INDUSTRIA - TAXONOMIA ECSO - QUÉ			
ID	Función	Categoría	Subcategoría
9	Protect	Identity Management & Access Control	Access Management
10	Protect	Identity Management & Access Control	Authentication
11	Protect	Identity Management & Access Control	Authorisation
12	Protect	Identity Management & Access Control	Identity Management
13	Protect	Awareness and Training	Awareness Trainings
14	Protect	Awareness and Training	Cyber Ranges
15	Protect	Data Security	PKI / Digital Certificates
16	Protect	Data Security	Data Leakage Prevention
17	Protect	Data Security	Encryption
18	Protect	Data Security	Cloud Access Security Brokers
19	Protect	Data Security	Hardware Security Modules (HSM)
20	Protect	Data Security	Digital Signature
21	Protect	Information Protection Processes and Procedures	Application Security
22	Protect	Information Protection Processes and Procedures	Static Application Security Testing (SAST)
23	Protect	Maintenance	Patch Management
24	Protect	Maintenance	Vulnerability Management
25	Protect	Maintenance	Penetration Testing / Red Teaming
26	Protect	Protective Technology	Wireless Security
27	Protect	Protective Technology	Remote Access / VPN
28	Protect	Protective Technology	IoT Security
29	Protect	Protective Technology	PC/Mobile/End Point Security
30	Protect	Protective Technology	Mobile Security /Device management
31	Protect	Protective Technology	Sandboxing
32	Protect	Protective Technology	Content Filtering & Monitoring
33	Protect	Protective Technology	Firewalls / NextGen Firewalls
34	Protect	Protective Technology	Unified Threat Management (UTM)
35	Protect	Protective Technology	Anti Spam
36	Protect	Protective Technology	Anti Virus/Worm/Malware
37	Protect	Protective Technology	Backup / Storage Security

INDUSTRIA - TAXONOMIA ECSO - QUÉ			
ID	Función	Categoría	Subcategoría
38	Detect	Anomalies and Events	
39	Detect	Anomalies and Events	
40	Detect	Security Continuous Monitoring	
41	Detect	Security Continuous Monitoring	
42	Detect	Security Continuous Monitoring	
43	Detect	Detection Processes	
44	Detect	Detection Processes	
45	Detect	Detection Processes	

INDUSTRIA - TAXONOMIA ECSO - QUÉ			
ID	Función	Categoría	Subcategoría
46	Respond	Planing Response	Incident Management
47	Respond	Planing Response	Crisis Management
48	Respond	Communication	Crisis Communication
49	Respond	Analysis	Fraud Investigation
50	Respond	Analysis	Forensics
51	Respond	Mitigation	Cyber Security Insurance
52	Respond	Mitigation	DDoS protection
53	Respond	Mitigation	Data Recovery
54	Respond	Mitigation	Incident Response Services (CSRIT aaS)
55	Respond	Mitigation	Takedown Services
56	Respond	Improvements	Containment support

INDUSTRIA - TAXONOMIA ECSO - QUÉ			
ID	Función	Categoría	Subcategoría
57	Recover	Recover y Planning	System Recovery
58	Recover	Recover y Planning	Business Continuity/ Recovery Planning
59	Recover	Improvements	Post Incident reviews & consulting
60	Recover	Communication	Communications coaching & consulting



IV. Taxonomía de competencias en la investigación (JRC)

+ Anexos

La taxonomía de capacidades definida por la Comisión Europea Joint Research Comitee (JRC) [54] se utiliza principalmente por los actores de la Investigación. Es una taxonomía basada en tres dimensiones:

· **Dominios de Investigación**, constituida por 15 categorías y 149 subcategorías.
· **Tecnologías y Casos de Uso**, constituida por 23 casos de uso.
· **Sectores**, constituida por 15 sectores.

Seguidamente se proporciona una lista de las 149 subcategorías agrupadas en las 15 categorías.

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	Categoría	Subcategoría
1	Assurance Audit and Certification	Assurance
2		Audit
3		Assessment
4		Certification
5	Cryptology (Cryptography & Cryptoanalisys	Asymmetric cryptography
6		Symmetric cryptography
7		Cryptanalysis methodologies, techniques and tools
8		Functional encryption
9		Mathematical foundations of cryptography
10		Crypto material management (e.g. key management, PKI)
11		Secure multi-party computation
12		Random number generation
13		Digital signatures
14		Hash functions
15		Message authentication
16		Quantum cryptography
17		Post-quantum cryptography
18		Homomorphic encryption
19		Privacy requirements for data management systems

INDUSTRIA - TAXONOMIA ECSO - QUÉ7		
ID	Categoría	Subcategoría
20	Data Security and Privacy	Design, implementation, and operation of data management systems that include security and privacy functions
21		Anonymity, pseudonymity, unlinkability, undetectability, or unobservability30
22		Data integrity
23		Privacy Enhancing Technologies (PET)
24		Digital Rights Management (DRM)
25		Risk analysis and attacks with respect to de-anonymization or data re-identification (e.g. inference attack)
26		Eavesdropping techniques (e.g. via electromagnetic radiation, visual observation of blinking LEDs, acoustic via keyboard typing noise)
27		Data usage control
28	Educational and Training	Higher Education
29		Professional training
30		Cybersecurity-aware culture (e.g. including children education)
31		Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness
32		Education methodology
33	Human Aspects	Vocational training
34		Accessibility
35		Usability
36		Human-related risks/threats (social engineering, insider misuse, etc.)
37		Socio-technical security
38		Enhancing risk perception
39		Psychological models and cognitive processes; Forensic cyberpsychology
40		User acceptance of security policies and technologies
41		Automating security functionality
42		Non-intrusive security
43		Privacy concerns, behaviours, and practices
44		Computer ethics and security
45		Transparent security
46		Cybersecurity profiling
47		Cyberpsychology
48		Security visualization
49		Gamification
50		Human aspects of trust
51		Human perception of cybersecurity
52	Identity Management	History of cybersecurity
53		Identity and attribute management models, frameworks, applications, technologies, and tools (e.g. PKI, RFID, SSO, attribute-based credentials, federated IdM etc.)
54		Protocols and frameworks for authentication, authorization, and rights management
55		Privacy and identity management (e.g. privacy-preserving authentication)
56		Identity management quality assurance
57		Optical and electronic document security
58		Legal aspects of identity management
59		Biometric methods, technologies and tools
60	Incident Handling and Digital Forensics	Incident analysis, communication, documentation, forecasting (intelligence based), response, and reporting
61		Theories, techniques and tools for the identification, collection, attribution, acquisition, analysis and preservation of digital evidence (e.g. code authorship and attacker identification, provenance assurance, digital evidence correlation, digital evidence triage)
62		Vulnerability analysis and response
63		Digital forensic processes and workflow models
64		Digital forensic case studies
65		Policy issues related to digital forensics
66		Resilience aspects
67		Anti-forensics and malware analytics
68		Citizen cooperation and reporting
69		Coordination and information sharing in the context of cross-border/organizational incidents
70	Legal Aspects	Cybercrime prosecution and law enforcement
71		Intellectual property rights
72		Cybersecurity regulation analysis and design
73		Investigations of computer crime (cybercrime) and security violations
74		Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation).

INDUSTRIA - TAXONOMIA ECSO - QUÉ7		
ID	Categoría	Subcategoría
75	Network and Distributed Systems	Network security (principles, methods, protocols, algorithms and technologies)
76		Distributed systems security
77		Managerial, procedural and technical aspects of network security
78		Requirements for network security
79		Protocols and frameworks for secure distributed computing
80		Network layer attacks and mitigation techniques
81		Network attack propagation analysis
82		Distributed systems security analysis and simulation
83		Distributed consensus techniques
84		Fault tolerant models
85		Secure distributed computations
86		Network interoperability
87		Secure system interconnection
88		Privacy-friendly communication architectures and services (e.g. Mix-networks, broadcast protocols, and anonymous communication)
89		Network steganography
90	Security Management and Governance	Risk management, including modelling, assessment, analysis and mitigations
91		Modelling of cross-sectoral interdependencies and cascading effects
92		Threats and vulnerabilities modelling
93		Attack modelling, techniques, and countermeasures (e.g. adversary machine learning)
94		Managerial aspects concerning information security
95		Assessment of information security effectiveness and degrees of control
96		Identification of the impact of hardware and software changes on the management of Information Security
97		Standards for Information Security
98		Governance aspects of incident management, disaster recovery, business continuity
99		Techniques to ensure business continuity/disaster recovery
100		Compliance with information security and privacy policies, procedures, and regulations
101		Economic aspects of the cybersecurity ecosystem
102		Privacy impact assessment and risk management
103		Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling)
104		Capability maturity models (e.g. assessment of capacities and capabilities)
105	Security Measurements	Security analytics and visualization
106		Security metrics, key performance indicators, and benchmarks
107		Validation and comparison frameworks for security metrics
108	Software and Hardware Security Engineering	Measurement and assessment of security levels
109		Security requirements engineering with emphasis on identity, privacy, accountability, and trust
110		Security and risk analysis of components compositions
111		Secure software architectures and design (security by design)
112		Security design patterns
113		Secure programming principles and best practices
114		Security support in programming environments
115		Security documentation
116		Refinement and verification of security management policy models
117		Runtime security verification and enforcement
118		Security testing and validation
119		Vulnerability discovery and penetration testing
120		Quantitative security for assurance
121		Intrusion detection and honeypots
122		Malware analysis including adversarial learning of malware
123		Model-driven security and domain-specific modelling languages
124		Self-* including self-healing, self-protecting, self-configuration systems
125		Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks)
126		Fault injection testing and analysis
127		Cybersecurity and cyber-safety co-engineering
128		Privacy by design
129	Steganography, Steganalysus and Watermarking	Steganography
130		Steganalysis
131		Digital watermarking

INDUSTRIA - TAXONOMIA ECSO - QUÉ7		
ID	Categoría	Subcategoría
132	Theoretical Foundations	Formal specification of various aspects of security (e.g properties, threat models, etc.)
133		Formal specification, analysis, and verification of software and hardware
134		Information flow modelling and its application to confidentiality policies, composition of systems, and covert channel analysis
135		New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications
136		Formal verification of security assurance
137		Cybersecurity uncertainty models
138		Cybersecurity concepts, definitions, ontologies, taxonomies, foundational aspects
139	Trust Management and Accountability	Semantics and models for security, accountability, privacy, and trust
140		Trust management architectures, mechanisms and policies
141		Trust and privacy
142		Identity and trust management
143		Trust in securing digital as well as physical assets
144		Trust in decision making algorithms
145		Trust and reputation of social and mainstream media
146		Social aspects of trust
147		Reputation models
148		Trusted computing
149		Algorithmic auditability and accountability (e.g. explainable AI)

En la segunda dimensión de la taxonomía JRC se detallan las 23 Tecnologías y Casos de Uso aplicables para la clasificación de las capacidades.

USER CASES - JRC	
ID	Subcategoría
1	Artificial Intelligence & Big Data Analytics
2	Big Data
3	Blockchain and Distributed Ledger Technology (DLT)
4	Cloud, Edge and Virtualization
5	Critical Infrastructures Protection (CIP)
6	Protection of public spaces
7	Disaster resilience and crisis management
8	Fight against crime and terrorism
9	Border and external security
10	Local/wide area observation and surveillance
11	Hardware technology (RFID, Networking, etc.)
12	High-Performance Computing (HPC)
13	Human Machine Interface (HMI)
14	Industrial IoT and Control Systems (e.g. SCADA & CPS)
15	Information Systems
16	Internet of Things, Embedded Systems, Pervasive Systems
17	Mobile Devices
18	Operating Systems
19	Quantum Technologies (e.g. Computing & communication)
20	Robotics
21	Satellite systems and applications
22	Vehicular Systems (e.g. autonomous vehicles)
23	UAV (unmanned aerial vehicles)

V. Propuesta de taxonomía integrada

+ Anexos

En este Anexo se propone una taxonomía integrada donde se establece un modelo de relación entre ECSO y JRC, de tal modo que exista una trazabilidad detalla la taxonomía de capacidades definida por ECSO [34] que se utiliza principalmente por los actores de la Industria. Está constituida por 5 funciones, 21 categorías y 60 subcategorías.

Seguidamente se proporciona la lista de las 60 subcategorías agrupadas por las cinco funciones principales: *Identify, Protect, Detect, Respond & Recover.*

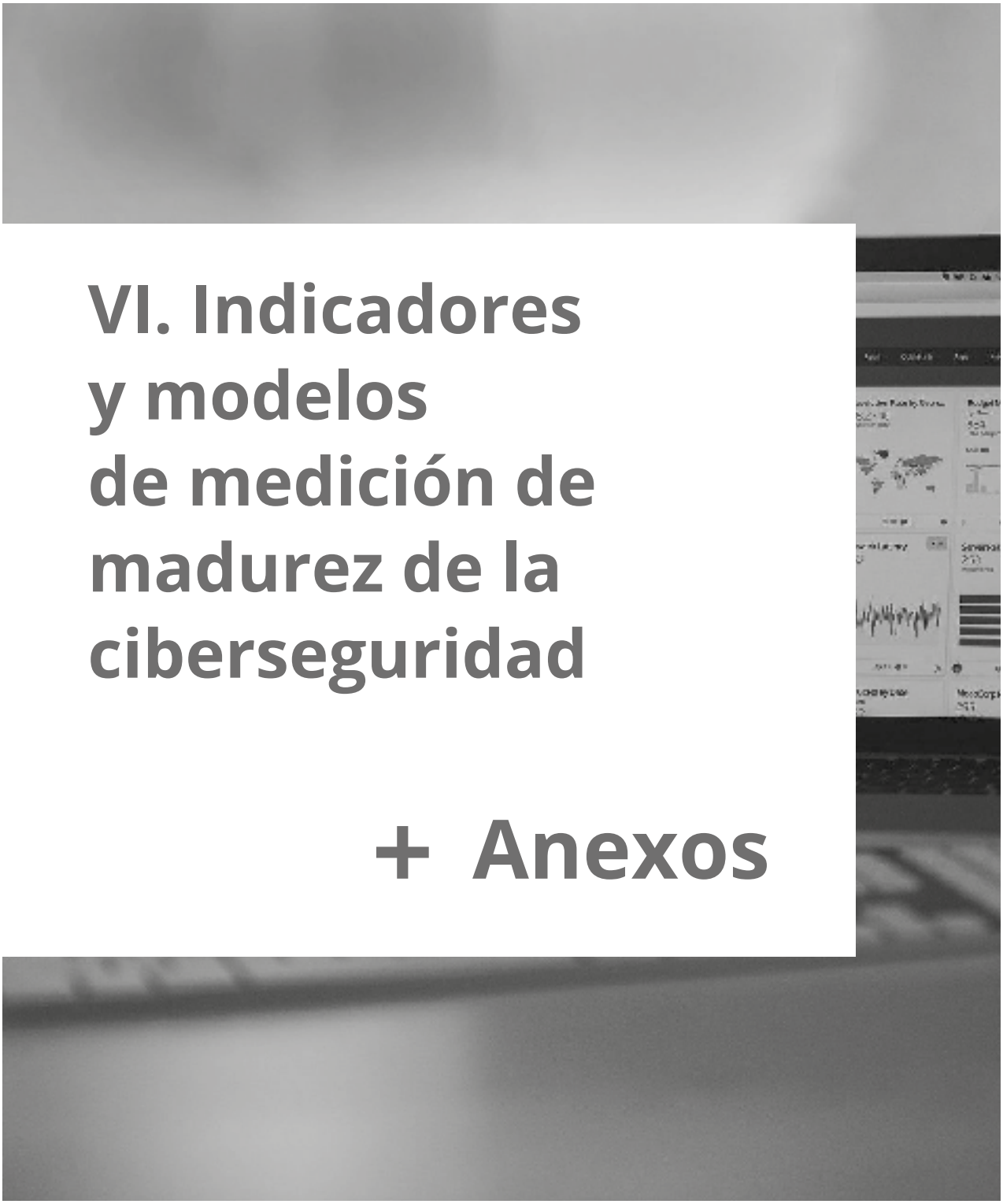
TAXONOMÍA ECSO				TAXONOMÍA JRC			
ID	Función	Categoría	Subcategoría	JRC-1	TAXONOMIA JRC - PRIMARIO	JRC-2	TAXONOMÍA JRC - SECUNDARIO
1	Identify	Asset Management	Software & Security Lifecycle Management	103, 109, 111, 112, 113, 114, 123, 124, 127, 128	Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling);Security requirements engineering with emphasis on identity, privacy, accountability, and trust; Secure software architectures and design (security by design); Security design patterns; Secure programming principles and best practices; Security support in programming environments; Model-driven security and domain-specific modelling languages; Self-* including self-healing, self-protecting, self-configuration systems; Cybersecurity and cyber-safety co-engineering; Privacy by design.	115, 116, 117, 133	Security documentation; Refinement and verification of security management policy models; Security testing and validation; Formal specification, analysis, and verification of software and hardware;
2	Identify	Asset Management	IT Service Management	94, 134	Managerial aspects concerning information security; Information flow modelling and its application to confidentiality policies, composition of systems, and covert channel analysis.		
3	Identify	Business Environment	Business Impact Analysis	72, 74, 101, 102, 137	Cybersecurity regulation analysis and design; Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation); Economic aspects of the cybersecurity ecosystem; Privacy impact assessment and risk management; Cybersecurity uncertainty models;		
4	Identify	Governance & Risk Management	Governance, Risk & Compliance (GRC)	1, 24, 40, 43, 44, 97, 106, 107, 108, 115, 116, 120, 138, 139, 140, 146	Assurance; Digital Rights Management (DRM); User acceptance of security policies and technologies; Privacy concerns, behaviours, and practices; Computer ethics and security; Standards for Information Security; Security metrics, key performance indicators, and benchmarks; Validation and comparison frameworks for security metrics; Measurement and assessment of security levels; Security documentation; Refinement and verification of security management policy models; Cybersecurity concepts, definitions, ontologies, taxonomies, foundational aspects; Quantitative security for assurance; Semantics and models for security, accountability, privacy, and trust; Semantics and models for security, accountability, privacy, and trust; Trust management architectures, mechanisms and policies; Social aspects of trust;		Techniques to ensure business continuity/disaster recovery, 99; Compliance with information security and privacy policies, procedures, and regulations, 100;
5	Identify	Governance & Risk Management	Security Certification	2, 3, 4, 65, 100, 132, 136	Audit; Assesment; Certification; Policy issues related to digital forensics; Compliance with information security and privacy policies, procedures, and regulations; Formal specification of various aspects of security (e.g properties, threat models, etc.); Formal verification of security assurance;		
6	Identify	N/A	Supply Chain Risk Assessment				
7	Identify	N/A	Risk Management Strategy	38, 90, 91, 92, 93, 96	Enhancing risk perception; Risk management, including modelling, assessment, analysis and mitigations; Modelling of cross-sectoral interdependencies and cascading effects; Threats and vulnerabilities modelling; Attack modelling, techniques, and countermeasures (e.g. adversary machine learning); Identification of the impact of hardware and software changes on the management of Information Security	102	Privacy impact assessment and risk management;
8	Identify	N/A	Risk Assessment	25, 26, 95, 104, 110	Risk analysis and attacks with respect to de-anonymization or data re-identification (e.g. inference attack); Eavesdropping techniques (e.g. via electromagnetic radiation, visual observation of blinking LEDs, acoustic via keyboard typing noise); Assment of information security effectiveness and degrees of control; Capability maturity models (e.g. assessment of capacities and capabilities); Security and risk analysis of components compositions;	90, 91, 92, 93, 96	Risk management, including modelling, assessment, analysis and mitigations; Modelling of cross-sectoral interdependencies and cascading effects; Threats and vulnerabilities modelling; Attack modelling, techniques, and countermeasures (e.g. adversary machine learning); Identification of the impact of hardware and software changes on the management of Information Security

TAXONOMÍA ECSO				TAXONOMÍA JRC			
ID	Función	Categoría	Subcategoría	JRC-1	TAXONOMIA JRC - PRIMARIO	JRC-2	TAXONOMÍA JRC - SECUNDARIO
9	Protect	Identity Management & Access Control	Access Management	34, 45	Accessibility; Transparent security		
10	Protect	Identity Management & Access Control	Authentication	59	Biometric methods, technologies and tools.	54	Protocols and frameworks for authentication, authorization, and rights management
11	Protect	Identity Management & Access Control	Authorisation	54	Protocols and frameworks for authentication, authorization, and rights management	54	Protocols and frameworks for authentication, authorization, and rights management
12	Protect	Identity Management & Access Control	Identity Management	46, 53, 58, 55, 56, 142	Cybersecurity profiling; Identity and attribute management models, frameworks, applications, technologies, and tools (e.g. PKI, RFID, SSO, attribute-based credentials, federated IdM etc.); Legal aspects of identity management; Privacy and identity management (e.g. privacy-preserving authentication); Identity management quality assurance; Cybersecurity profiling; Identity and trust management	54	Protocols and frameworks for authentication, authorization, and rights management
13	Protect	Awareness and Training	Awareness Trainings	28, 29, 30, 32, 33, 36, 39, 47, 49, 50, 51, 52, 68	Higher Education; Professional training; Cybersecurity-aware culture (e.g. including children education); Education methodology; Vocational training; Human-related risks/threats (social engineering, insider misuse, etc.); Psychological models and cognitive processes; Forensic cyberpsychology; Cyberpsychology; Human aspects of trust; Human perception of cybersecurity; Gamification; History of cybersecurity; Citizen cooperation and reporting;		
14	Protect	Awareness and Training	Cyber Ranges	31	Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/ training tools, cybersecurity awareness;		
15	Protect	Data Security	PKI / Digital Certificates	10, 135	Crypto material management (e.g. key management, PKI); New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications;		
16	Protect	Data Security	Data Leakage Prevention	19, 20, 21, 23, 27, 48, 57, 71, 141, 148	Privacy requirements for data management systems; Design, implementation, and operation of data management systems that include security and privacy functions; Anonymity, pseudonymity, unlinkability, undetectability, or unobservability30; Privacy Enhancing Technologies (PET); Data usage control; Security visualization; Optical and electronic document security; Intellectual property rights; Trust and privacy; Trusted computing;	128	Protocols and frameworks for secure distributed computing; Privacy by design;
17	Protect	Data Security	Encryption	5, 6, 7, 8, 9, 11, 12, 14, 16, 17, 18, 22, 129, 130	Asymmetric cryptography; Symmetric cryptography; Cryptanalysis methodologies, techniques and tools; Functional encryption; Mathematical foundations of cryptography; Secure multi-party computation; Random number generation; Hash functions; Quantum cryptography;Post-quantum cryptography;Homomorphic encryption; Data integrity; Steganography; Steganalysis;	135, 148	New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications; Trusted computing;
18	Protect	Data Security	Cloud Access Security Brokers	85	Secure distributed computations;		
19	Protect	Data Security	Hardware Security Modules (HSM)	133	Formal specification, analysis, and verification of software and hardware;		
20	Protect	Data Security	Digital Signature	13, 15, 131	Digital signatures; Message authentication; Digital watermarking		
21	Protect	Information Protection Processes and Procedures	Application Security	41, 149	Automating security functionality; Algorithmic auditability and accountability (e.g. explainable AI).		
22	Protect	Information Protection Processes and Procedures	Static Application Security Testing (SAST)	118	Security testing and validation;	125, 126, 119	Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks); Fault injection testing and analysis; Vulnerability discovery and penetration testing; Fault injection testing and analysis;
23	Protect	Maintenance	Patch Management				
24	Protect	Maintenance	Vulnerability Management	92		92, 119	Threats and vulnerabilities modelling; Vulnerability discovery and penetration testing;
25	Protect	Maintenance	Penetration Testing / Red Teaming	119, 126	Vulnerability discovery and penetration testing; Fault injection testing and analysis;		
26	Protect	Protective Technology	Wireless Security	88	Privacy-friendly communication architectures and services (e.g. Mix-networks, broadcast protocols, and anonymous communication);		
27	Protect	Protective Technology	Remote Access / VPN	78, 87, 89	Requirements for network security; Secure system interconnection; Network steganography.		
28	Protect	Protective Technology	IoT Security				
29	Protect	Protective Technology	PC/Mobile/End Point Security	35, 37, 42	Usability; Socio-technical security; Non-intrusive security;		
30	Protect	Protective Technology	Mobile Security /Device management	143	Trust in securing digital as well as physical assets;		
31	Protect	Protective Technology	Content Filtering & Monitoring	77, 83	Managerial, procedural and technical aspects of network security; Distributed consensus techniques;		
32	Protect	Protective Technology	Firewalls / NextGen Firewalls	75, 80, 81, 86	Network security (principles, methods, protocols, algorithms and technologies); Network layer attacks and mitigation techniques; Network attack propagation analysis; Network interoperability;		
33	Protect	Protective Technology	Unified Threat Management (UTM)	76, 82	Distributed systems security; Distributed systems security analysis and simulation;		
34	Protect	Protective Technology	Anti Spam			122	Malware analysis including adversarial learning of malware;
35	Protect	Protective Technology	Anti Virus/Worm/ Malware	67	Anti-forensics and malware analytics;	122	Malware analysis including adversarial learning of malware;
36	Protect	Protective Technology	Backup / Storage Security	84	Fault tolerant models;		

TAXONOMÍA ECSO				TAXONOMÍA JRC			
ID	Función	Categoría	Subcategoría	JRC-1	TAXONOMIA JRC - PRIMARIO	JRC-2	TAXONOMÍA JRC - SECUNDARIO
37	Detect	Anomalies and Events	Fraud Management	70	Cybercrime prosecution and law enforcement;		
38	Detect	Anomalies and Events	Intrusion Detection	79	Protocols and frameworks for secure distributed computing;	121	Intrusion detection and honeypots;
39	Detect	Security Continuous Monitoring	SIEM / Event Correlation Solutions	117, 144	Runtime security verification and enforcement; Trust in decision making algorithms;		
40	Detect	Security Continuous Monitoring	Cyber Threat Intelligence	125	Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks);	67, 122	Anti-forensics and malware analytics; Malware analysis including adversarial learning of malware;
41	Detect	Security Continuous Monitoring	Security Operations Center (SOC)	105	Security analytics and visualization;		
42	Detect	Detection Processes	Underground/Darkweb investigation			119	Vulnerability discovery and penetration testing;
43	Detect	Detection Processes	Honeypots / Cybertraps	121	Intrusion detection and honeypots;		
44	Detect	Detection Processes	Social Media & Brand Monitoring	145, 147	Trust and reputation of social and mainstream media; Reputation models;		
45	Respond	Planing Response	Incident Management	60	Incident analysis, communication, documentation, forecasting (intelligence based), response, and reporting;		
46	Respond	Planing Response	Crisis Management				
47	Respond	Communication	Crisis Communication				
48	Respond	Analysis	Fraud Investigation	73	Investigations of computer crime (cybercrime) and security violations;		
49	Respond	Analysis	Forensics	61, 63, 64, 122	Theories, techniques and tools for the identification, collection, attribution, acquisition, analysis and preservation of digital evidence (e.g. code authorship and attacker identification, provenance assurance, digital evidence correlation, digital evidence triage); Digital forensic processes and workflow models; Digital forensic case studies; Malware analysis including adversarial learning of malware;		
50	Respond	Mitigation	Cyber Security Insurance				
51	Respond	Mitigation	DDoS protection			124	Self-* including self-healing, self-protecting, self-configuration systems;
52	Respond	Mitigation	Data Recovery				
53	Respond	Mitigation	Services (CSRIT aaS)	69	Coordination and information sharing in the context of cross-border/ organizational incidents.		
54	Respond	Mitigation	Incident Response	62	Vulnerability analysis and response;	144	Trust in decision making algorithms;
55	Respond	Mitigation	Takedown Services				
56	Respond	Improvements	N/A				
57	Recover	Improvements	N/A				
58	Recover	Recover y Planning	Business Continuity/ Recovery Planning	98, 66	Governance aspects of incident management, disaster recovery, business continuity; Resilience aspects;	124	Self-* including self-healing, self-protecting, self-configuration systems;
59	Recover	Recover y Planning	System Recovery	99	Techniques to ensure business continuity/disaster recovery		
60	Recover	Communication	N/A				

Igualmente se tendrá en cuenta la clasificación por Casos de Uso para la identificación de capacidades.

USER CASES - JRC	
ID	Subcategoría
1	Artificial Intelligence & Big Data Analytics
2	Big Data
3	Blockchain and Distributed Ledger Technology (DLT)
4	Cloud, Edge and Virtualization
5	Critical Infrastructures Protection (CIP)
6	Protection of public spaces
7	Disaster resilience and crisis management
8	Fight against crime and terrorism
9	Border and external security
10	Local/wide area observation and surveillance
11	Hardware technology (RFID, Networking, etc.)
12	High-Performance Computing (HPC)
13	Human Machine Interface (HMI)
14	Industrial IoT and Control Systems (e.g. SCADA & CPS)
15	Information Systems
16	Internet of Things, Embedded Systems, Pervasive Systems
17	Mobile Devices
18	Operating Systems
19	Quantum Technologies (e.g. Computing & communication)
20	Robotics
21	Satellite systems and applications
22	Vehicular Systems (e.g. autonomous vehicles)
23	UAV (unmanned aerial vehicles)



VI. Indicadores y modelos de medición de madurez de la ciberseguridad

+ Anexos

La mayor parte de los indicadores se han diseñado para medir grados y objetos de madurez genéricos, en los que los componentes industriales y de investigación tienen un desarrollo limitado. Así, se puede encontrar una comparación de los modelos de madurez globales en el informe de ENISA sobre National Capabilities Assessment Framework – NCAF [20].

Los últimos modelos de medición de madurez aparecidos en 2020 prestan mayor atención los aspectos de industria e investigación:

· Cyber Power Index (CPI), de Economist Intelligence Unit [17]. Compara la madurez de los países del G20 en los contextos regulatorio, económico, infraestructuras, aplicaciones industriales y social (incluidos educación e I+D+i).

· National Cyber Power Index (NCPI), de Belfer Center de Harvard Kennedy School [5]. Mide las capacidades en ciberseguridad de 30 países para monitorizar su ecosistema, reforzar sus capacidades defensivas y ofensivas, potenciar el crecimiento industrial y comercial o definir estándares y normas, entre otros, mediante indicadores cuantitativos (32) y cualitativos (27).

· National Capabilities Assessment Framework (NCAF), de ENISA [20].

Este último merece especial interés porque puede convertirse en el estándar europeo de madurez, ya que se ha elaborado para que los Estados miembros desarrollen y adapten sus estrategias de ciberseguridad (National Cybersecurity Strategies – NCSS). Establece las siguientes dimensiones y factores: políticas y estratégicas (6), cultura (5), conocimiento (3), regulación (3) y riesgos (7). Se clasifican según su madurez en: inicial, en formación, establecida, estratégica y dinámica.

El NCAF [20] armoniza diecisiete objetivos estratégicos estructurados en cuatro grupos: Gobierno y estándares (3), Capacidad de construcción y concienciación (7), Marco legal y regulatorio (4) y Cooperación (3). Entre dichos objetivos figuran algunos para fomentar la investigación y el desarrollo de productos y servicios de ciberseguridad, y pretende evaluar las debilidades de la I+D+i, estimular los intercambios entre sus miembros, estrechar la relación entre investigación e industria y mejorar la oferta de productos y servicios.

Los modelos más conocidos analizan la contribución de los países al avance de la agenda global de la ciberseguridad o el avance de sus propias agendas.

· Global Cybersecurity Index (GCI) de la International Telecommunications Union (ITU) [53]. Los veinticinco indicadores del GCI miden la madurez legal, técnica, organizacional, intangibles y acuerdos de cooperación que la ITU considera necesarios para medir el compromiso de las agendas de ciberseguridad de los países respecto a la agenda global.

· Cybersecurity Capacity Maturity Model for Nations (CMM) [77]. El CMM del Global Cyber Security Capacity Centre de la Universidad de Oxford agrupa los distintos indicadores en cinco áreas de política, regulación, formación, organización y cultura.

· UK Cyber Sectorial Analysis (UKCSA) [89]. Facilita información global del sector en Reino Unido, incluyendo información económica.

Todos ellos aportan gran valor para identificar la madurez del ecosistema de ciberseguridad. Sin embargo, no miden en detalle la madurez de los subsistemas de la industria y la investigación dentro de la ciberseguridad, aunque ofrecen algunos indicadores que se pueden aprovechar para ese fin.

Por el contrario, indicadores como el de ECSO [35] para evaluar el acuerdo de colaboración público-privada de ciberseguridad sí tienen en cuenta aspectos de investigación y desarrollo, siempre en el ámbito del acuerdo entre ECSO y la Comisión Europea, donde los participantes deben proporcionar información sobre las características de su organización, las inversiones dedicadas, los empleos y sus perfiles, así como las medidas de diseminación y comunicación.

También se han consultado modelos que miden la madurez interna de los actores, como los diseñados por el NIST [75] para las infraestructuras críticas o por Logitech [55] que compara la madurez de las organizaciones en IT y OT mediante CMM2 para las organizaciones de ciberseguridad. En la práctica, no tienen utilidad a los efectos del presente Informe ya que han sido diseñados para evaluar las funciones de identificación, protección, detección, respuesta y recuperación de entidades, y no de ecosistemas.

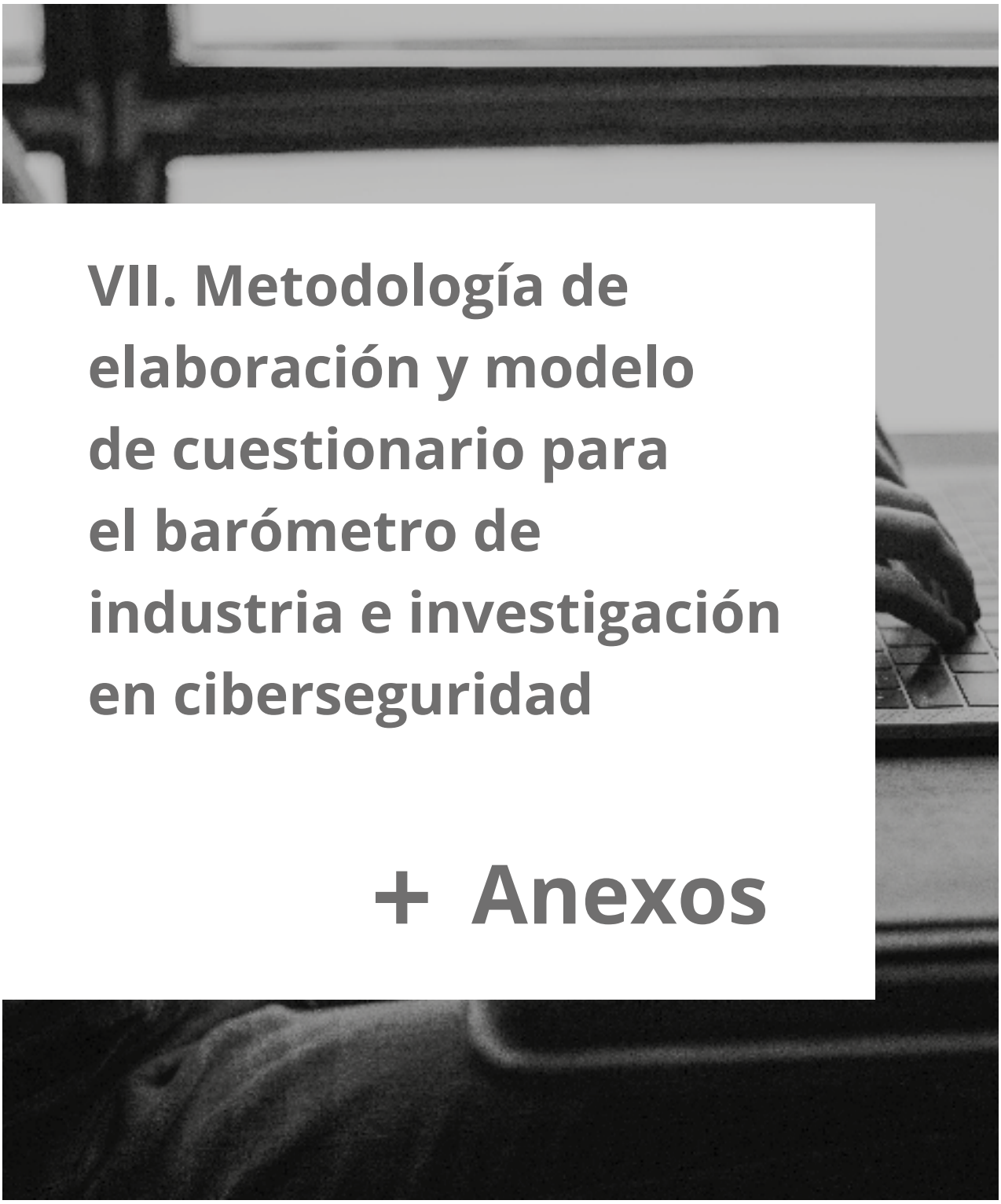
Otros barómetros, como el de la EU Cybersecurity Industry Market Analysis (CIMA) [25], miden el mercado de la ciberseguridad, sus sectores o soluciones, pero no los componentes de investigación.

Algunos informes, como el del sector de las tecnologías de la información del Observatorio Nacional de las Tecnologías y Sociedad de la Información (ONTSI) [76], aportan indicadores económicos de interés sin que aparezcan desglosados para la ciberseguridad, al igual que el Digital Economy and Society Index (DESI) de la UE [24] que dedica capítulos específicos a la I+D+i de las TIC y del programa Horizon 2020, así como a la digitalización de las empresas.

Dentro del panorama nacional, se encuentran indicadores de interés en algunos documentos elaborado por INCIBE como el Catálogo de empresas y soluciones de ciberseguridad [45] o el Catálogo y mapa de conocimiento de la I+D+i en ciberseguridad, junto con las fichas de ciberseguridad del ICEX que contienen información económica sobre terceros países.

El Catálogo de INCIBE ofrece datos sobre los productos y servicios de ciberseguridad que proporcionan las empresas, pero no analiza el impacto económico del ecosistema de ciberseguridad ni de la investigación asociada. Por su parte, el Catálogo y mapa de conocimiento de la I+D+i en ciberseguridad ofrece información sobre las áreas de investigación y la caracterización de los investigadores, sin plantear su impacto económico.

La Red Vasca de Ciencia y Tecnología e Innovación (RVCTI) establece anualmente indicadores para evaluar a sus centros de investigación [83]. Entre ellos figuran las publicaciones científicas indexadas y las de primer cuartil; la solicitud de patentes y los ingresos por ellas; facturación; financiación privada e internacional; investigadores transferidos a empresas o empresas en proyectos internacionales, entre otros.



VII. Metodología de elaboración y modelo de cuestionario para el barómetro de industria e investigación en ciberseguridad

+ Anexos

Metodología de elaboración

Una vez fijados los objetivos, los barómetros precisan contar con bases de datos estadísticos objetivos que se pueden complementar con encuestas y consultas cuando aquellas no lleguen a proporcionar la información necesaria.

INCIBE emplea cuestionarios en el registro de su Catálogo de Empresas y Soluciones de Seguridad y en su Catálogo y mapa de conocimiento de la I+D+i en ciberseguridad. El UKCSA solicita directamente a las compañías sus datos, ingresos, tamaño, sectores, región, exportaciones y ayudas públicas, mientras que el GCI distribuye un cuestionario a los Estados. A partir de las respuestas, se elaboran los indicadores y los grados de madurez que miden el progreso hacia los objetivos.

En relación con la industria y la investigación, la elaboración de un barómetro presenta cierta complejidad por su novedad y la falta de buenas prácticas, por lo que sería recomendable su externalización a un equipo de especialistas, que pueda estar soportado por un entorno de colaboración público-privada como el FNCS.

Esta podría incluir tanto la definición y elaboración de los datos e indicadores necesarios para evaluar la madurez, como la interpretación del estado y tendencias. Algunos barómetros como el UKCSA [89] del Reino Unido externalizan ambas funciones a una entidad independiente, lo que proporciona al Gobierno y al sector una auditoría operativa objetiva.

En el mismo sentido, la Red Vasca RVCTI dispone de un Sistema Integral de Monitorización [42] que complementa la evaluación interna de su Estrategia de Especialización Inteligente, PCTI Euskadi 2020, y de su Informe Innobasque de Innovación con una evaluación externa (Kevin Morgan de la Universidad de Cardiff y el Instituto Vasco de Competitividad, Orkestra).

Este modelo de elaboración es importante tanto por criterios de eficacia en su elaboración como para preservar la necesaria neutralidad entre el medidor y el sujeto de la medición.

En la elaboración del barómetro español sería conveniente considerar la opción de externalizar tanto la identificación de indicadores y cuestionarios como su interpretación y el seguimiento y adaptación de su metodología.

La externalización obviaría la dificultad de elaborar un barómetro base por primera vez y facilitaría la actualización metodológica del barómetro para su seguimiento, evaluación y explotación, por lo que se propone que INCIBE externalice la elaboración del barómetro en colaboración con el ecosistema industrial y de innovación para sus componentes específicos.

Para la elaboración del barómetro, INCIBE debería incluir a representantes de la industria y la investigación en ciberseguridad para asegurar que se tienen en cuenta sus criterios de medición. Se pueden obviar en la localización de datos y elaboración de métricas si se delegan en un actor externo, pero deberán participar en su validación y revisión. También deben participar en la elaboración de los cuestionarios tal y como se indica en el apartado siguiente.

Otro elemento interesante del barómetro es el de su periodicidad. El futuro barómetro debería articularse, al menos parcialmente, sobre una herramienta de medición continua. La ventaja de este modelo es la disponibilidad de información actualizada en todo momento, frente a fórmulas basadas en lecturas puntuales o incluso periódicas.

A pesar de esta ventaja, lo cierto es que no parece realista que todos los indicadores identificados en el apartado 3.1.3 sean susceptibles de ser incluidos en una herramienta de medición continua de este tipo. Probablemente, el barómetro se basará en una combinación de metodologías: medición continua de los indicadores cuya naturaleza así lo permita y medición periódica para el resto de indicadores.

Para una gestión inteligente sería de utilidad disponer de un instrumento de medición continua similar a la herramienta INES [8] del CCN-CERT (Informe de Estado de Seguridad para el ENS), que permita conocer la evolución en menor tiempo, por lo que se recomienda la elaboración de una herramienta de estas características para facilitar la evaluación en tiempo real.

Modelo de cuestionarios

El objetivo es conocer el estado del subsistema de la industria y la investigación de ciberseguridad en España, y facilitar el análisis evolutivo gracias a mediciones periódicas.

La recogida de datos se realizará por medio de cuestionarios dirigidos a los diferentes actores descritos en la cadena de valor (ver Figura 5).

Idealmente, se utilizará una herramienta automatizada y amigable, y será contrastada por el propietario del barómetro y por organismos independientes bajo un modelo de colaboración público-privada como el FNCS.

El trabajo se estructura en seis fases:

· **Fase 1**. Definición de los datos necesarios y del modelo de cuestionario para cada entidad de la cadena de valor. Selección del medio de recogida de información y el formato de los cuestionarios para facilitar su usabilidad.

· **Fase 2**. Diseño e implementación del cuestionario y el modelo de datos en la plataforma de acuerdo al sistema de encuestación definido en la fase anterior.

· **Fase 3**. Envío del cuestionario, recopilación de los datos y almacenamiento para su análisis.

· **Fase 4**. Análisis cuantitativo y cualitativo de los resultados obtenidos, comparación con los resultados obtenidos en años anteriores y definición de acciones a adoptar.

· **Fase 5**. Publicación de los datos a través del medio o medios identificados y por parte del agente encargado de la creación y mantenimiento del barómetro.

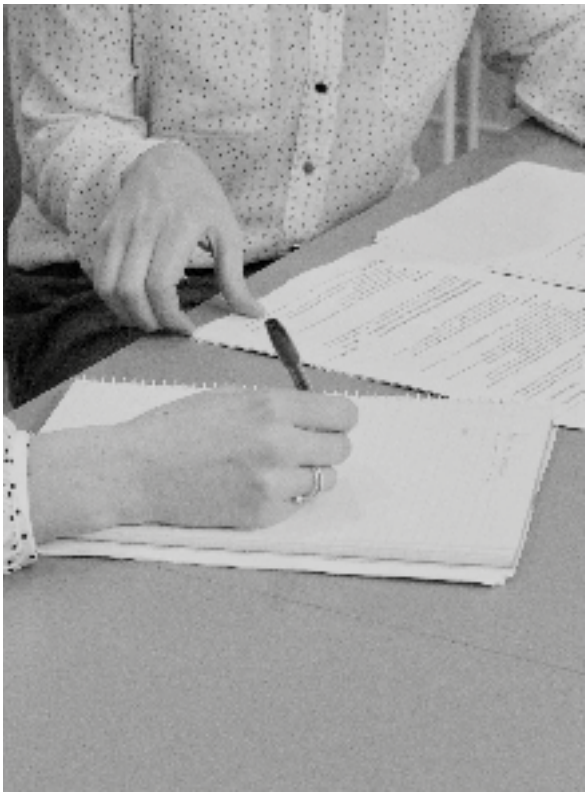
· **Fase 6**. Revisión de los cuestionarios e incorporación de mejoras.

En la lectura inicial (T0) deberá realizarse el ciclo completo con objeto de definir los datos de partida con los que trabajar, mientras que en las lecturas sucesivas será suficiente con aplicar las fases 3 a 6. Se recomienda una frecuencia de actualización anual.

Deberá identificarse qué entidad a nivel nacional será la encargada de la definición de los cuestionarios y de la gestión del proceso.

Se sugiere un cuestionario que, siguiendo la cadena de valor, la taxonomía y los indicadores KPIs definidos, pueda obtener los datos necesarios para el barómetro. Se propone a continuación un planteamiento del cuestionario, que no constituye una lista exhaustiva, sino una primera aproximación.

El cuestionario permitiría asimismo incorporar preguntas relacionadas con talento, cultura de ciberseguridad o cualquier otro parámetro que resulte interesante estudiar.



Datos generales de la entidad (Quién):

· **Identificación de la entidad y datos de contacto**.

· **Posicionamiento en la cadena de valor:**
- · Prescripción
- · Investigación
- · Oferta
- · Demanda

· **Categoría dentro de la cadena de valor**:
- · Decisor
- · Facilitador
- · Conocedor
- · Desarrollador
- · Apoyo
- · Cliente
- · Otro

· **Subcategoría:**
- · Administración pública
- · Entidad de estandarización y certificación
- · *Think-Tank*
- · Asociación, *clusters* o *hubs* de Ciberseguridad
- · *European Digital Innovation Hubs*
- · Universidad
- · Centro Tecnológicos y de Investigación I+D+i
- · Empresas fabricante
- · Empresas integradora
- · Empresa consultora
- · Empresa mayoristas o distribuidora
- · *Startup*
- · Incubadora
- · Entidad Financiadora de Proyectos
- · Medio de comunicación
- · CSIRTs
- · Ciudadano

· **Ámbito de actuación:**
- · Mundial
- · Europeo
- · Nacional
- · Autonómico
- · Local

· **Tipo de entidad:**
  · Público
  · Privado
  · Público-privado

Área de trabajo de la entidad, siguiendo la taxonomía propuesta (Qué):

· **Universidades y Centros Tecnológicos y de Investigación I+D+i:** se mapearán respecto a la taxonomía JRC (columna primaria y, en caso de ser necesario, columna secundaria).

· **Empresas (fabricantes, integradoras, consultoras, mayoristas o distribuidoras) y *start-ups*:** se mapearán respecto a la taxonomía ECSO.

· Ambas subcategorías de actores **se mapearán contra los casos de uso de la taxonomía JRC**:
  · Artificial Intelligence & Big Data Analytics
  · Blockchain and Distributed Ledger Technology (DLT)
  · Cloud
  · Edge and Virtualization
  · Critical Infrastructures
  · Hardware Technology
  · High Performance Computing
  · Human Machine Interface
  · Industrial Control Systems
  · Internet of Things
  · Embedded Systems
  · Pervasive Systems
  · Quantum Technologies
  · Vehicular Systems

Cómo y cuánto:

· **Universidades y Centros Tecnológicos y de Investigación I+D+i:**
  · Número de investigadores
  · Publicaciones realizadas en el último año
  · Proyectos de I+D+i:
    · Ámbito: regional, nacional, europeo
    · Título
    · Programa
    · Duración
    · Presupuesto
  · Proyectos de transferencia a empresas

· **Empresas (fabricantes, integradoras, consultoras, mayoristas o distribuidoras) y *start-ups*:**
  · Número de personas trabajando en ciberseguridad
  · Incremento de trabajadores en ciberseguridad
  · Ingresos anuales obtenidos en el último año
  · Inversiones realizadas
  · Proyectos de I+D+i:
    · Ámbito: regional, nacional, europeo
    · Título
    · Programa
    · Duración
    · Presupuesto

A modo de prueba de concepto, se propone utilizar a las entidades que forman parte del FNCS para que utilicen el modelo de catálogo de actores, taxonomía de competencias y cuestionarios iniciales para verificar la validez del modelo propuesto y participen en un piloto que complete las cuatro primeras fases del proceso.

VIII. El contexto de la colaboración público-privada en ciberseguridad

+ Anexos

Hay que diferenciar entre la CPP genérica dentro de la ciberseguridad y la CPP asociada a sus aspectos industriales y de investigación. La primera ha tenido un laboratorio de experimentación en el ámbito de las infraestructuras críticas, donde ha consolidado un modelo de colaboración.

Posteriormente, desde que la Directiva NIS [16] ampliara el ámbito de la CPP desde la seguridad hacia la economía, la colaboración se ha resentido de las diferencias de intereses. Para remediarlo, la ENCS incluyó la creación del Foro Nacional de Ciberseguridad, cuya puesta en marcha coincide con los trabajos del Grupo de Trabajo «Impulso a la industria y a la I+D+i en ciberseguridad», encargado de la elaboración de este Informe.

La constitución del Foro Nacional de Ciberseguridad ha servido para impulsar el desarrollo de las medidas de colaboración público-privada de la ENCS en materia de industria e investigación, y para debatir y articular mecanismos de cooperación como el EI2C. En la Tabla 9 se resumen las carencias, objetivos y medidas de la colaboración público-privada en ámbitos ligados a aspectos económicos, industriales y de investigación.

Carencias	Objetivos	Medidas
Debilidad pre y post COVID-19 de la colaboración público-privada.	Reforzar la colaboración público-privada aprovechando la actualización de los planes de industria e investigación [67] [58][62][62].	Implantar un ecosistema de ciberseguridad público-privado a nivel nacional especializado en industria e investigación (EI2C).
Indefinición del sistema de ciencia, tecnología e innovación en el ámbito de ciberseguridad.	Aprovechar el impulso de la Estrategia Española de Ciencia y Tecnología (EECTI 2021-2027) [61] para consolidar y reforzar el EI2C en el ámbito de la ciberseguridad.	Lanzamiento de una línea estratégica sobre seguridad civil para la sociedad en materia de ciberseguridad[8].
Fragmentación de los programas de investigación e I+D+i.	Incrementar la autonomía tecnológica e industrial.	Crear un programa nacional de investigación e innovación específico para el sector de la ciberseguridad[9] con una agenda estratégica de investigación[10].
	Coordinar las prioridades públicas y privadas.	
	Coordinar los programas públicos y privados.	

[8] Incluye comunicaciones cuánticas, criptografía cuántica, cifrado post cuántico, nuevas tecnologías para la evaluación y gestión de riesgos, biometría, privacidad y aspectos éticos en ciberseguridad y control digital, gobierno del dato, modelos zero trust, ingeniería de software seguro, ciberseguridad en entornos industriales y en infraestructuras y servicios críticos, sistemas para la detección, predicción y atribución frente a ciberataques.

[9] Como programas de I+D+i e iniciativas público-privadas en otros países se han analizado el programa KIRAS Security Research del gobierno austriaco o el RCUK Global Uncertainties Programme del gobierno británico.

[10] Como ejemplo, la Agenda de Investigación Nacional en Ciberseguridad (NCSRA) de los Países Bajos.

Carencias	Objetivos	Medidas
Insuficiencia de los instrumentos de inversión públicos y privados [61].	Disponer de un presupuesto propio para asegurar la tracción industrial y de I+D+i.	Crear un presupuesto nacional de ciberseguridad [73].
	Crear nuevos instrumentos que faciliten la inversión.	Revisar y ampliar los instrumentos fiscales y de inversión (incluidos los de la UE).
	Priorizar las subvenciones frente a los créditos, ya que estos no funcionan como motor de inversión.	Crear inversiones de riesgo para programas estratégicos y dotar de subvenciones al programa específico.
Insuficiencia de los instrumentos regulatorios.	Progresar hacia una cooperación proactiva e inclusiva.	Crear un método de coordinación regulatoria entre los sectores público y privado.
Dispersión de instrumentos de apoyo a las cadenas de suministro (*start-ups*, pymes, clústeres).	Apoyo a la escala, internacionalización e integración en cadenas globales de suministro.	Integración de los instrumentos locales, nacionales y europeos.
Carencia de instrumentos de retención, captación y promoción de talento (centros y redes de excelencia).	Crear entornos atractivos de investigación.	Desarrollar mecanismos e incentivos públicos y privados de estabilización de los centros y redes industriales, tecnológicas y de I+D+i.

Tabla 9: Carencias, objetivos y medidas de la colaboración público-privada (CPP)

En la Tabla 10 se incluyen las medidas de la Línea de Acción 5 de la ENCS de 2019 y su nivel de desarrollo.

	Medidas	Desarrollo
LA 5 M1	Impulsar programas de apoyo a la I+D+i, facilitar el acceso a programas nacionales e internacionales y de compra pública innovadora.	Parcial
LA5 M2	Dinamizar el sector industrial y de servicios, incentivando las medidas de apoyo a la innovación, inversión, internacionalización y trasferencia tecnológica, sobre todo pymes y micropymes.	Pendiente
LA5 M3	Incrementar las actividades nacionales para desarrollo de productos y servicios seguros desde el diseño, de interés para la seguridad nacional y para fortalecer la autonomía digital y la propiedad intelectual.	Pendiente
LA5 M4	Promover normalización y exigencia de requisitos de ciberseguridad, fomentando la evaluación, certificación y catalogación.	Parcial
LA5 M5	Actualizar marcos de competencias que respondan a las necesidades del mercado laboral.	Pendiente
LA5 M6	Identificar necesidades de capacidades profesionales y fomentar la educación, acreditación y certificación profesional.	Parcial
LA5 M7	Incluir perfiles profesionales de ciberseguridad en el sector público.	Pendiente
LA5 M8	Detectar, fomentar y retener el talento.	Pendiente
LA5 M9	Impulsar programas específicos de I+D+i.	Pendiente

Tabla 10: Nivel de desarrollo de las medidas de la Línea de Acción 5 de la ENCS

IX. Ejemplo de buena práctica de integración vertical: El ecosistema industrial y tecnológico de la defensa europea

+ Anexos

La demanda industrial o tecnológica se establece desde los órganos de planeamiento europeos (Estrategia Industrial Europea, Horizonte Europa). También se identifican las prioridades de investigación y desarrollo (Fondo Europeo de Defensa, PESCO), las prioridades tecnológicas (CAPTECHS) y las necesidades militares (Agencia Europea de Defensa).

Los Estados miembros participan en el proceso, y tienen más influencia aquellos países que tienen mejor coordinada la definición de prioridades y la estrategia de influencia para incluirlas en las prioridades colectivas.

Figura 11: Integración vertical del ecosistema industrial y tecnológico de defensa

La integración en el nivel de los Estados miembros tiene en cuenta los marcos anteriores tanto para participar en ellos (interés colectivo) como para desarrollar de manera individual las necesidades no atendidas (interés nacional).

Se replica la integración de las necesidades y objetivos de defensa en el marco general de las políticas industriales y tecnológicas del país. Para ello se identifican las necesidades de tecnología y capacidades para la defensa, la oferta industrial y tecnológica disponible, y se establecen programas para satisfacerlas mediante consorcios europeos o nacionales, según los casos.

La integración favorece a los países que coordinan los intereses industriales y tecnológicos de la defensa con la del resto de los sectores, y penaliza a los que mantienen una base industrial y tecnológica de defensa autárquica.

X. Contexto y antecedentes de la I+D+i en ciberseguridad en España

+ Anexos

Contexto actual en la Universidad

El sistema universitario de educación superior en España está constituido por 76 universidades: 50 públicas y 26 privadas. En todas ellas se realiza una labor docente, de investigación y de transferencia de conocimiento tanto al sector productivo como a la sociedad.

Docencia

En lo que respecta a la parte docente, los profesores se agrupan en departamentos con una o varias áreas de conocimiento. Por su parte, en la labor de investigación y transferencia, se conforman Grupos de Investigación alrededor de una o varias líneas temáticas de interés común para todos los profesores e investigadores que forman parte de los mismos.

Las universidades españolas están empezando a ofrecer los primeros Grados en ciberseguridad, tres hasta la fecha, mientras que el número de másteres con algún contenido en ciberseguridad asciende a setenta y dos [51].

Sin embargo, en los estudios de Formación profesional y en los Grados de perfil generalista (Ingeniería en Informática y en Telecomunicaciones, por poner dos ejemplos) la enseñanza de ciberseguridad se considera escasa y no siempre orientada al mundo empresarial. La formación en inglés es prácticamente inexistente en estos niveles docentes.

Por su parte, los Doctores con tesis doctorales orientadas a ciberseguridad son apenas una veintena al año en todo el país, y suelen contar con baja empleabilidad a nivel de industria, lo que reduce el atractivo de esta opción.

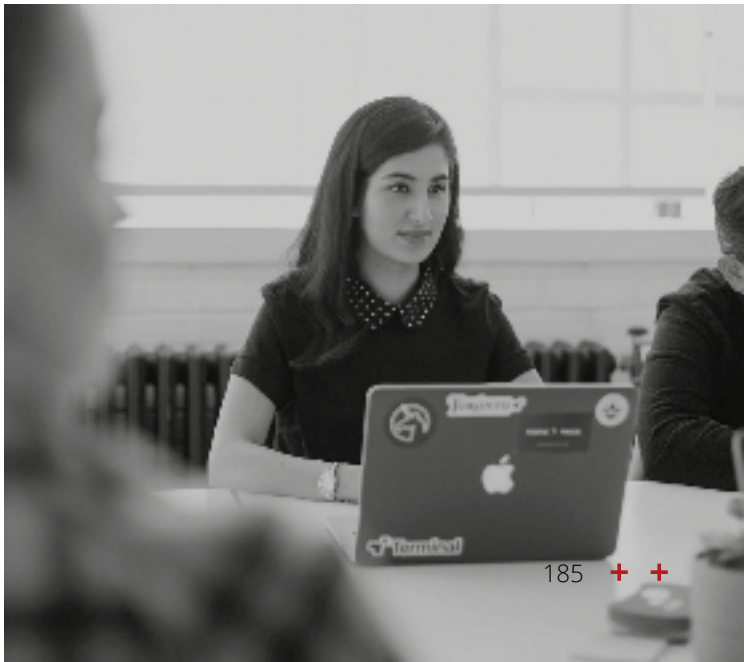
Investigación

En cuanto a la investigación, si bien son múltiples los Grupos de Investigación que se dedican parcial o totalmente a la ciberseguridad en las universidades españolas, muy pocos pueden considerar como grupos de excelencia. Tomando como indicador RENIC, solo doce universidades (once públicas y una privada) cuentan con al menos un Grupo de Investigación en ciberseguridad con excelencia acreditada [85].

Esto limita la participación internacional en convocatorias competitivas como H2020 u Horizon Europe, limitando a unos pocos grupos los que tienen proyectos en estas convocatorias y a solo dos los que participan en alguno de los cuatro proyectos piloto de ciberseguridad en Europa [30].

Una primera revisión de la situación actual permite concluir que las fuentes de financiación específicas para la investigación en ciberseguridad resultan insuficientes. A esto se unen la escasez de incentivos a los profesores universitarios y la falta de mecanismos apropiados de colaboración entre distintos grupos de investigación.

El resultado es que, a diferencia de lo que sucede en los países europeos punteros en ciberseguridad, el punto de partida para el desarrollo de un tejido fuerte de I+D+i en las universidades españolas dista mucho de ser el adecuado.



Transferencia

La situación de la transferencia de conocimiento en la universidad española no ofrece una imagen más esperanzadora que docencia e investigación en ciberseguridad.

Se observa una escasez de foros de encuentro universidad-empresa relacionados directamente con la ciberseguridad, y un insuficiente número de patentes y registros software en esta temática que luego se puedan transferir mediante licenciamiento al sector productivo nacional.

Esto viene motivado en parte por la escasa visión empresarial que tienen los investigadores y los profesores de universidad, y por los limitados programas de fomento de la transferencia que ha sido, de largo, la faceta más olvidada de la universidad en España.

Contexto actual en los Centros Tecnológicos

Los centros tecnológicos (CCTT) son organismos de investigación y difusión de carácter privado que tienen como misión la dinamización del ecosistema I+D+i. Su investigación tiene un marcado carácter tecnológico, está orientado al mercado y fomenta la colaboración público-privada.

A nivel nacional existe un conjunto destacado de CCTT que desde hace años desarrollan actividades de I+D+i en el campo de la ciberseguridad. Entre los más destacados por su capacidad de transferencia, su participación relevante en proyectos europeos y nacionales, y su pertenencia a asociaciones sectoriales representativas (como ECSO, RENIC, AEI Ciberseguridad o CYBASQUE) se encuentran los siguientes (orden alfabético): CEIT, EURECAT, FIDESOL, GRADIANT, I2CAT, IKERLAN, ITCL, TECNALIA y VICOMTECH.

La I+D+i en ciberseguridad de los centros tecnológicos está fragmentada en la práctica y dispersa a nivel nacional. Si bien la mayor parte de estos centros opera a nivel regional, nacional e internacional, en cada uno de estos ámbitos existen diferencias importantes.

A nivel regional, en aquellas Comunidades Autónomas donde existen varios centros relevantes existe una mayor cohesión. En estos casos, entre los que destaca el País Vasco, se evita la fragmentación de la I+D+i en ciberseguridad, se obtiene una mayor colaboración público-privada y transferencia a empresas.

En el plano internacional (principalmente en el ámbito europeo), el nivel de colaboración es menor, por la dificultad de encontrar financiación conjunta. Un ejemplo es el recientemente finalizado programa H2020.

Es a nivel nacional donde la cohesión es menor y se produce mayor fragmentación. En 2019, el CDTI

creó un programa a nivel nacional para aumentar la colaboración de centros tecnológicos, denominado CERVERA. Dicho programa no garantiza la financiación de la ciberseguridad y en la práctica penaliza a los centros tecnológicos grandes (como EURECAT o TECNALIA), al no permitir que un centro opte a más de tres proyectos.

La fragmentación se ve agravada por la falta de programas nacionales que fomenten la colaboración entre universidades y centros tecnológicos en los proyectos I+D+i en ciberseguridad. Ciertas líneas de investigación en ciberseguridad de los CCTT han alcanzado un nivel de madurez adecuado. Sin embargo, su adopción por las empresas no está siguiendo el ritmo esperado. Se necesita un enfoque eficaz que vincule la investigación en los centros con la industria, con el objetivo de aumentar la transferencia.

En la actualidad, se han creado asociaciones que incorporan diferentes agentes, incluidos centros tecnológicos, que funcionan como pieza clave para el alineamiento de las actividades de Ciberseguridad. Algunos ejemplos son CYBASQUE, CIBER.GAL o el Clúster de ciberseguridad en Madrid. Se trata, en su mayoría, de asociaciones de ámbito regional y, de nuevo, producen fragmentación.

Es necesario establecer iniciativas de financiación a nivel nacional (un ejemplo es BDIH Konexio 2020 en el País Vasco) que fomenten la transferencia tecnológica en el campo de la ciberseguridad. Igualmente, sería interesante potenciar iniciativas de Compra Pública Innovadora en Ciberseguridad desde el sector público nacional y autonómico, que fomenten la colaboración entre centros tecnológicos y empresas.

En la actualidad existe una falta de coordinación a nivel europeo desde los centros tecnológicos nacionales. Iniciativas que fomenten la cohesión a nivel nacional beneficiarían sin duda una mayor coordinación a nivel europeo. Este aspecto es clave de cara a la creación del Centro de Competencias de Ciberseguridad.

La colaboración efectiva entre los centros tecnológicos a nivel nacional, de la mano de INCIBE como centro espejo, será fundamental para un mejor posicionamiento de las actividades de I+D+i nacionales a nivel europeo.

Otro aspecto a mejorar es la definición de las actividades de I+D+i en ciberseguridad. Los distintos enfoques en taxonomías de ciberseguridad y su fragmentación dificulta la coordinación efectiva entre los centros.

Los CCTT tienen dificultades para captar talento por la gran demanda de profesionales del sector TIC en general y ciberseguridad en particular. Una generación de profesionales de ciberseguridad centrados en la I+D+i es clave para poder afrontar las oportunidades presentes y futuras. Para ello es necesaria la estabilidad, de forma que estos profesionales puedan ver la I+D+i como una carrera a largo plazo.

Igualmente, es necesario mejorar las capacidades profesionales, así como la sensibilización y concienciación de los estudios de ciberseguridad en etapas tempranas y entre el alumnado femenino. Se necesita caracterizar la formación existente en ciberseguridad y alinearla con la demanda, además de enriquecer los programas curriculares en competencias de ciberseguridad.

Contexto actual en la empresa

La digitalización constante y acelerada de nuestra sociedad conlleva de manera inevitable la necesidad de incrementar e incorporar servicios y soluciones de ciberseguridad (oferta) que garanticen el cumplimiento de medidas (marcos normativos) para dar respuesta a las necesidades de los sectores públicos y privados nacionales (demanda).

A pesar de la situación provocada por la escalada continua de los ciberincidentes, la demanda de soluciones y servicios de ciberseguridad es proporcionalmente baja en nuestro país como consecuencia de la falta de percepción del riesgo digital en una parte de la sociedad.

La oferta de servicios de ciberseguridad es amplia y creciente, y es patente la necesidad de invertir de forma continuada en la generación de talento que asegure las necesidades de personal cualificado para dar respuesta a las necesidades del mercado. La prestación de estos servicios se basa principalmente en soluciones de seguridad por empresas extranjeras o en desarrollos propios que resuelven aspectos concretos.

La oferta nacional de soluciones de ciberseguridad es reducida con respecto a la amplitud de aspectos a cubrir por su especialización, tal como muestra ECSO Radar [34]. Se trata de una opción muy poco conocida por la demanda nacional pública y privada, y en desventaja frente a fabricantes extranjeros con posicionamientos consolidados de marca y fuertes capacidades de inversión.

Por tanto, se hace necesario formalizar, fomentar y divulgar la oferta nacional de ciberseguridad con mayor énfasis y favorecer su adopción por los prestadores de servicios y las entidades públicas y privadas.

La industria nacional de ciberseguridad no invierte suficiente en el desarrollo de una tecnología propia que proporcione cierta independencia tecnológica al carecer de incentivos para ello:

· El mercado está copado de ofertas agresivas de tecnologías extranjeras, principalmente americanas.

· No se fomenta, ni en el ámbito público ni en el privado, el uso de tecnología nacional.

· No se dispone de instrumentos potentes de apoyo a medio o largo plazo para la inversión en tecnología propia.

· Cuando una empresa decide invertir en el desarrollo de tecnología propia, además de tener que competir en un mercado con peores herramientas, sus activos intangibles no son valorados de forma adecuada en comparación con otro tipo de activos tangibles de otras compañías.

Como consecuencia, la inversión base en proyectos de I+D+i en universidades y centros tecnológicos españoles, que deberían ser usados en gran parte por las empresas de ciberseguridad españolas o europeas, acaban siendo utilizados por compañías multinacionales, principalmente estadounidenses, con alta capacidad de inversión y riesgo. De esta forma, la industria nacional se centra principalmente en los servicios, y no en el producto.

Se hace necesario formalizar, fomentar y divulgar las soluciones de seguridad nacionales con mayor énfasis, y favorecer su adopción tanto por los prestadores de servicio como por entidades públicas y privadas.

Igualmente, es preciso crear herramientas de apoyo adecuadas que permitan diseñar, desarrollar y explotar estas soluciones. Como ejemplo de este tipo de herramientas cabe citar, en el ámbito público, el uso de instrumentos como la compra pública innovadora para que pueda traccionar la industria nacional de productos de ciberseguridad.

Del mismo modo, la industria nacional y su cadena de valor debe ser articulada, cohesionada y alineada a los propósitos de la ENCS. Los instrumentos públicos de financiación deben guiarse por criterios de especialización, viabilidad, oportunidad y escalabilidad.

Esta orientación persigue mejorar en la supervisión y seguimiento de resultados del emprendimiento e innovación, además de incrementar y potenciar el efecto inversión en la creación de talento y de soluciones en las empresas nacionales (principalmente en pymes, micropymes, empresas de base tecnológica – EBT – y *start-ups*).

El conocimiento y experiencia que se genera en investigación nacional en ciberseguridad desde los CCTT y universidades es conocido, aunque poco usado por la industria nacional desde una aproximación individual. En tanto en cuanto se alineen las necesidades de la demanda con las capacidades de la cadena de valor de la ciberseguridad nacional (CCTT, universidades, empresas, servicios y soluciones), se podrán diseñar mejores programas de financiación, fomento de la innovación y consumo de la industria nacional a través de retos transversales dirigidos a la demanda.

Proteger, poner en valor y promocionar el conocimiento generado a nivel nacional y potenciar su crecimiento en España, Europa y Latinoamérica, permitirá formalizar una industria nacional de ciberseguridad capaz y creciente para abordar los desafíos a los que debe enfrentarse la sociedad digital.

XI. Análisis DAFO y CAME de la I+D+i en ciberseguridad en España

+ Anexos

Análisis DAFO

DAFO. Perspectiva de las ideas	
Debilidades	**Fortalezas**
• Escasez de oferta de productos de ciberseguridad con tecnología española. • Escasez de patentes de ciberseguridad y de licenciamiento. • Muy limitadas iniciativas público-privadas • Insuficiente transferencia tecnológica de universidades y centros tecnológicos a la industria española. • Las principales tecnologías de ciberseguridad exitosas son proporcionadas por empresas no españolas, principalmente estadounidenses o israelíes. • El concepto de Industria 4.0, íntimamente ligado a la ciberseguridad, no está completamente maduro. • Fragmentación de la oferta que cubre parcialmente los desafíos. • Déficit de conocimiento de los retos de los sectores de actividad económica que conforman el mercado. • Déficit de agentes transversales independientes (clústeres, asociaciones). • Ausencia de un modelo transversal de apoyo, de supervisión y de seguimiento de resultados para el emprendimiento y la innovación, guiados por criterios de especialización, viabilidad, oportunidad y escalabilidad.	• Ecosistema de ciberseguridad bastante completo que cubre todos los servicios asociados a la cadena de valor. • Número de empresas oferentes de servicios de ciberseguridad. • Espíritu emprendedor consolidado y número de start-ups en ciberseguridad alrededor de ciertos nodos de concentración regionales. • Crecimiento de actores relevantes en ciberseguridad: start-ups, pymes y grandes empresas. • Programas de fomento de creación de empresas de base tecnológica (EBT) en las universidades. • Experiencia en ciberseguridad de algunos Centros de Investigación de Excelencia (IMDEA, BCAM), así como de universidades y centros tecnológicos.
Amenazas	**Oportunidades**
• Falta de anticipación a la evolución de la demanda y de las ciberamenazas. • Dificultad para la internacionalización por la alta competencia. • Competencia de otros países europeos que invierten y potencian su industria (Estonia como ejemplo) • Fuga de datos a través de los unicornios americanos y chinos. Perfilado masivo de la población por potencias no europeas. • Legislación actual que impide establecer mecanismos de compra pública para favorecer la adopción temprana de la industria local emergente innovadora.	• Soluciones para la pyme. • Especialización de la ciberseguridad en Europa. • Re-industrialización europea en diferentes sectores y en constante evolución. • Emprendedores en serie con éxito previo contrastado. • Ciberseguridad de nuevas tecnologías como IA, 5G, 6G, Cuántica, IIoT.

Tabla 11: DAFO desde la perspectiva de las ideas

DAFO. Perspectiva del talento	
Debilidades	**Fortalezas**
• Déficit de talento investigador especialista en ciberseguridad. • Falta de presencia de la mujer. • Insuficiente visión empresarial por parte de los investigadores. Falta de dominio del mercado de ciberseguridad. • Baja tasa de incorporación de doctores como profesores en universidades, centros tecnológicos y menor aún en empresas. • Falta de formación específica en ciberseguridad dentro de los grados universitarios y FP. • Escasez de grupos de investigación potentes (12-15), sobre una base de 84 universidades (datos de 2019). • Amplias zonas geográficas sin grupos de investigación de una cierta entidad y presencia en la comunidad. • Falta de reconocimiento a la figura del Doctor por la industria. • Pensamiento computacional muy débil en la sociedad española. • Falta de calidad de la oferta educativa en inglés.	• Buena base investigadora en ciberseguridad. • Existencia de algunos Grados y Másteres de Ciberseguridad. • Diversidad de grupos de investigación en Universidades y Centros Tecnológicos. • Algunos doctores con buenos conocimientos para dirigir proyectos de investigación e innovación industrial. • Acceso casi universal a formación universitaria o formación profesional de calidad. • Altos niveles de calidad de vida (clima, gastronomía, renta disponible).
Amenazas	**Oportunidades**
• Fuga / Diáspora de Talento formado y pagado por el sistema educativo español porque no se invierte en I+D+i ni se pagan salarios adecuados. • Desplazamiento de alumnos hacia otras áreas TIC con mayor visibilidad temporal/circunstancial. • Dificultad para atraer y retener talento.	• Formación continua masiva en pensamiento computacional. • Aumento de personas desempleadas o con futuro incierto post-COVID que presenten perfiles reutilizables. • Programa de doctorados industriales. • Demografía y crecimiento universitario de países hispanohablantes (LATAM). • Educar en ciberseguridad desde la infancia.

Tabla 12: DAFO desde la perspectiva del talento

DAFO. Perspectiva de la inversión	
Debilidades	**Fortalezas**
• Fuentes de financiación para la investigación en ciberseguridad insuficientes. Dato general: España ha invertido el 1,25% del PIB en I+D+i. • Pobres esquemas de financiación pública de la I+D+i (<30%) frente a esquemas como Reino Unido, EEUU o Suecia. • Ausencia o escasez de incentivos a los profesores universitarios y a doctorandos. • Falta de fondos para incentivar la colaboración entre múltiples grupos de investigación en convocatorias nacionales e internacionales. • No se valoran adecuadamente los activos intangibles (propiedad intelectual). • Dificultad para financiar la inversión de la I+D+i en la industria a no ser que sea a través de subvenciones. • Exigencia de avales por duraciones excesivas. • Déficit en la protección de la tecnología española frente a inversores extranjeros o no europeos.	• Potencial del mercado local en sectores PIC y NIS: energía, fabricación, transporte, financiero, TIC, salud, alimentación. • Gobierno sensible hacia la ciberseguridad. • Regulaciones potenciadas desde Europa. • Existencia de mecanismos de compra como la Compra Pública Innovadora. • Infraestructura tecnológica de base.
Amenazas	**Oportunidades**
• Competición interna por los recursos financieros. • Dependencia de la microelectrónica realizada fuera de España y de Europa. Lo mismo ligado a tecnologías digitales y de telecomunicaciones de uso masivo. • Adquisición por parte de capitales externos de las iniciativas de emprendimiento ligadas a actividades de I+D+i españolas. • El crecimiento y las grandes inversiones que se están realizando en tecnologías de ciberseguridad no europeas. • Adopción lenta de la ciberseguridad por parte del mercado nacional. • Falta de inversión pública de grupos de investigación. • Impacto del Brexit potenciado por el posicionamiento de Reino Unido en los rankings globales (2º del mundo en el Global Cybersecurity Index de 2020 de ITU). • Mayor velocidad de creación de ecosistemas fuera de España (Irlanda, Israel, Estonia). • Regulación inapropiada que puede frenar el desarrollo de actividades de I+D+i frente a otras regiones del mundo con una legislación mucho más laxa.	• Contribución para acelerar el fortalecimiento del mercado digital europeo. • EU Cybersecurity Act. • Latinoamérica como mercado de expansión • Mercado nacional voluminoso con capacidad tractora, 4ª mayor economía de la UE. • Necesidad creciente de protección debido al incremento de los ciberataques, cada vez más sofisticados y con un coste cada vez mayor para quien lo sufre. • Nuevo programa marco europeo Horizonte Europa y Europa Digital. Plan europeo para el desarrollo real de una Economía Digital. • Estrategia Nacional de Ciberseguridad. • Uso de herramientas de financiación a la I+D+i. • Relevancia transversal de la ciberseguridad tanto a nivel industrial como público y social. • Utilizar “campeones nacionales” para potenciar las inversiones y generar tracción en PYMES

Tabla 13: DAFO desde la perspectiva de la inversión

DAFO. Perspectiva de las relaciones	
Debilidades	**Fortalezas**
• Fragmentación investigadora. Falta de cohesión en el sector a lo largo de la cadena de valor de ciberseguridad entre Universidades, CCTT y empresas, principalmente a nivel estatal (funciona mejor a nivel autonómico). • Falta de imagen y conciencia de marca. • Desconocimiento del posicionamiento frente a posibles competidores. • Falta de conocimiento y reconocimiento nacional de pymes y start-ups de base tecnológica en ciberseguridad. • Escasa proyección internacional de grupos de investigación en convocatorias competitivas (H2020). • Falta de conocimiento profundo y espacios de diálogo con otros ecosistemas investigadores internacionales de referencia. • Criterios de medición de la excelencia en la investigación en España, basado en publicaciones de impacto en WoS (Web of Science). • Falta de madurez y recursos en la colaboración desde las start-ups con la comunidad investigadora de universidades y centros tecnológicos. • Minifundismo digital europeo. • Escasez de foros de encuentro universidad-empresa relacionados con la ciberseguridad.	• Importantes esfuerzos en sensibilizar hacia la ciberseguridad a ciudadanos y empresas. • Existencia de algunas asociaciones de ciberseguridad de ámbito parcial, tanto industriales como de I+D+i (por ejemplo, RENIC). • Cohesión del sector en determinadas regiones. • Existencia de una política de clústeres consolidada en algunos sectores y en algunas regiones. • Buen posicionamiento de alguna región en foros globales de alta especialización. • Empresas tecnológicas con reconocimiento en el mercado nacional. • Alto impacto en las publicaciones conseguidas. • Buen posicionamiento de algunos agentes (gubernamentales, investigadores, industriales y start-ups) a nivel europeo. • País pionero en la regulación gubernamental (Ley PIC, ENS) posicionado el 2º de la Unión Europea (y 4º global) en la 4ª edición del Global Cybersecurity Index (GCI) de ITU publicado en 2020. • Experiencia en el liderazgo de proyectos de colaboración público-privada.
Amenazas	**Oportunidades**
• Pérdida de sinergia causada por duplicidad de esfuerzos. • Bajo posicionamiento de las empresas tecnológicas nacionales especializadas frente fabricantes extranjeros asentados. • Representatividad a nivel europeo con la próxima constitución del Centro Europeo de Competencias en Ciberseguridad. • Mejor posicionamiento en *rankings* internacionales y cantidad de universidades en otros países competidores como amenaza en términos de competir por talento e ideas. • Vinculación de la estrategia y de las relaciones público-privadas a ciclos legislativos.	• Creación del futuro Centro Espejo. • Sector en crecimiento y mercado público-privado inmaduro en adopción de la tecnología y servicios en empresas y organismos. • Cooperación internacional. • Posicionamiento actual de liderazgo de algunas regiones en nichos de especialización. • Dinámicas de colaboración público-privada. • Proyectos Faro Europeos de Ciberseguridad.

Tabla 14: DAFO desde la perspectiva de las relaciones

Análisis CAME

CAME. Perspectiva de las ideas	
Corregir (debilidades)	**Mantener (fortalezas)**
• Creación de espacios de trabajo entre Universidades, CCTT y empresas para identificar líneas de trabajo. • Crear modelos jurídicos que den soporte a la posibilidad de patentar software como sí se puede hacer fuera de Europa. • Apostar por la I+D+i en productos y soluciones que reduzcan la dependencia tecnológica europea. • Potenciar la tecnología nacional y la colaboración investigadora/empresa para proteger la supervivencia y mejorar la competitividad de los agentes productivos. • Promover y reforzar la cooperación entre competidores para generar soluciones innovadoras más completas fruto de la cooperación y la diversidad. • Crear mapas de demanda industrial por sectores donde se pueda conocer mejor la demanda y que la I+D+i pueda orientarse a ella de manera anticipada. • Promover y reforzar la cooperación entre competidores para generar soluciones innovadoras más completas fruto de la cooperación y la diversidad. Potenciar la cadena de suministro • Crear una capacidad de *Venture building* transversal que actúe como mecanismo de filtrado y que guíe la canalización de ayudas para *start-ups*.	• Apostar por la I+D+i en productos y soluciones que reduzcan la dependencia tecnológica europea (extranjera). • Crear un mapa de capacidades de I+D+i y emprendimiento identificando los hubs donde se produce concentración y especialización. • Estudiar si es conveniente promover la consolidación del sector ciber en agentes de mayor tamaño. • Extender los casos de éxito a otros Centros de Investigación.
Afrontar (amenazas)	**Explotar (oportunidades)**
• Mejorar el posicionamiento de marca y crear un Plan de Marketing para enfatizar los diferenciadores. • Estudiar si la ciberseguridad puede necesitar unos mecanismos de compra basados en criterios de seguridad nacional.	• Crear modelos servitizados orientados a democratizar la tecnología ligada con la transformación digital. • Centrar los recursos de I+D+i en los nichos de oportunidad con menor madurez y mayor potencial. • Apostar por start-ups born-digital y big bang disruptor. • Proyectos del Plan de recuperación alineados con la transformación digital europea. • Programas de fomento a la innovación empresarial (PoC, retos industriales). • Transformar el liderazgo actual en ciencia en liderazgo en innovación y emprendimiento apoyándose en role models y emprendedores en serie.

Tabla 15: CAME desde la perspectiva de las ideas

CAME. Perspectiva del talento	
Corregir (debilidades)	**Mantener (fortalezas)**
• Actuar sobre el sistema educativo desde edades tempranas para captar talento natural o generar vocaciones investigadoras, apalancado en el carácter social de la ciberseguridad. • Visibilizar la I+D+i y la ciberseguridad en general como una opción profesional entre el alumnado femenino. • Potenciar los programas de contratos Torres Quevedo (o similares) para la contratación laboral de doctores en empresas, centros tecnológicos, etc. • Enriquecer los programas curriculares incorporando competencias de ciberseguridad no solo en grados TIC (tecnología) sino también en todos los relacionados con sectores digitalizados (buenas prácticas). • Incrementar la calidad y abaratar el coste del acceso a la oferta educativa en inglés.	• Extender a otros centros universitarios y de formación profesional los casos de éxito de grados y másteres especializados en ciberseguridad. • Evolucionar los contenidos educativos hacia una mayor especialización y orientación aplicada a las necesidades de las empresas. • Establecer una relación permanente con universidades extranjeras donde poder captar talento investigador.
Afrontar (amenazas)	**Explotar (oportunidades)**
• Reforzar el posicionamiento internacional de las universidades españolas en relación con la ciberseguridad. • Actuar sobre el sistema educativo desde edades tempranas para captar talento natural o generar vocaciones investigadoras, apalancado en el carácter social de la ciberseguridad. • Evitar dinámicas de mercado que presionen salarios a la baja	• Creación de ecosistemas de entrenamiento. • Desarrollo de grandes plataformas SPOC para el impulso rápido de las tecnologías habilitadoras en todos los campos. • Innovar en los procesos de re-skilling para mitigar la brecha de talento en el sector incorporando personas procedentes de otros nichos profesionales. • Enriquecer con retos y contenidos de ciberseguridad en los programas de doctorado.

Tabla 16: CAME desde la perspectiva del talento

CAME. Perspectiva de la inversión	
Corregir (debilidades)	**Mantener (fortalezas)**
• Acercarse lo más posible a la media actual de la UE (2,18%) y más allá hasta el objetivo UE del 3%. • Identificar esquemas de financiación para I+D en ciberseguridad más acordes a los llevados a cabo en otros países que puedan servir como referencias exitosas. • Mejorar las condiciones laborales de profesorado universitario y doctorandos a través de mecanismos de financiación público-privados para facilitar que el talento investigador pueda mejorar su desempeño. • Valorar el incremento de los incentivos económicos para la I+D+i llevada a cabo en las empresas. • Crear una cultura de inversión en empresas de base tecnológica frente al modelo inversor en activos materiales. • Revisar el modelo para flexibilizar las condiciones de los avales y tratar de mejorar la situación actual. • Crear una red de inversión público-privada para retener activos I+D+i e impulsar el crecimiento de las *start-ups*.	• Incentivar la adopción temprana de soluciones nacionales de ciberseguridad por las infraestructuras críticas. • Incentivar la adopción temprana de soluciones nacionales de ciberseguridad por las administraciones públicas. • Fomentar e incentivar la adopción de reglamentación europea a través de la industria nacional.
Afrontar (amenazas)	**Explotar (oportunidades)**
• Definir una única estrategia de I+D+i común que facilite la canalización adecuada de los recursos. • Diseñar nuevos programas de financiación a nivel nacional para la I+D+i en ciberseguridad que cubra corto, medio y largo plazo. • Crear un cuadro de mando para evaluar los resultados obtenidos en los proyectos financiados por el programa nacional. • Velar por mantener o mejorar posición en siguientes ediciones del GCI de ITU. • Acortar los plazos y reducir la burocracia para la creación de infraestructuras I+D+i. • Valorar cómo afecta el dimensionamiento de la ética en la protección de datos y derechos • Fomentar las patentes de software	• Enriquecer el programa nacional RETOS DE INVESTIGACIÓN y similares convirtiéndolo en un instrumento (incluso de carácter competitivo) más dirigido a aquellas prioridades relacionadas con la Estrategia Nacional y que evite repetir trabajos. • Promover capacidades para dar soporte a los esquemas de certificación asociados a la regulación. • Poner en marcha mecanismos de la economía digital para financiar la inversión en I+D+I «IDITECH». • Asegurar la continuidad a largo plazo de las líneas de acción que responden a la Estrategia Nacional y de los espacios de diálogo (como el Foro Nacional de Ciberseguridad). • Impulsar la Compra Pública Innovadora.

Tabla 17: CAME desde la perspectiva de la inversión

CAME. Perspectiva de las relaciones	
Corregir (debilidades)	**Mantener (fortalezas)**
• Crear una agenda estratégica de investigación (SRIA) en ciberseguridad. • Mejorar el posicionamiento de marca enfatizando los diferenciadores. • Realizar un estudio que compare las capacidades de España respecto a otros países modelo de mejores prácticas. • Programas específicos para fomentar su divulgación e impulsar su adopción en los sectores público, privado y servicios. • Definir modelos de incentivación que motiven la participación del profesorado universitario (reducción de carga docente, complementos salariales, etc.). • Diseñar un plan de alianzas para establecer puentes con subsistemas investigadores de interés. • Aparte de Web of Science, determinar en qué otros medios (revistas o conferencias) se ha de reforzar la presencia nacional. • Identificar qué temáticas de I+D+i pueden ser interesantes y en qué lugares y formatos podría interesar dinamizarlas. • Impulsar programas que fomenten la cultura de relacionarse y la consecución de objetivos. • Crear espacios de diálogo entre empresas, universidades y centros tecnológicos (ejemplo: plataformas de innovación abierta o programas colaborativos de subvenciones).	• Reforzar y evolucionar acciones de concienciación entre las organizaciones usuarias. • Promover y reforzar la cooperación entre competidores para generar soluciones innovadoras más completas fruto de la cooperación y la diversidad. • Extender los casos de éxito desde las regiones y sectores más maduros a los demás. • Ampliar los nichos y potenciar la imagen de las regiones/nodos que actualmente no estén posicionadas. • Visibilizar el éxito individual bajo una imagen de marca basada en una estrategia común de posicionamiento. • Velar por mantener o mejorar posición en siguientes ediciones GCI.

Tabla 18: CAME desde la perspectiva de las relaciones

CAME. Perspectiva de las relaciones	
Afrontar (amenazas)	**Explotar (oportunidades)**
• Reconocer, validar, posicionar, potenciar, incentivar la industria nacional para fomentar su adopción en los sectores públicos, privados y servicios. • Participar activamente para posicionar y visibilizar las evoluciones de España. • Reforzar el posicionamiento internacional de las I+D+i española en relación con la ciberseguridad.	• Identificar proyectos país de ciberseguridad alineados con la estrategia de I+D nacional y/o con la estrategia europea en la ciberseguridad. • Nadie puede producirlo todo. Identificar subsistemas complementarios con los que establecer una balanza comercial bidireccional y equilibrada. • Creación de un modelo distribuido basado en nodos que aproveche la diversidad de la economía y potencie la especialización. • Potenciar el espacio de diálogo público-privado e integrador proporcionado por el Foro Nacional de Ciberseguridad. • Continuar el posicionamiento en el ecosistema europeo de la ciberseguridad apalancándose en proyectos como SPARTA (Indra/Tecnalia/Vicomtech), CONCORDIA (Telefónica I+D/ATOS/Caixabank), Cybersec4Europe (UMU/UMA/ATOS/ BBVA), ECHO (Telefónica).

XII. Propuesta de incentivos salariales y no salariales

+ Anexos

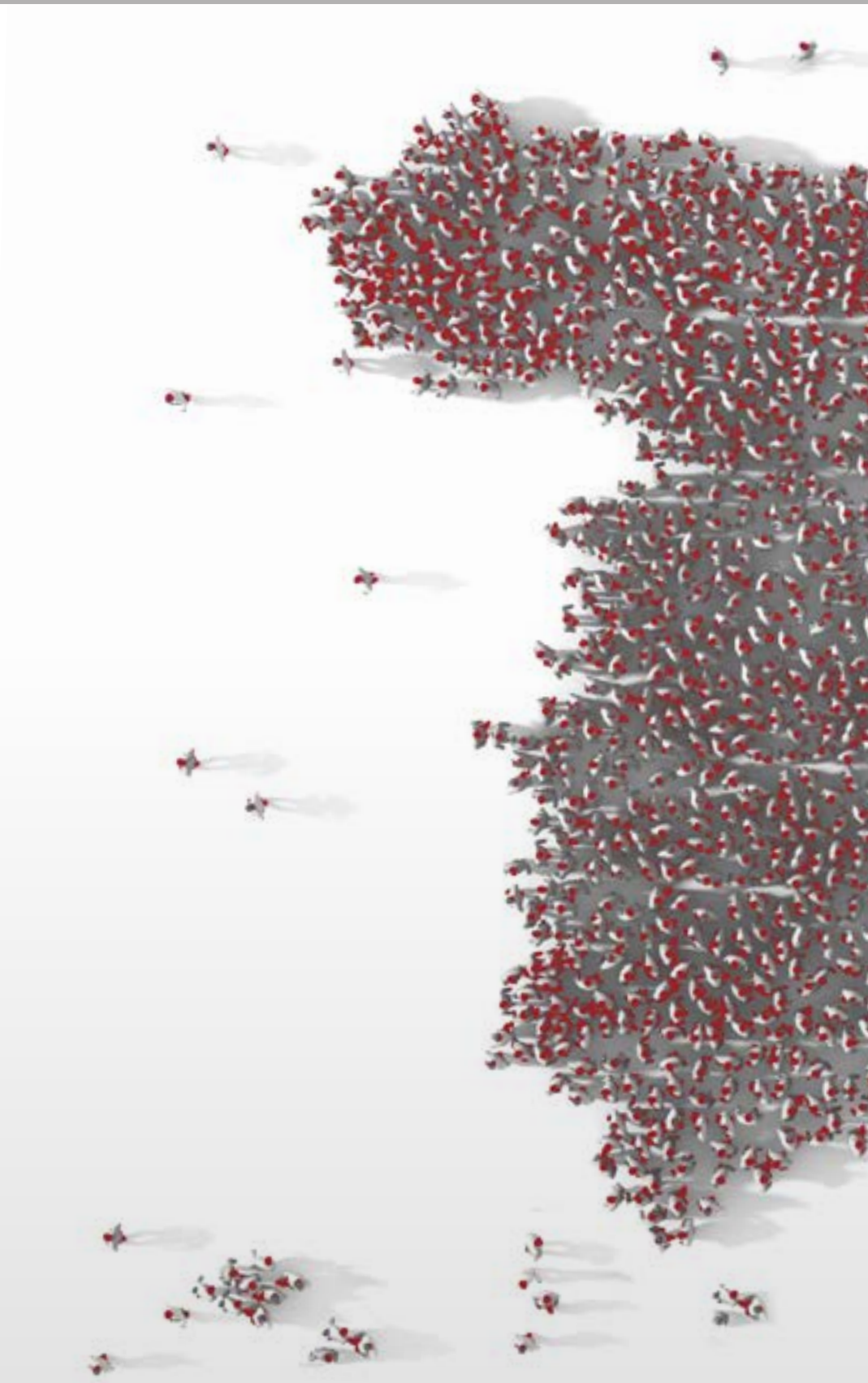
Incentivos no salariales

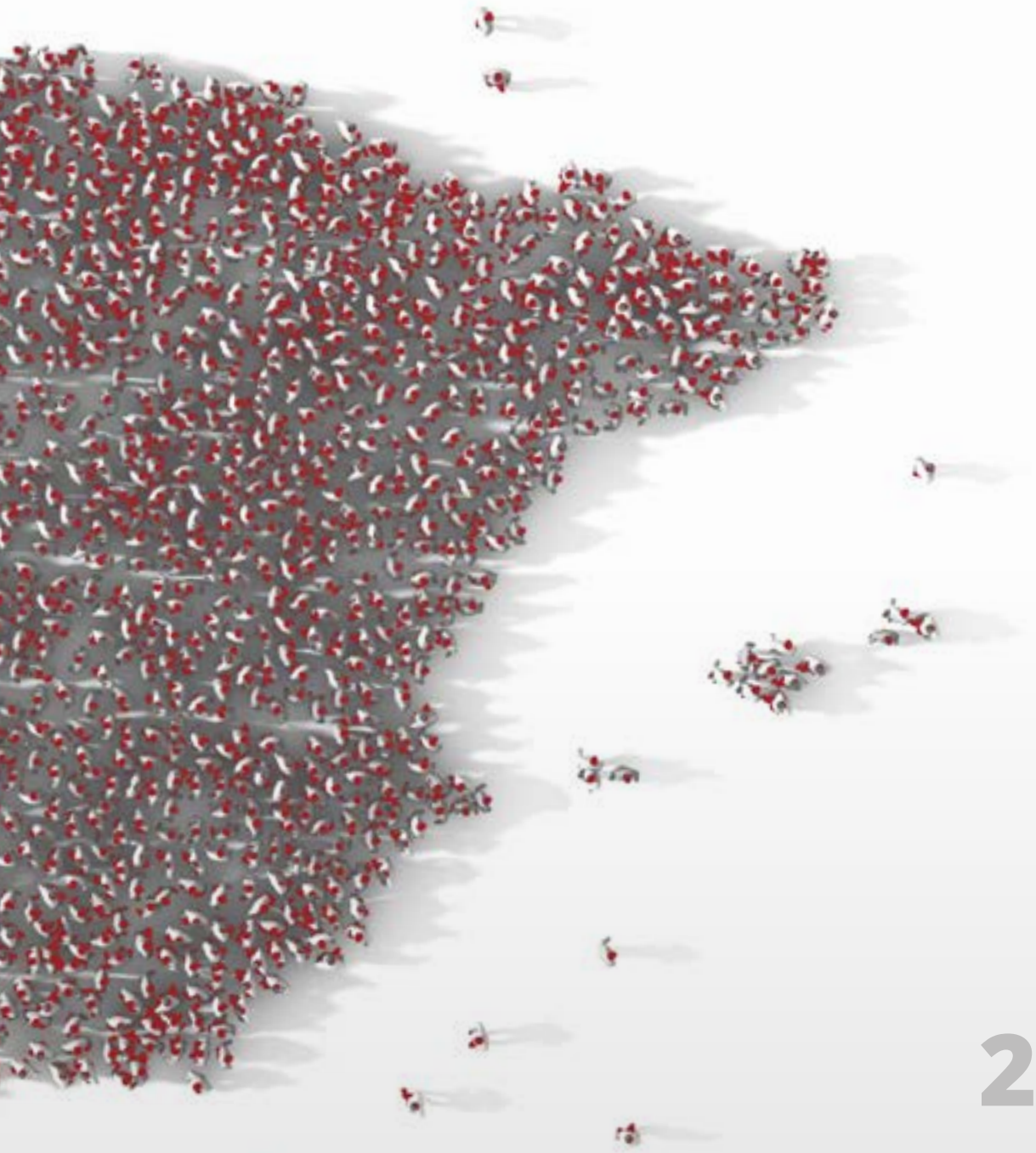
Incentivo	Medidas concretas
Formación	Becas de estudio de libre elección por el empleado Capacitación y desarrollo competencial planificado por la compañía Plan de mentoría dentro de la compañía Capacitación gerencial Aprendizaje «en el puesto de trabajo» de nuevas tecnologías incorporadas por la compañía Seminarios externos
Calidad de vida	Actividades socio-laborales, celebraciones de fechas especiales Instalaciones con áreas de trabajo amplias, silenciosas y privadas Área de descanso interior y exterior. Cocina. Gimnasio. Guardería. Botiquín. Mejoras en los lugares de trabajo: acceso, luminosidad, decoración, condiciones ambientales, etc. Parking para vehículo propio Atención a la calidad de vida del trabajador, desarrollo del mismo Herramientas de trabajo de calidad: terminal móvil, ordenador portátil, conexión a internet. Flexibilidad en vestimenta y en horarios de trabajo Teletrabajo Permisos especiales Convenios con entidades bancarias, de la salud, grandes almacenes, restauración, etc.
Plan de carrera	Desarrollo de carrera del personal clave Capacitación cruzada para potenciar la polivalencia de los empleados. Planes de carrera Planes de desarrollo profesional y personal Programa de ascenso por méritos propios de acuerdo a las capacitaciones que vayan completando los empleados. Rotación interior a la compañía y rotación geográfica en el mismo puesto.
Proceso de ingreso	Transparencia en los procesos de selección y promoción Programa de promoción interna de vacantes, con desarrollo de empleados en aquellas competencias faltantes. Planes de reemplazo por jubilación Inducción y entrenamiento Proceso organizado de atracción de talento que cumpla con los perfiles que la compañía requiere. Seleccionar *soft-skills* para cada puesto, y tenerlo en cuenta en los procesos de selección.

Incentivo	Medidas concretas
Clima laboral	Beneficios sociales y cultura empresarial Buen ambiente laboral Gerencia de puertas abiertas. Acercamiento de la dirección a los trabajadores. Monitorización del clima laboral
Integración familiar	Becas para hijos de empleados Actividades de socialización con familias Diversos programas no solo dirigidos a los trabajadores sino también a las familias de los trabajadores. Vacaciones recreativas
Estabilidad laboral	Vinculación directa Cláusula de permanencia mínima
Plan de sucesión	Plan de sucesión Planes de reemplazo, carreras profesionales dentro de la organización
Reconocimiento	Reconocimientos simbólicos Consolidación de la cultura por medio de espacios de reconocimiento. Reconocimiento público al personal (a través de cartas de felicitación, reconocimiento en público de trabajadores destacados). Símbolos distintivos de reconocimiento (diploma, placa, complemento de vestuario, elemento decorativo en el lugar de trabajo, etc.).
Sentido de pertenencia	Crear un sentido de pertenencia Persuadir a los empleados para que se adhieran a un propósito mayor. Participación de la empresa en iniciativas altruistas y filantrópicas de las que el empleado pueda sentirse orgulloso.
Tareas desafiantes	Enriquecimiento del cargo Retos en el trabajo Tareas desafiantes en las que los líderes del proceso propongan mejoras continuas sin desviarse de los objetivos.
Gestión del conocimiento	Procesos de intercambio de conocimientos y experiencias, de aprendizaje y de administración de la tecnología que aseguren que no se pierde el conocimiento necesario en los puestos críticos. Documentar red de contactos (agendas personales) de las partes interesadas (*stakeholders*) del puesto.
Contraprestación legal	Capacitación como contraprestación por permanencia mínima en la empresa.

Incentivos salariales

Incentivo	Medidas concretas
Paquete de beneficios	Ayuda de transporte Ayuda a manutención Ayuda para gastos extraordinarios, seguro de vida, seguro de salud y dental. Ayuda para estudios universitarios y formación del empleado Beneficios económicos para cónyuge e hijos del empleado: guardería, material estudio, vacaciones, idiomas, etc. Mutualidad para previsión social de empleados Préstamos ventajosos de libre disposición y para adquisición vivienda, vehículo o material informático. Alquiler de vivienda empleados en rotación Programa de renting de vehículo Conexión a internet
Bonificaciones - Incentivos	Aumento salarial o contraprestación en opciones sobre acciones y bonos de la empresa. Bonificaciones (de acuerdo a los resultados) e incentivos por cumplimiento de metas, logros o utilidades netas de la compañía o del departamento. Comisiones por ventas Premios al empleado, por rendimiento, innovación, votación de los clientes, cursos de capacitación, etc. Prima por permanencia (similar a los trienios en el sector público) Reconocimiento económico de los ascensos Salarios y bonificaciones por encima del promedio de la industria
Políticas salariales	Salario mínimo superior al SMI Estabilidad salarial. Nivelación de la escala salarial Equidad salarial, teniendo en cuenta el desempeño y competencias. Aumento salarial Equidad salarial dentro del sector frente al salario en el extranjero para el mismo puesto y competencias Equidad salarial para ejecutivos, acorde al cargo y al mercado internacional
Compensación variable	Componente variable del salario en función del rendimiento personal, departamental o empresarial.
Compensación flexible	Permuta de parte del salario por compensaciones en especie, ventajosas financiera y fiscalmente para el empleado





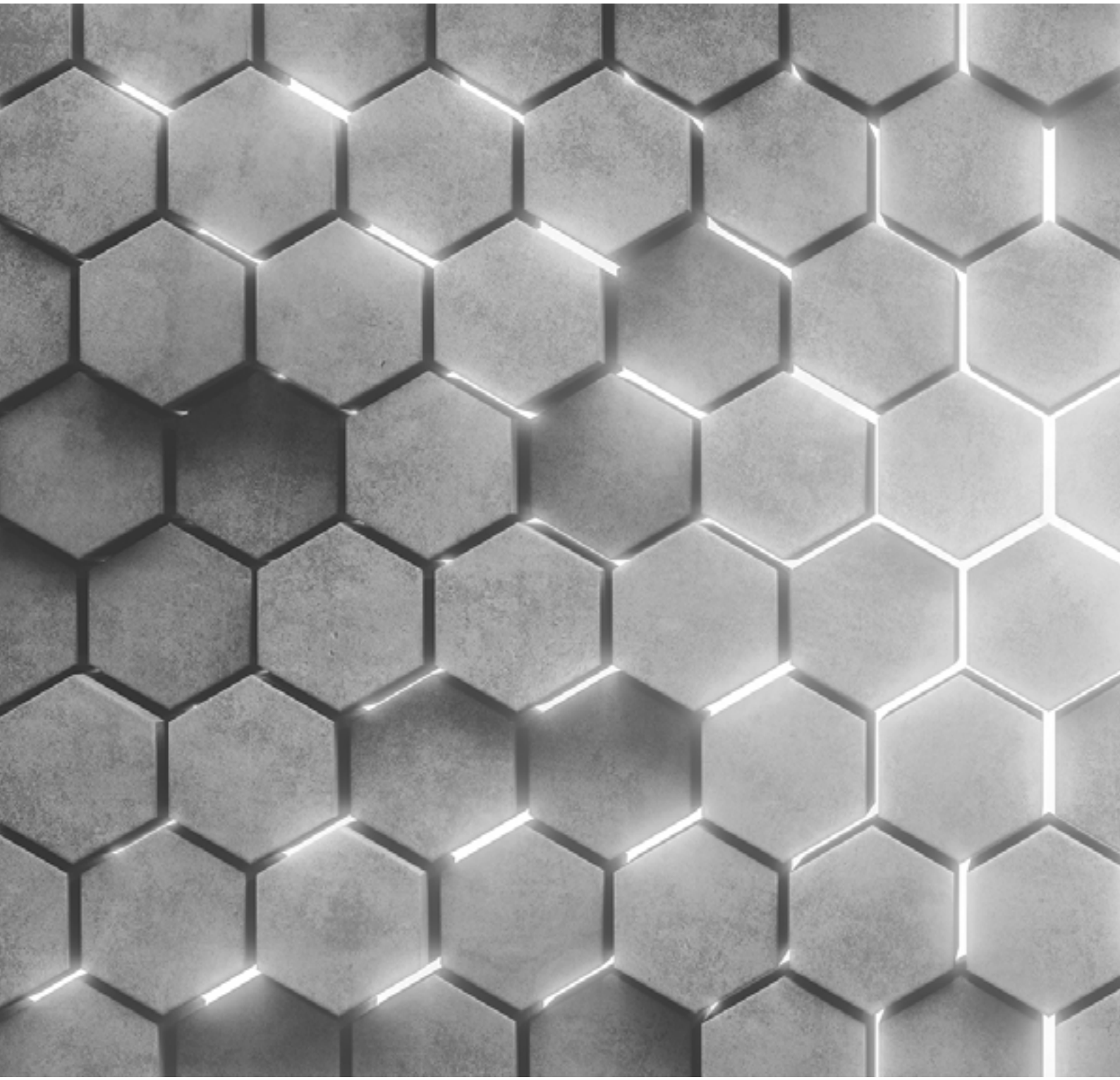
2021

ESQUEMA NACIONAL DE CERTIFICACIÓN DE RESPONSABLES DE CIBERSEGURIDAD

FORO NACIONAL DE CIBERSEGURIDAD

Índice

+ Esquema Nacional de Certificación de Responsables de Ciberseguridad (RCSEG)

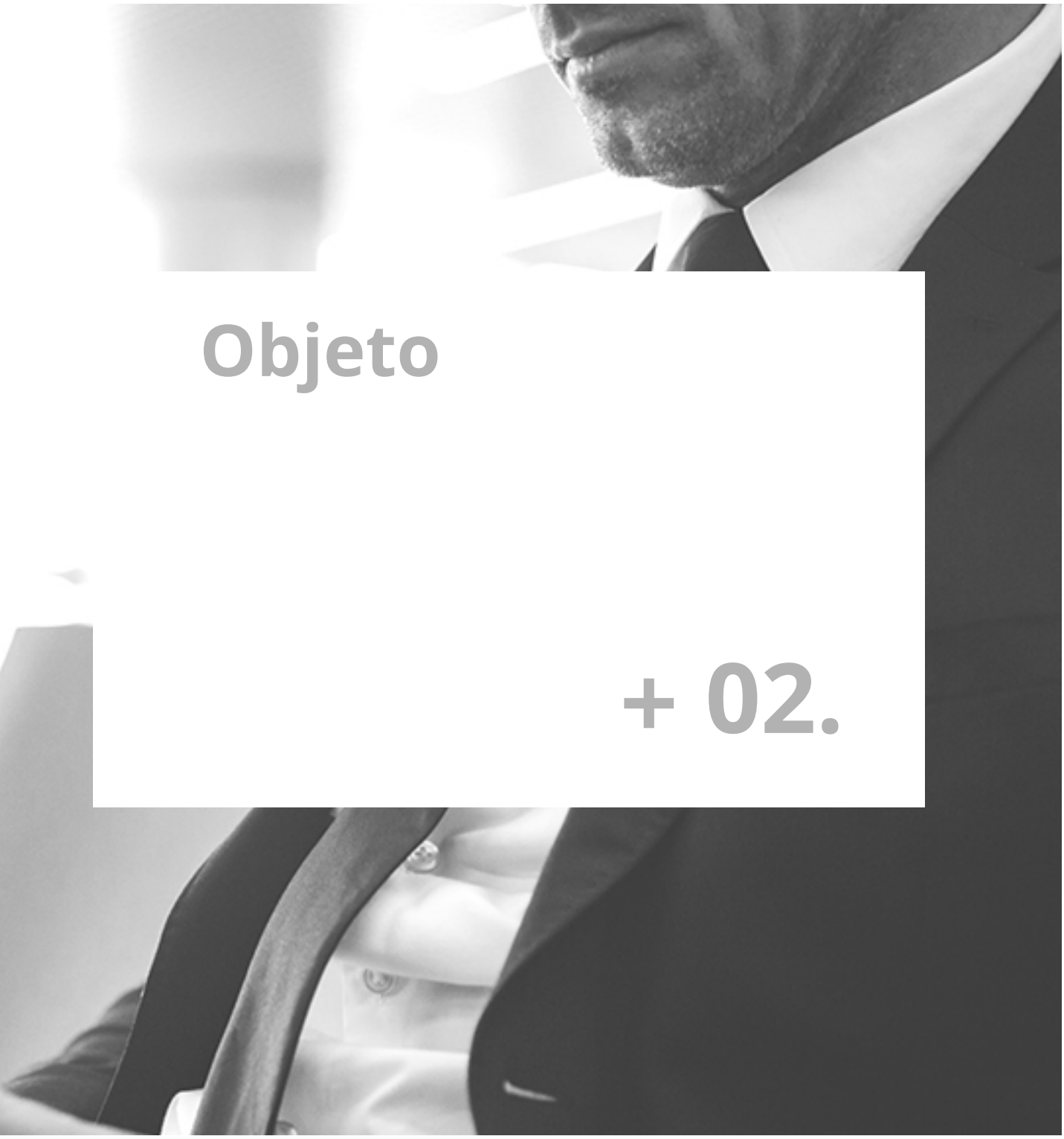


Acrónimos y terminología

+ 01.

Acrónimos y terminología

/// AEPD	Agencia Española de Protección de Datos.
/// CCN	Centro Criptológico Nacional.
/// CE	Comité del Esquema.
/// CGE	Comité de Gestión del Esquema.
/// CSIRT	Computer Security Incident Response Team: Equipo de Respuesta ante Incidencias de Seguridad Informáticas.
/// DPD	Delegado de Protección de Datos.
/// EC	Entidad de Certificación de Responsables de Ciberseguridad o Entidad de Certificación de RCSEG.
/// ENAC	Entidad Nacional de Acreditación.
/// ENS	Esquema Nacional de Seguridad.
/// Esquema de Certificación de RCSEG	Esquema Nacional de Certificación de Responsables de Ciberseguridad.
/// OCC	Oficina de Coordinación de Ciberseguridad.
/// RCSEG	Responsable de Ciberseguridad.
/// RGPD	Reglamento General de Protección de Datos.
/// SGAD	Secretaría General de Administración Digital.



Objeto

+ 02.

Objeto

El objeto de este documento [ENCRCSEG-01] es establecer las condiciones y requisitos que conforman y regulan el funcionamiento del Esquema Nacional de Certificación de Personas en lo que respecta a competencias relacionadas con la ciberseguridad:

Responsable de la Seguridad del Esquema Nacional de Seguridad	Según lo determina el **art. 10 del RD 3/2010**, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
Responsable de Seguridad y Enlace de las infraestructuras críticas	Según lo determina el **art. 16 de la Ley 8/2011**, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
Responsable de la seguridad de la información	Según lo determina el **art. 7 del Real Decreto 43/2021**, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
Responsables de Seguridad de servicios o productos TIC de empresas proveedoras de infraestructuras críticas o de servicios esenciales	En el alcance de la **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público.

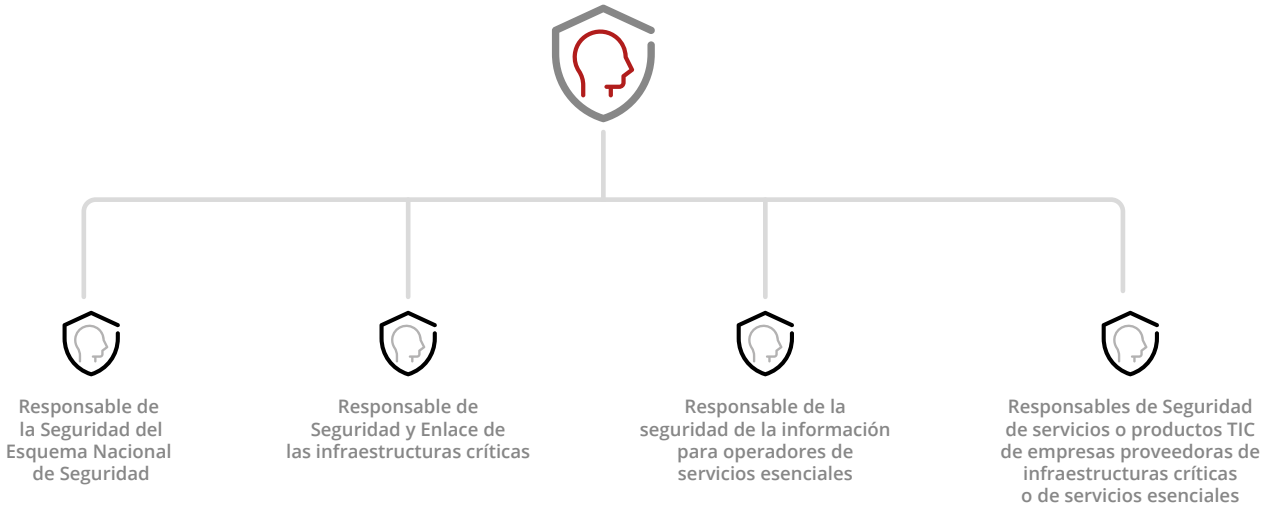
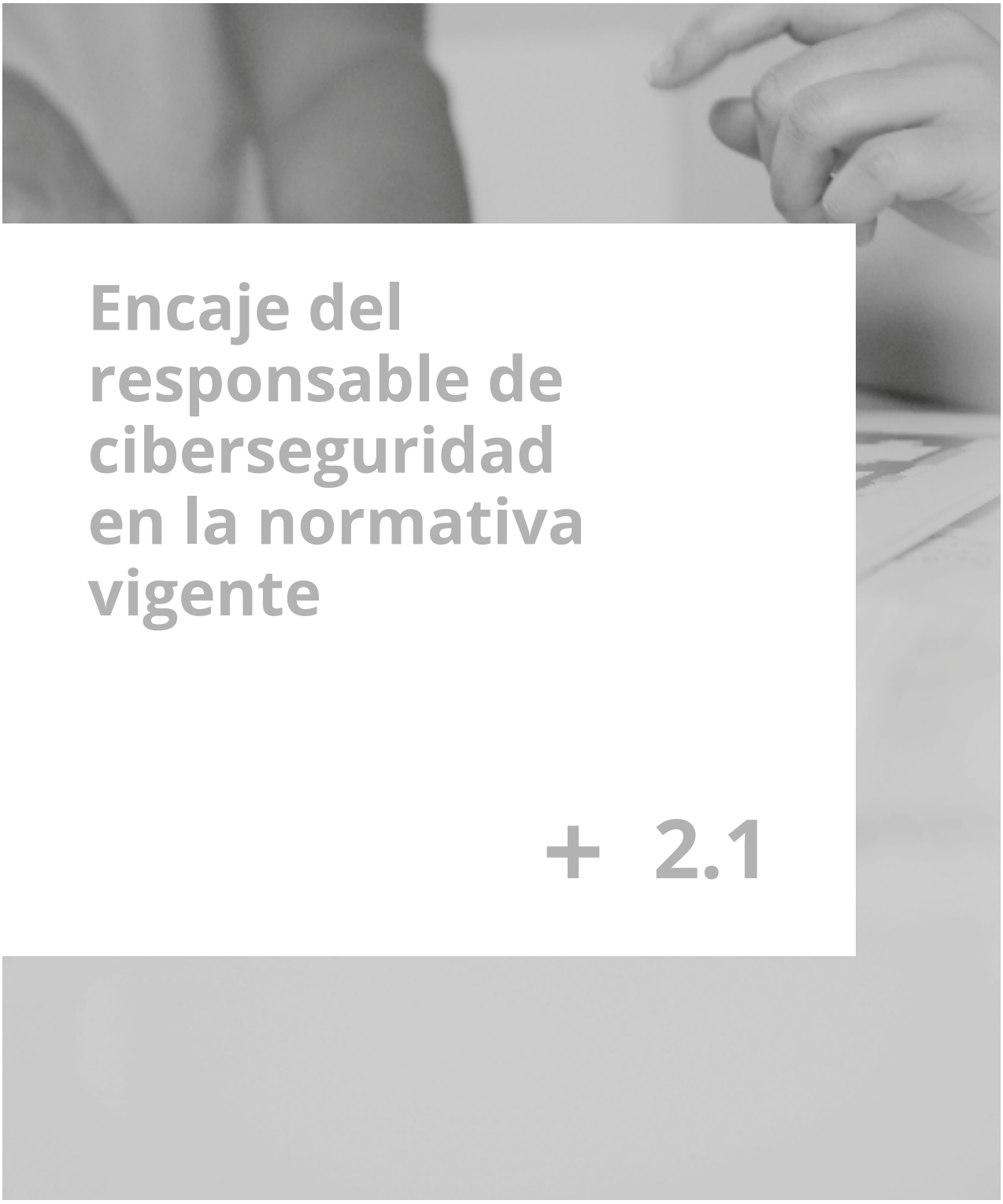


Figura 1. Competencias incluidas en el Esquema Nacional de Certificación de Responsables de Ciberseguridad

En adelante se denominará Esquema Nacional de Certificación de Responsables de Ciberseguridad, Esquema RCSEG o el Esquema.

La certificación de personas es un método adecuado y válido para la evaluación objetiva e imparcial de la competencia de un individuo para realizar una actividad determinada. La declaración pública, hecha por el certificador, proporciona a la sociedad en general una información útil y contrastada sobre los criterios aplicados y los requisitos exigidos a las personas para obtener la certificación profesional. La validez y vigencia de las reglas del Esquema se asegura a través de la implicación activa de expertos y de representantes de las diferentes partes interesadas en su desarrollo.

La **competencia técnica de las Entidades de Certificación** involucradas y su alineamiento con los requisitos fijados por el Esquema, así como su actuación sistemática e imparcial, se consiguen a través de su **acreditación por parte de ENAC**, de acuerdo con requisitos de normas internacionales para la certificación de personas, como es la norma UNE-EN ISO/IEC 17024:2012.



Encaje del responsable de ciberseguridad en la normativa vigente

+ 2.1

El RCSEG es una función o desempeño profesional común, en todo o en parte, a determinadas figuras introducidas por diferentes normas jurídicas sobre la seguridad como función diferenciada, siendo habitual en todas ellas que dicho responsable determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, teniendo, entre otras, las siguientes funciones:

- **Mantener la seguridad de los sistemas de información** que soportan los servicios prestados, y la información manejada por estos, en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización.

- **Promover la formación y concienciación** en materia de seguridad de la información dentro de su ámbito de responsabilidad.

- **Supervisar la ciberseguridad corporativa**, en su sentido amplio, centrada en el diseño, despliegue, cumplimiento y mejora continua de las estrategias definidas en la organización.

- **Participar en la toma de decisiones del órgano de dirección de la entidad** en materia de seguridad de la información, incluyendo las decisiones relativas a las partidas presupuestarias destinadas a ciberseguridad, valorando su oportunidad, en función de los riesgos.

- **Ejercer la Secretaría del Comité de Seguridad de la Información**, si existe, y como tal, bajo las directrices de su Presidente:

  - **Convocar** las reuniones del Comité.
  - **Preparar los temas** a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
  - **Elaborar el acta** de las reuniones.
  - **Responsabilizarse de la ejecución** directa o delegada de las **decisiones del Comité**.

- **Elaborar y proponer**, para su aprobación por los órganos directivos de la **organización, las Políticas, Normativas y Procedimientos de Seguridad de la Información**, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.

- **Supervisar y colaborar en la implantación de las políticas, normativas y procedimientos de seguridad**, supervisando su eficacia y llevando a cabo controles periódicos de seguridad y verificación de cumplimiento y eficacia.

- **Elaborar el documento de Declaración de Aplicabilidad de las medidas de seguridad**, atendiendo en su caso a la normativa que resulte de aplicación (por ejemplo, RD 3/2010 y RD 43/2021).

- Proponer la **implantación de las medidas organizativas y técnicas necesarias** para **prevenir**, **detectar**, **reaccionar** y, en su caso, **paliar**, las posibles consecuencias de los diferentes escenarios que se prevean relacionados con la ciberseguridad y participar en la recuperación de forma proactiva.

- **Proponer la implantación de otras medidas preventivas y de mantenimiento** en el ámbito de la ciberseguridad. Por ejemplo: ejercicios y simulacros, preparación e instrucción/capacitación del personal, articulación de los canales de comunicación precisos, para abordar posibles escenarios adversos.

- **Adoptar medidas de coordinación** con el Plan Nacional de Protección de las Infraestructuras Críticas.

- **Actuar como capacitador de buenas prácticas en seguridad** de las redes y sistemas de información, tanto en sus aspectos físicos como lógicos.

- **Constituirse**, cuando así se encuentre prescrito en la normativa de aplicación, **en el punto de contacto con la autoridad competente en materia de seguridad** de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan de dicha normativa.

- **Remitir a la autoridad competente**, a través del CSIRT de referencia y sin dilación indebida, **las notificaciones de incidentes** que tengan efectos perturbadores en la prestación de los servicios a los que, en su caso, se refiera la normativa de aplicación (por ejemplo, RD 3/2010 y RD-ley 12/2018).

- **Recibir, interpretar y supervisar la aplicación de las instrucciones y guías** emanadas de la autoridad competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

- **Recopilar, preparar y suministrar información o documentación** a la autoridad competente o al CSIRT de referencia, a su solicitud o por propia iniciativa.

Asimismo, **el RCSEG deberá disponer de conocimientos especializados y experiencia en materia de seguridad de la información y ciberseguridad**, desde los puntos de vista estratégico y de gobierno, táctico y de gestión, organizativo, operativo, técnico, jurídico y de cumplimiento, adecuados al desempeño de las funciones indicadas, así como experiencia y capacidad de liderazgo, dirección de personas, equipos y gestión del talento.

Para asegurar un adecuado desarrollo de sus competencias, es necesario que el RCSEG:

- **Cuente con los recursos necesarios** —humanos, materiales y económicos— para el desarrollo de las funciones señaladas.

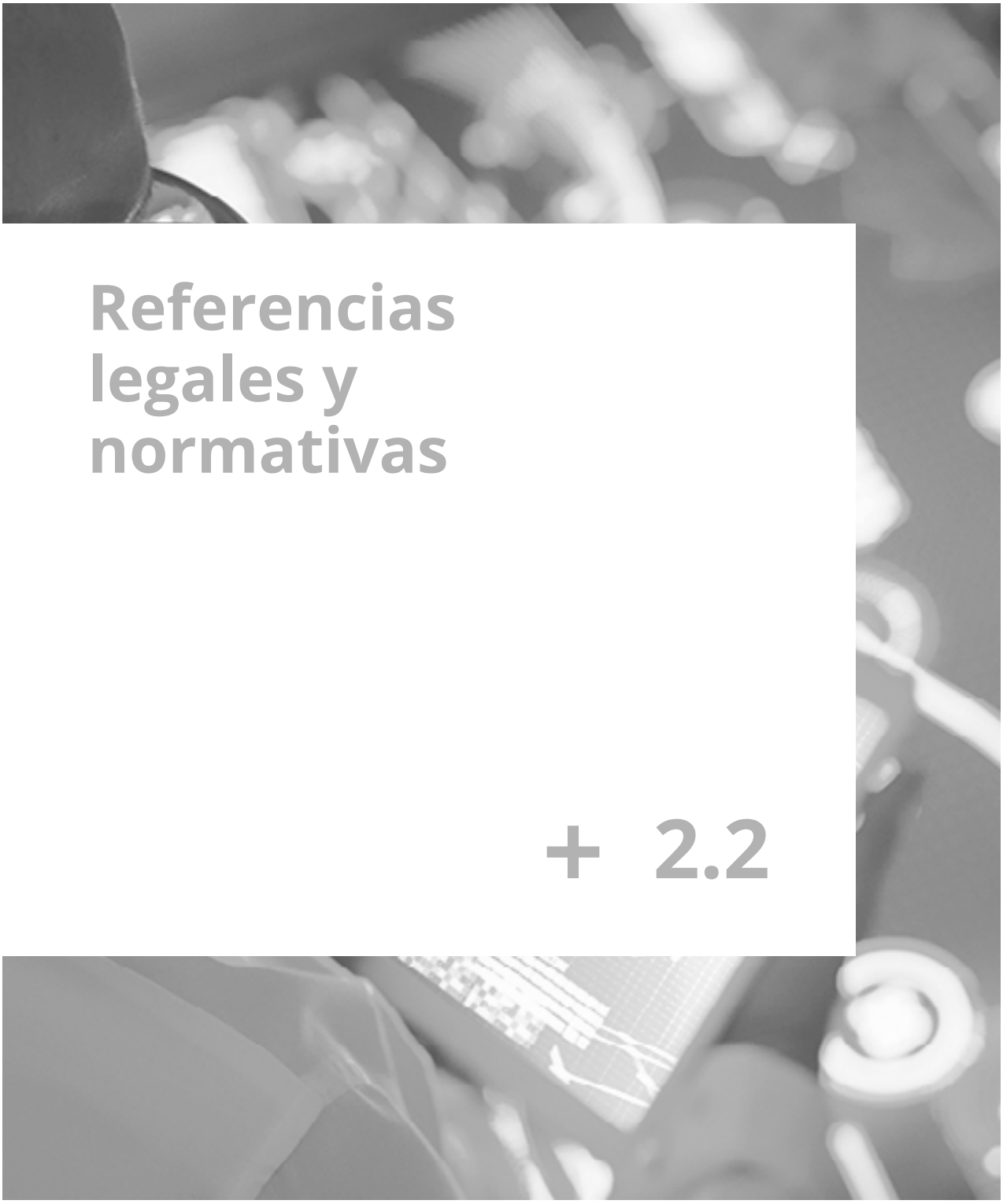
- **Ocupe una posición en la organización que facilite el desempeño de sus funciones**, participando de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad y ciberseguridad, y manteniendo una comunicación real y efectiva con la alta dirección y con el resto de responsables y sus funciones, tales como riesgos (CRO), privacidad (DPD), legal (CLO), cumplimiento (CCO), continuidad (CCNO), sistemas (CIO), etc.

- **Mantenga la debida independencia** respecto de los responsables de la explotación de las redes y los sistemas de información y, cuando sea preceptivo, necesario o conveniente, del resto de funciones de la organización.

- **Participe de manera activa en el análisis** de riesgos, vulnerabilidades, amenazas e impactos, en materia de ciberseguridad.

Por todo ello, siempre que se satisfagan los requisitos de capacidad, experiencia, e independencia y, en su caso, titulación, las funciones y responsabilidades descritas para el RCSEG resultarán de aplicación a las equivalentes del Responsable de la Seguridad del ENS, Responsable de Seguridad y Enlace en los operadores de servicios esenciales, el Responsable de Seguridad de la Información derivado de la Directiva NIS y, en su caso las del Delegado de Protección de Datos (DPD), de conformidad con lo dispuesto en la regulación de aplicación a cada una de estas figuras.

Para desarrollar sus funciones, **el RCSEG podrá apoyarse en servicios prestados por terceros**.



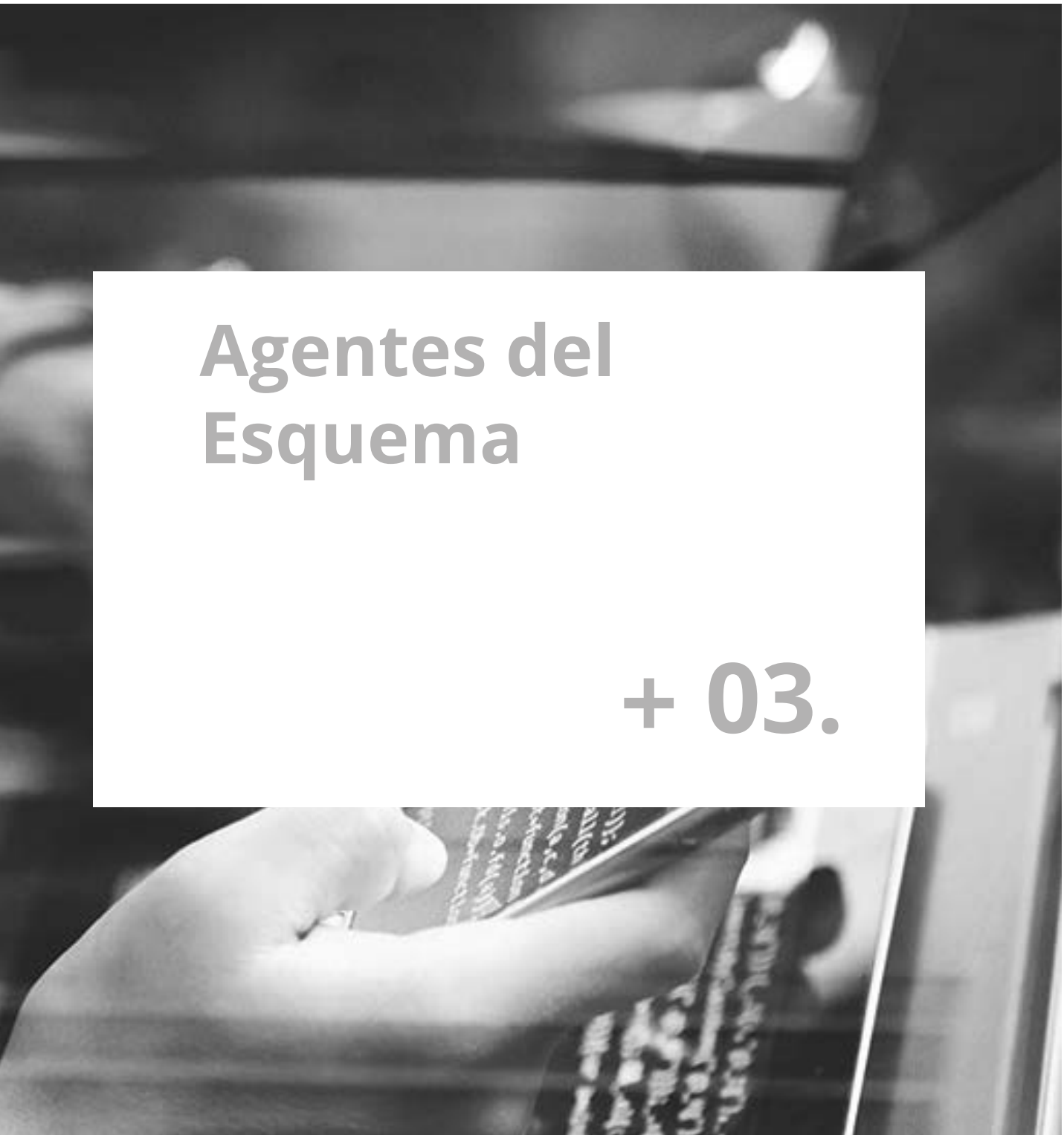
Referencias legales y normativas

+ 2.2

Las referencias legales y normativas que se han tenido en cuenta para el estudio, consulta y elaboración del presente Esquema han sido:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y normas de desarrollo (en adelante, ENS).
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (en adelante, LPIC).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD).
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y regulación de desarrollo.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- UNE-EN ISO/IEC 17024:2012. Evaluación de Conformidad. Requisitos generales para los organismos que realizan certificación de personas.

Todas las normas y documentos citados son aplicables en su última versión.



Agentes del Esquema

+ 03.

Agentes del esquema

El Centro Nacional de Inteligencia, a través del CCN; la Secretaría de Estado de Digitalización e Inteligencia Artificial, a través de la SGAD; y la Secretaría de Estado de Seguridad, a través de la OCC, como copropietarios todos ellos del Esquema Nacional de Certificación de Responsables de Ciberseguridad, son responsables de promover su desarrollo, revisión y validación continua, autorizando al resto de los agentes para formar parte activa del mismo, en la medida descrita en el presente documento.

Agentes del Esquema

Figura 2

Comité del Esquema (CE)

Comité que ha elaborado el esquema.

Comité de Gestión del Esquema (CGE)

Comité responsable de la supervisión y perfeccionamiento del esquema.

La Entidad Nacional de Acreditación (ENAC)

Entidad Nacional de Acreditación designado por el RD 1715/2010.

Las Entidades de Certificación de RCSEG (EC)

Ofrecen la certificación, exclusivamente bajo acreditación de ENAC y de acuerdo con lo requerido por el presente Esquema y la norma UNE-EN ISO/IEC 17024:2012.

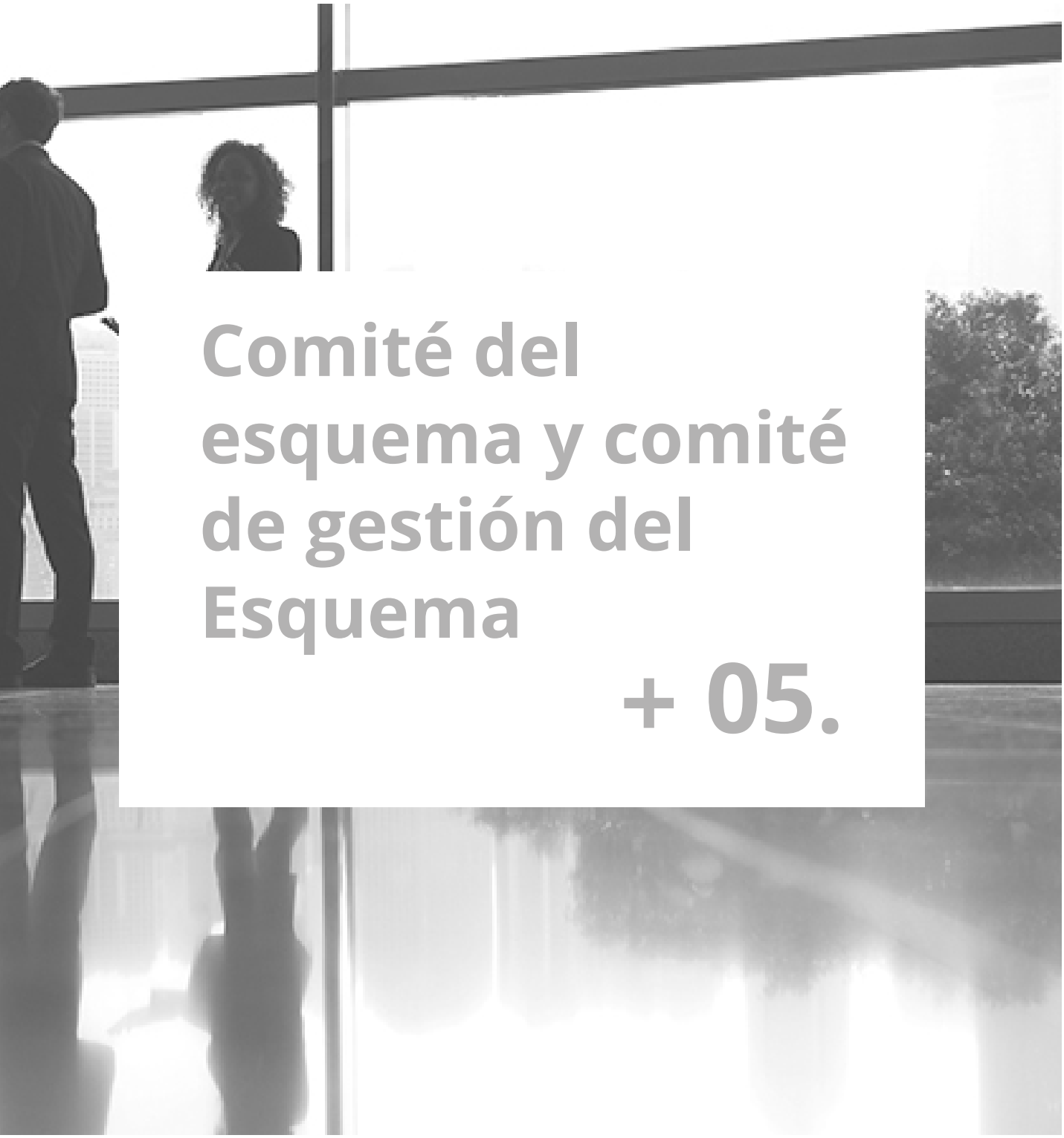
Marca de certificación

+ 04.

Marca de certificación

Las EC podrán usar la marca de certificación específica para este esquema por sí sola o asociada a una marca propia. Cuando se utilice una marca propia, dicha marca incluirá una referencia explícita al esquema (incluyendo el nombre completo o sus siglas) así como el número de Certificado al que está asociada, y deberá haber sido aprobada por el comité de gestión del esquema antes de poder ser usada por la entidad.

Las reglas sobre el uso del sello o marca de certificación se desarrollan en el Reglamento del Esquema Nacional de certificación de RCSEG. Las EC que dispongan de marca propia deberán establecer reglas para su uso siempre que respeten en todo caso el reglamento establecido por el CGE.



Comité del esquema y comité de gestión del Esquema

+ 05.

Comité del esquema y comité de gestión del esquema

5.1. Comité del Esquema

El Comité del Esquema (CE), constituido por sus tres (3) copropietarios y responsables paritarios citados anteriormente se reservan el derecho a ampliar sus miembros de común acuerdo si ello fuere necesario o conveniente. Dicho Comité, ha desarrollado y aprobado el presente Esquema Nacional de Certificación de RCSEG siguiendo lo establecido en la cláusula 8 de la norma UNE-EN ISO/IEC 17024:2012.

La Presidencia del Comité del Esquema será ejercida anualmente y de forma rotatoria entre sus miembros.

Decisiones

Las decisiones del Comité del Esquema se adoptarán por **unanimidad**.

Presidencia

La **Presidencia** del Comité del Esquema **será ejercida anualmente y de forma rotatoria entre sus miembros**, y su función esencial será la representación del Comité del Esquema durante el ejercicio de su mandato.

El Comité del Esquema y la ENAC colaborarán para mantener la máxima eficacia del Esquema y el prestigio de los certificados emitidos. Para garantizar dicha colaboración podrá ser necesario que la ENAC comparta información con el CE en relación con las entidades de Certificación y los procesos de auditoría, circunstancia que deberá ser expresamente consentida por las EC al solicitar la acreditación para este Esquema.

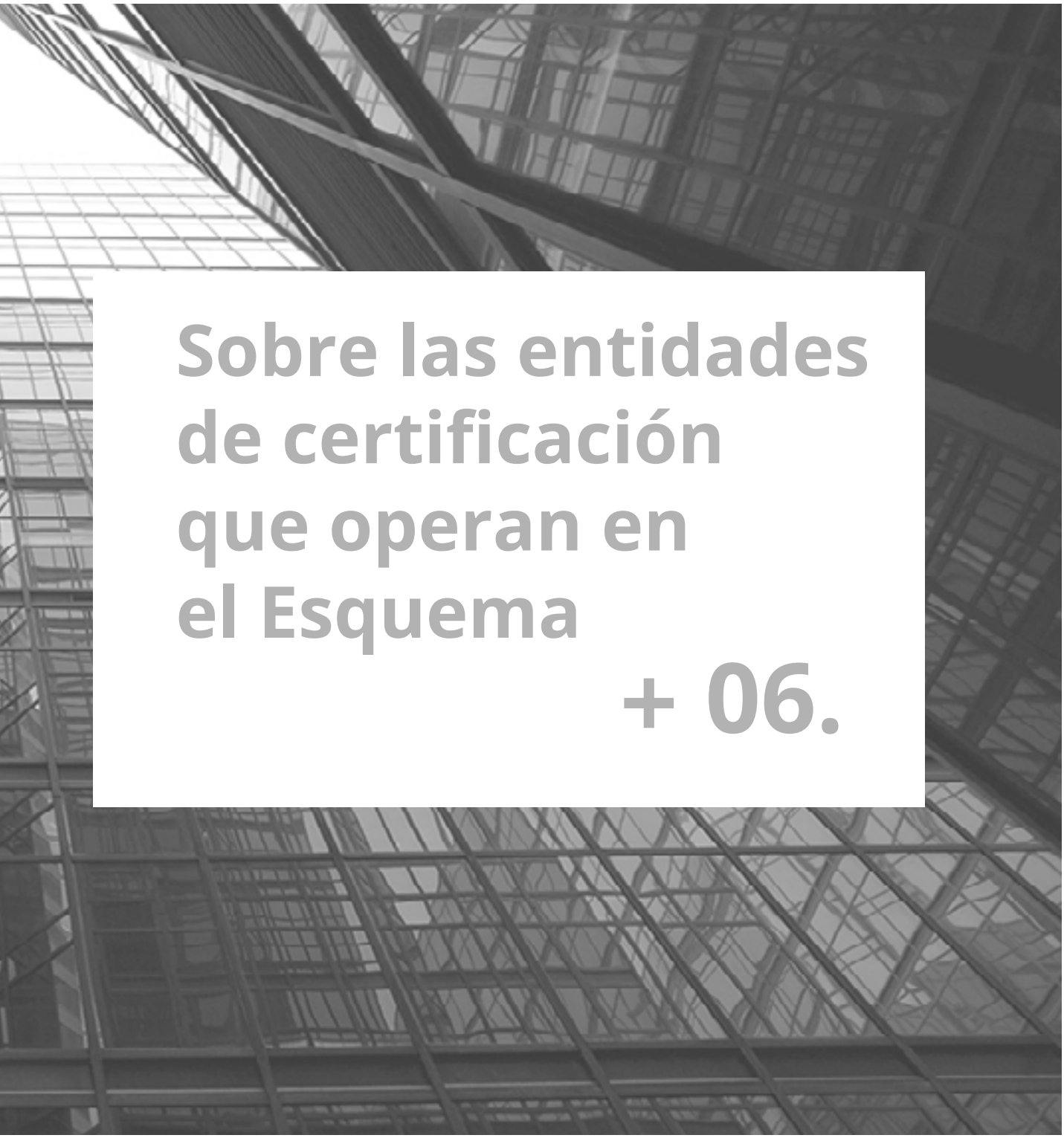
5.2. Comité de Gestión del Esquema

Para garantizar la gestión continuada del Esquema, el Comité del Esquema ha creado y mantiene un Comité de Gestión del Esquema (CGE) que se responsabiliza del perfeccionamiento, revisión, validación y supervisión periódica del Esquema, pudiendo -con la autorización del CE- intercambiar información con la ENAC, para el mejor acometimiento de sus funciones.

En particular, el CGE tendrá las siguientes **atribuciones**:

- **Decidir sobre la interpretación del cumplimiento con los requisitos del Esquema** salvo en aquellos casos en los que, de acuerdo a su Reglamento de funcionamiento, corresponda tal decisión al CE.
- **Validar los bancos de preguntas generadas por las EC** tal y como se indica en el Esquema.
- **Actualizar las previsiones del Esquema** en aquellos aspectos que no estén asignados al CE.
- **Aprobar las marcas específicas del Esquema**, así como sus posibles modificaciones y/o ampliaciones futuras de las mismas.

La organización, régimen de funcionamiento y responsabilidades, tanto del CE como del CGE, se regirá por su correspondiente **Reglamento interno**.



Sobre las entidades de certificación que operan en el Esquema

+ 06.

Sobre las entidades de certificación que operan en el Esquema

6.1. Requisitos generales

Para poder operar dentro del Esquema, las EC de RCSEG deberán estar acreditadas por la ENAC, de acuerdo con los requisitos establecidos en la norma UNE-EN ISO/IEC 17024:2012 para este Esquema.

6.2. Requisitos relativos a los evaluadores

Las EC son responsables de designar los evaluadores de acuerdo con los requisitos descritos en el Reglamento del Esquema Nacional de Certificación de RCSEG.

6.3. Proceso de entrada al esquema

Las entidades que deseen actuar dentro del Esquema y no estén todavía acreditadas, deberán obtener previamente la aprobación del CGE de la marca de certificación que pretendan usar (en el caso de que decidan utilizar una marca propia) y demostrar disponer de un mínimo de diez (10) personas evaluadas (entendiéndose por "persona evaluada" aquella que ha pasado todas las fases del proceso de evaluación, incluyendo la toma de decisiones, independientemente de que el resultado de dicho proceso haya sido positivo o negativo).

El régimen de funcionamiento de la aprobación del CGE se desarrollará en el **correspondiente Reglamento interno**.

En relación con el uso de la antedicha marca propia, las entidades deberán enviar al Comité de Gestión del Esquema una propuesta de la marca de certificación que se propongan usar, así como una declaración responsable, firmada por el representante legal de la entidad, en la que este se comprometa a:

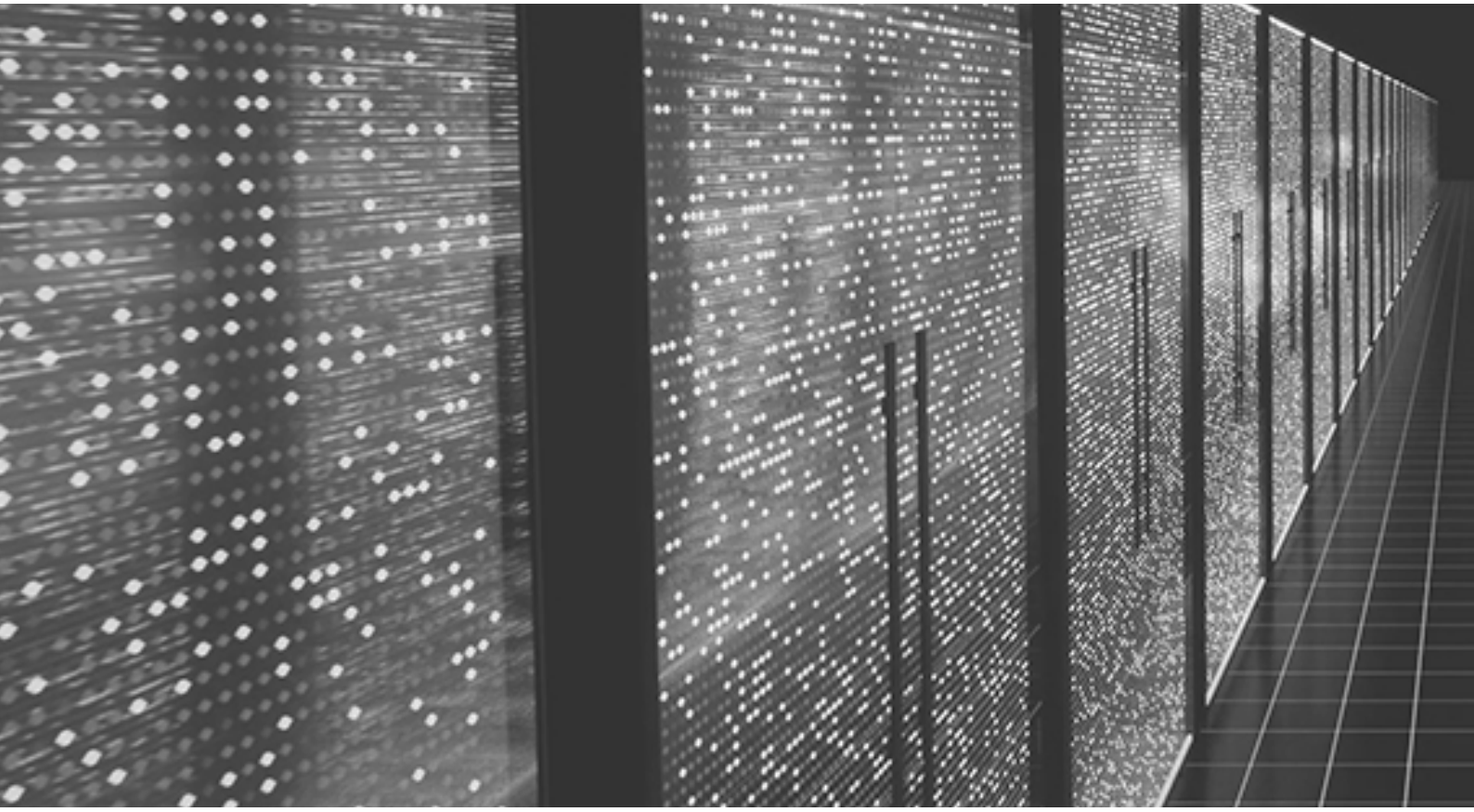
- **No hacer uso de la marca** hasta no haber sido acreditado para el Esquema.
- **No hacer ninguna referencia, en ningún tipo de soporte** (digital o físico), que pueda ser susceptible de entenderse como que la entidad ha sido autorizada, aprobada o acreditada para certificar en el Esquema[1].
- **No emitir certificados de ningún tipo** a las personas evaluadas hasta no haber sido acreditadas[2].
- **Cesar cualquier actividad en el Esquema** e informar a las personas que pudiesen haber sido evaluadas si son inhabilitadas para operar en el esquema.
- **Disponer de una declaración firmada por cada persona solicitante de la certificación** en la que declaren que aceptan que la obtención de un certificado dentro del Esquema está condicionado a que la entidad obtenga su acreditación y que aceptan que, en función del resultado del proceso de acreditación, la entidad les podría exigir repetir el proceso de certificación, o parte de él, para conseguir el certificado.

Si el CGE acepta la propuesta de la marca, debe informar a la entidad acusando también recibo de la recepción de la declaración responsable.

Se generará un Registro de Entidades de Certificación ya acreditadas (las autorizadas por el CE y las nuevas solicitudes en curso) y un Registro de Personas Certificadas. De esta forma, se da fiabilidad y todos los actores lo conocen, impidiéndose el uso de marcas sin estar autorizado o acreditado.

[1] Las entidades sí podrán, una vez aprobada la marca por el comité del Esquema, hacer público que se encuentran en proceso de evaluación con el único fin de disponer del número mínimo de personas evaluadas.

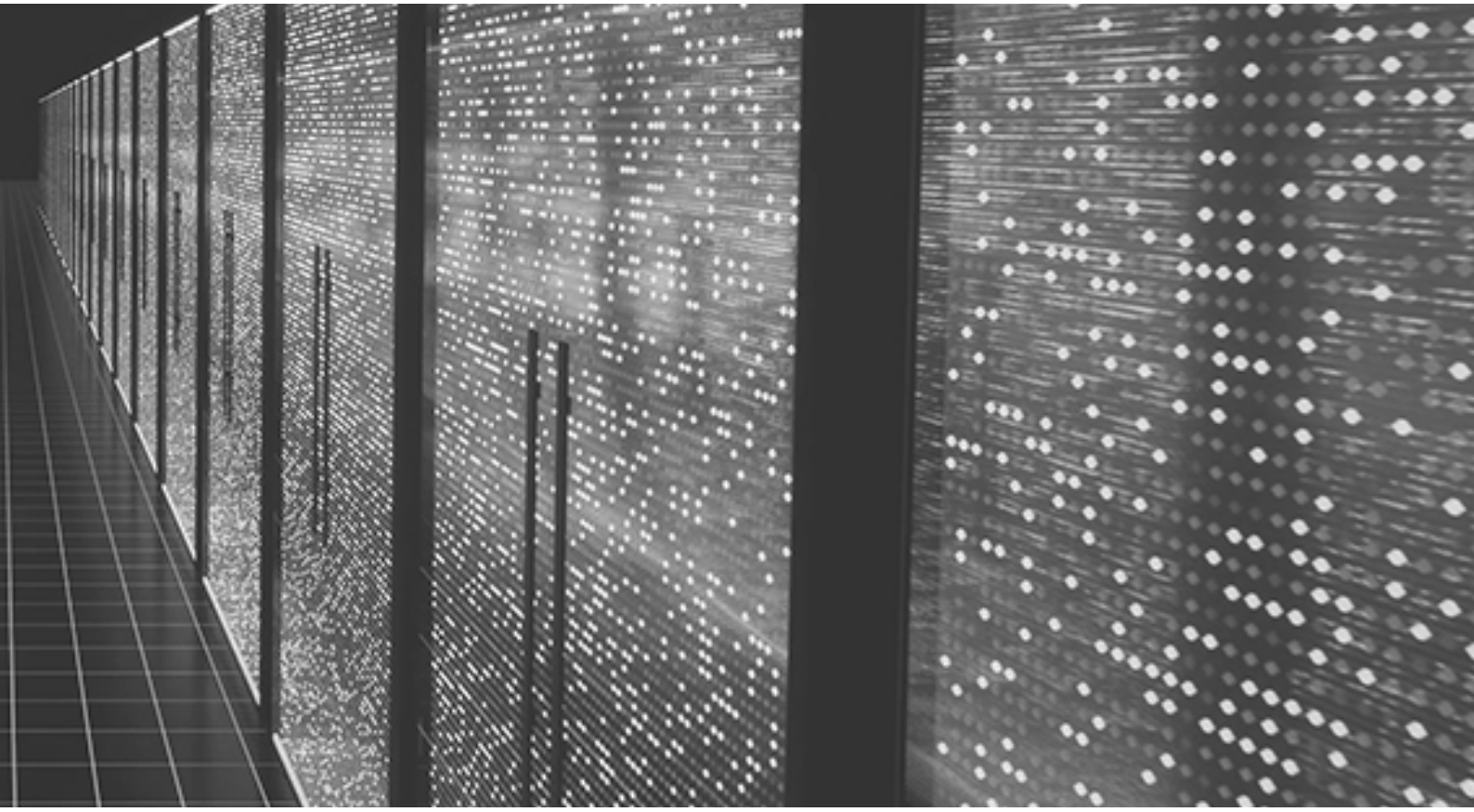
[2] Una vez acreditada la entidad actuará sobre dichos procesos de evaluación tal y como establece la NT 37 de ENAC.



6.4. Inhabilitación para operar en el esquema

El incumplimiento de cualquiera de los requisitos establecidos en la declaración responsable por parte de la entidad, implicará la revocación de la aceptación de la marca y, por tanto, su inhabilitación para operar en el Esquema, no pudiendo volver a solicitar su acceso en los seis (6) meses siguientes a la decisión de su revocación.

Esta función la asumirá el CGE, que evaluará estas casuísticas, apreciando si se detecta algún factor no alineado con el Esquema y dictaminando si se debe suspender o no la marca.



6.5. Proceso de Acreditación inicial

Para solicitar la acreditación, la entidad deberá seguir el proceso establecido por la ENAC y aportar la información que ésta establezca (toda la información está disponible en la web www.enac.es).

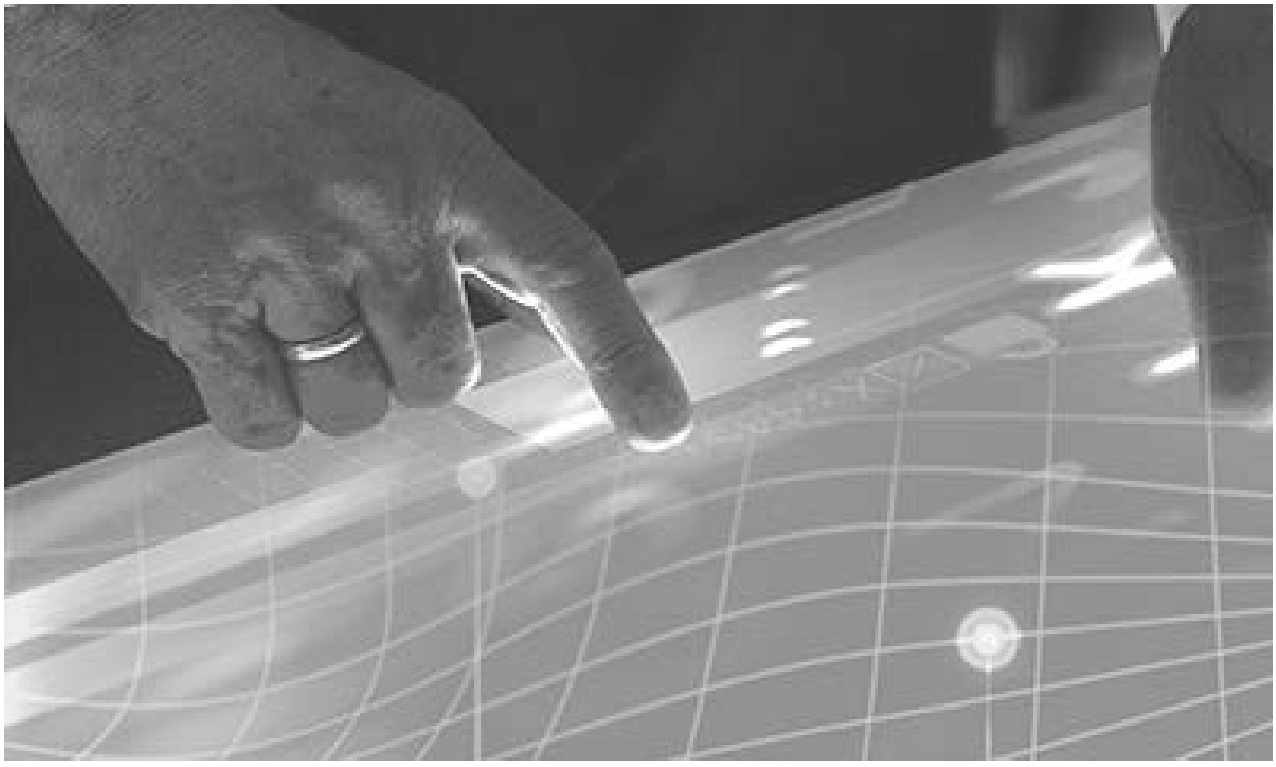
Adicionalmente, cuando la entidad decida la utilización de una marca de certificación propia, deberá enviar a la ENAC evidencia de la aceptación del CGE de dicha marca propia, acuse de recibo y copia de la declaración responsable indicada en 6.3.

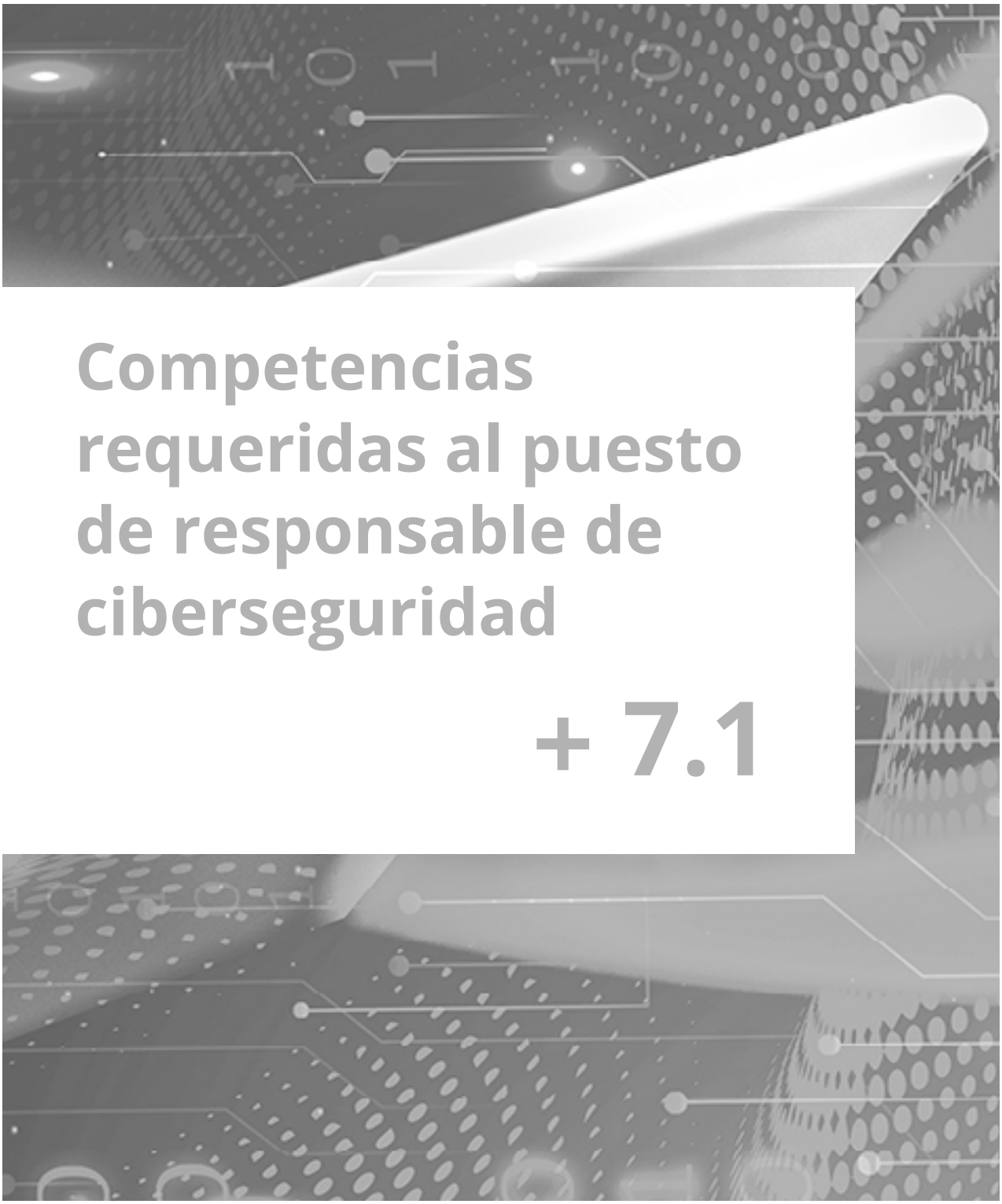
Proceso de certificación para responsables de ciberseguridad

+ 07.

Sobre las entidades de certificación que operan en el Esquema

El Esquema Nacional de Certificación de RCSEG establece los requisitos de competencia para la persona que desempeñe o haya desempeñado de forma constatada el puesto de Responsable de Ciberseguridad, así como los criterios para evaluar tales competencias por parte de los aspirantes, de manera que, cuando el resultado de tal proceso de evaluación sea satisfactorio, la EC pueda emitir el correspondiente Certificado.





Competencias requeridas al puesto de responsable de ciberseguridad

+ 7.1

El RCSEG deberá reunir conocimientos especializados de ciberseguridad, así como experiencia práctica en materia de seguridad de la información y, en su caso, protección de datos.

Asimismo, debe conocer el ENS, la Directiva NIS y su transposición al ordenamiento jurídico español, la LPIC, incluyendo las normativas derivadas o de desarrollo de dichas regulaciones, así como aquella normativa que resulte de aplicación.

No obstante, se han identificado aquellos conocimientos, habilidades y destrezas necesarias que debe poseer la persona que desee obtener el correspondiente Certificado para llevar a cabo cada una de las funciones propias de la posición de RCSEG.

Las **competencias genéricas del RCSEG** se pueden concretar en las siguientes capacidades, clasificadas por áreas:

Figura 3. Áreas de competencias del Responsable de Ciberseguridad.

Prevención y asesoramiento

- **Habilidad y competencias** tanto para **elaborar y presentar para su aprobación la Estrategia de Ciberseguridad**, como para **elaborar y defender los presupuestos** para su ámbito de responsabilidad.

- **Habilidad y competencias** para **relacionarse con la Alta Dirección proporcionando la información de avances, riesgos y prioridades**, así como de **cualquier otra información relevante** que se requiera para evaluar la situación, tomar decisiones o apoyar en las mismas.

- Habilidad y competencias para **relacionarse con las Fuerzas y Cuerpos de Seguridad del Estado**, así como otras terceras partes relevantes en esta materia.

- Habilidad y competencias para promover y/o **impartir la formación, instrucción, capacitación, concienciación y sensibilización** en materia de ciberseguridad.

- Capacidad y disposición para **asesorar en materia de ciberseguridad a los Responsables de los Servicios** y a los **Responsables de la Información de las organizaciones**. Así como a la Dirección y, en general, a las Partes Interesadas, como proveedores en la cadena de suministro.

- Capacidad para **relacionar la naturaleza y contexto de los Servicios con los riesgos de ciberseguridad inherentes a su actividad**, para poder desarrollar una estrategia de ciberseguridad que sea consecuente con los mismos.

- Facultades de convicción para **asesorar al Responsable del Sistema en materia de ciberseguridad** y **consensuar con él las medidas de seguridad más adecuadas** para los sistemas de información concernidos.

- Capacidad y compromiso para **responsabilizarse de la determinación de la Declaración de Aplicabilidad**, como muestra de conformidad para impulsar y supervisar todas las medidas de seguridad que resulten de aplicación.

- Capacidad para **elaborar o supervisar la elaboración, de políticas, normas y procedimientos internos** relacionados con la seguridad de los sistemas de información que soportan los servicios y la información que éstos manejan.

- Capacidad para **elaborar y supervisar** los **planes de contingencia y la formación**.

» Cuando resulte aplicable, **tener conocimientos para asesorar respecto a las medidas necesarias de protección de datos**, de conformidad con lo señalado en la Disposición adicional primera de la Ley Orgánica 3/2018.

» **Competencia para estar al corriente**, **conocer** e **interpretar adecuadamente la normativa jurídica y de cumplimiento** que se vaya promulgando o modificando, relacionada con la ciberseguridad, asesorando asimismo en su aplicación a la organización.

» **Capacidad de organización y análisis para clasificar e interpretar**, respecto a la organización donde presta sus servicios, **las diferentes guías que publique el CCN y otras organizaciones**, así como los demás actores involucrados en la ciberseguridad.

Supervisión

» **Conocimientos y experiencia para supervisar la gestión de la ciberseguridad**, apoyándose, si fuera preciso, en terceros, internos o externos, en función de las exigencias de la organización, asumiendo la coordinación global.

» **Compromiso de colaboración con las demás líneas de defensa**: Auditoría Interna y Externa, así como con las áreas operativas.

» **Conocimiento de las buenas prácticas y estándares internacionales** y capacidad para **supervisar el cumplimiento de los mismos**.

» **Capacidad para revisar las valoraciones en las cinco (5) dimensiones de la seguridad de los servicios y de la información** que estos manejan, efectuadas por sus Responsables, asesorándolos con criterio respecto a las mismas.

» **Compromiso para participar en los diferentes procesos de adquisición de nuevos componentes** para la organización, tanto hardware como software o servicios, verificando que cumplan con los criterios de seguridad establecidos.

» **Compromiso para supervisar**, junto al Responsable del Sistema, **que a los nuevos componentes se les apliquen los criterios de bastionado establecidos por la organización o el fabricante**, bajo el principio de seguridad por defecto, diseño y definición.

» **Compromiso para verificar**, junto al Responsable del Sistema, **que se efectúe el mantenimiento** (gestión de versiones, análisis de vulnerabilidades y aplicación de parches de seguridad) **de los componentes del sistema**, así como su mantenimiento de hardware.

- **Capacidad para elaborar o supervisar las diferentes métricas e indicadores** relacionados con la seguridad.

- **Capacidad para supervisar a los proveedores** en los que se han externalizado servicios, en base a los informes facilitados.

- **Conocimientos del contexto de la organización y de sus planes de continuidad** para verificar los mismos y supervisar sus pruebas, siempre que se consideren necesarios según las circunstancias de la organización y sus sistemas de información.

- **Capacidad y conocimientos para supervisar las medidas de seguridad física y de protección de las infraestructuras** TIC en los CPD y demás dependencias, verificando las inspecciones preceptivas, colaborando activamente con Seguridad Corporativa / Física y con Servicios Generales y Prevención de Riesgos Laborales.

- **Conocimientos para supervisar** con los Departamentos de Recursos Humanos y/o Compras **los acuerdos de confidencialidad de los empleados** de la organización y de **los colaboradores externos**.

- **Capacidad para estudiar los contratos y acuerdos de prestación de servicio de proveedores externos**, como pueden ser prestadores de servicios de nube, verificando que sean acordes con los requisitos de seguridad de la organización y de los sistemas de información que se apoyen en ellos.

- **Compromiso para participar en la aprobación de los cambios en el sistema** que puedan tener implicaciones respecto a la seguridad, así como de los requisitos de seguridad de nuevos desarrollos, bajo el principio de seguridad desde el diseño, por defecto y por definición.

Identificación

» **Capacidad para identificar**, en colaboración con los Responsables de los Servicios y la Información, **los posibles riesgos de seguridad, calcular su valor y consensuar las acciones de mitigación** para aquellos que se consideren inaceptables en base al umbral de riesgo establecido en la organización.

» **Capacidad para dirigir y gestionar la realización de las sucesivas nuevas iteraciones** del análisis de riesgos.

» **Capacidad para participar en la revisión del Análisis de Impacto al Negocio (BIA)**, al menos anualmente, y siempre que se desarrollen e incorporen servicios nuevos o le sea requerido por el responsable de continuidad.

Detección

» **Capacidad para estar al corriente y gestionar los diferentes incidentes** de seguridad que se produzcan en la organización.

» **Capacidad para analizar el impacto ocasionado** por un determinado ciberincidente.

» **Capacidad para estar al corriente y gestionar los informes procedentes de controles y amenazas**, verificando la idoneidad de la protección y su ajuste, en caso de ser necesario.

» **Capacidad para analizar y gestionar los informes sobre la actividad de los usuarios**, a ser posible apoyándose en herramientas automatizadas, con el objetivo de detectar conductas sospechosas.

» **Capacidad de colaboración con el DPD**, en caso de que se produzca una violación de datos personales, según dispone el art. 33 del RGPD.

Respuesta y recuperación

» **Capacidad para diseñar y probar los planes de respuesta** ante incidentes de ciberseguridad.

» **Compromiso para notificar al CSIRT de referencia** y, en su caso, a la Autoridad de Control de Protección de Datos y al resto de entidades competencialmente habilitadas para ello, los **incidentes relevantes** y **brechas de seguridad**.

» **Capacidad para coordinar la respuesta ante una crisis de ciberseguridad**, incluyendo la coordinación con el CSIRT de referencia hasta su resolución y su vuelta a la normalidad.

» **Capacidad para interpretar informes forenses**, reflexionar sobre las lecciones aprendidas, **definir planes de acción** y **hacer seguimiento** de su aplicación.

Coordinación y seguimiento

» **Compromiso para responsabilizarse del seguimiento de las decisiones adoptadas** por el Comité de Seguridad, habitualmente, en calidad de Secretario de dicho Comité.

» **Capacidad de decisión para convocar reuniones extraordinarias** del Comité de Seguridad, cuando así lo aconsejen las circunstancias.

Además de las capacidades señaladas en los párrafos anteriores, **la Secretaría de Estado de Seguridad del Ministerio del Interior**, como autoridad competente y para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales que sean designados operadores críticos conforme a la Ley 8/2011, de 28 de abril, según el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, y aquellos otros cuyas competencias le hayan sido conferidas en virtud del Real Decreto 43/2021, de 26 de enero, **podrá establecer obligaciones específicas adicionales del Responsable de Seguridad para este tipo de entidades**.

La Secretaría de Estado de Seguridad del Ministerio del Interior, como autoridad competente y para garantizar la seguridad de las redes y sistemas de información, podrá establecer obligaciones específicas adicionales del Responsable de Seguridad para este tipo de entidades.

Modos de acceso a la Certificación de RCSEG

+ 7.2

Se establecen dos (2) modos de acceso a la certificación de RCSEG:

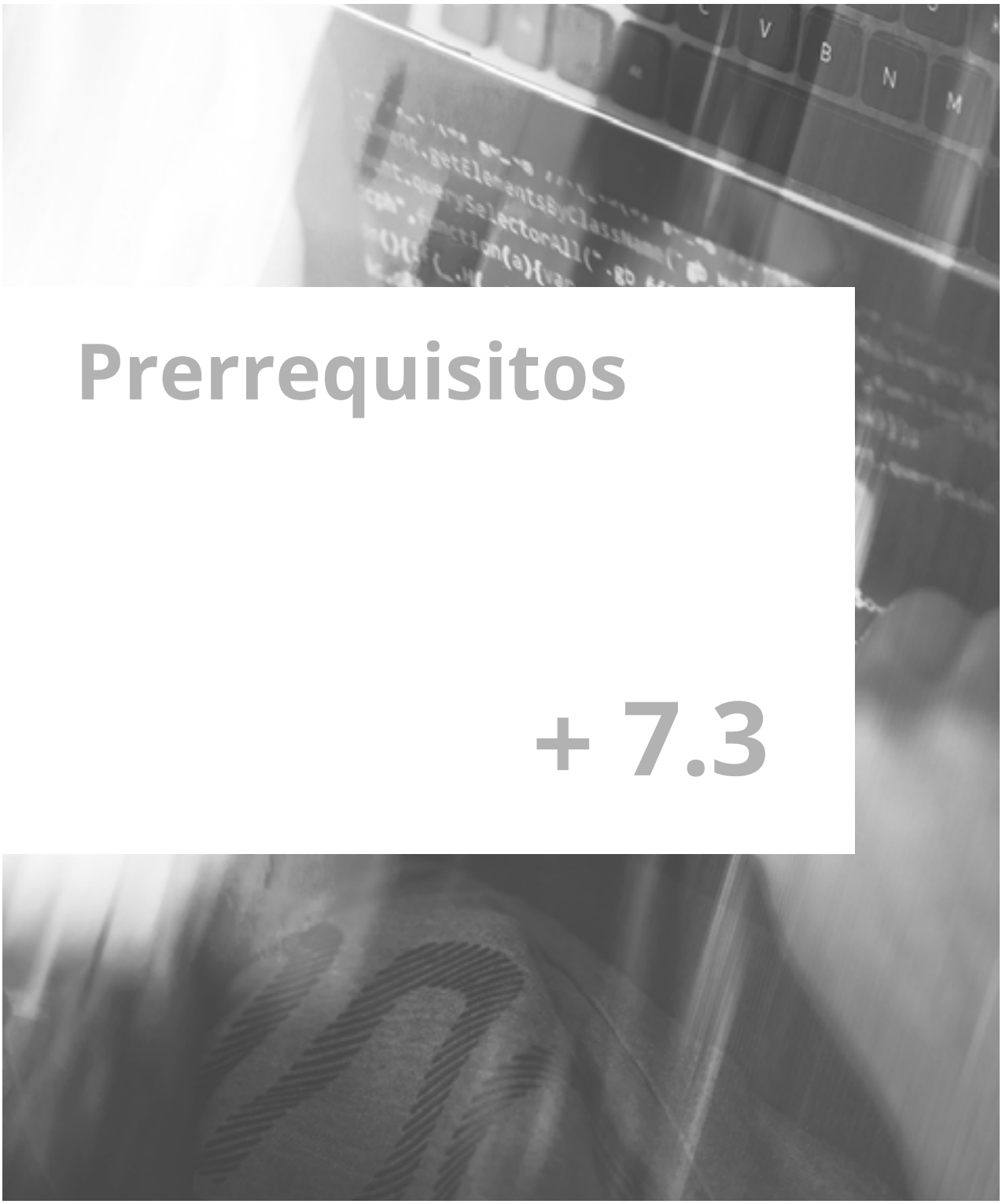
Modo 1

Certificación dirigida a profesionales con más de 15 años de experiencia continuada en las áreas competenciales cubiertas por el Esquema.

Modo 2

Certificación dirigida al resto de profesionales.

A cada modo de acceso le corresponde un **proceso de evaluación específico**, de acuerdo con lo descrito más adelante.



Prerrequisitos

+ 7.3

Para acceder a la fase de evaluación de la idoneidad para alcanzar la Certificación, será necesario estar en posesión de titulación académica en áreas TIC, que deberá ser:

- **Titulación de nivel 1 o superior** dentro del Marco Español de Cualificaciones para la Educación Superior (MECES) para el Modo de Acceso 1.

- **Titulación universitaria equivalente o superior a grado universitario** (en áreas TIC) para el Modo de Acceso 2.

Adicionalmente se deberá justificar, al menos, el cumplimiento de uno de los siguientes prerrequisitos:

- **Para el Modo de Acceso 1:** justificar una experiencia profesional regular y continuada de, al menos, quince (15) años en proyectos y/o actividades y tareas relacionadas con las funciones del RCSEG.

- **Para el Modo de Acceso 2:**

  - **Justificar una experiencia profesional regular y continuada** de, al menos, **cinco (5) años** en proyectos y/o actividades y tareas **relacionadas con las funciones del RCSEG**.

  - **Justificar una experiencia profesional regular y continuada** de, al menos, **tres (3) años en proyectos y/o actividades y tareas** relacionadas con las **funciones del RCSEG**, y una **formación mínima de 150 horas**[3] en relación con las materias incluidas en el **programa del Esquema**.

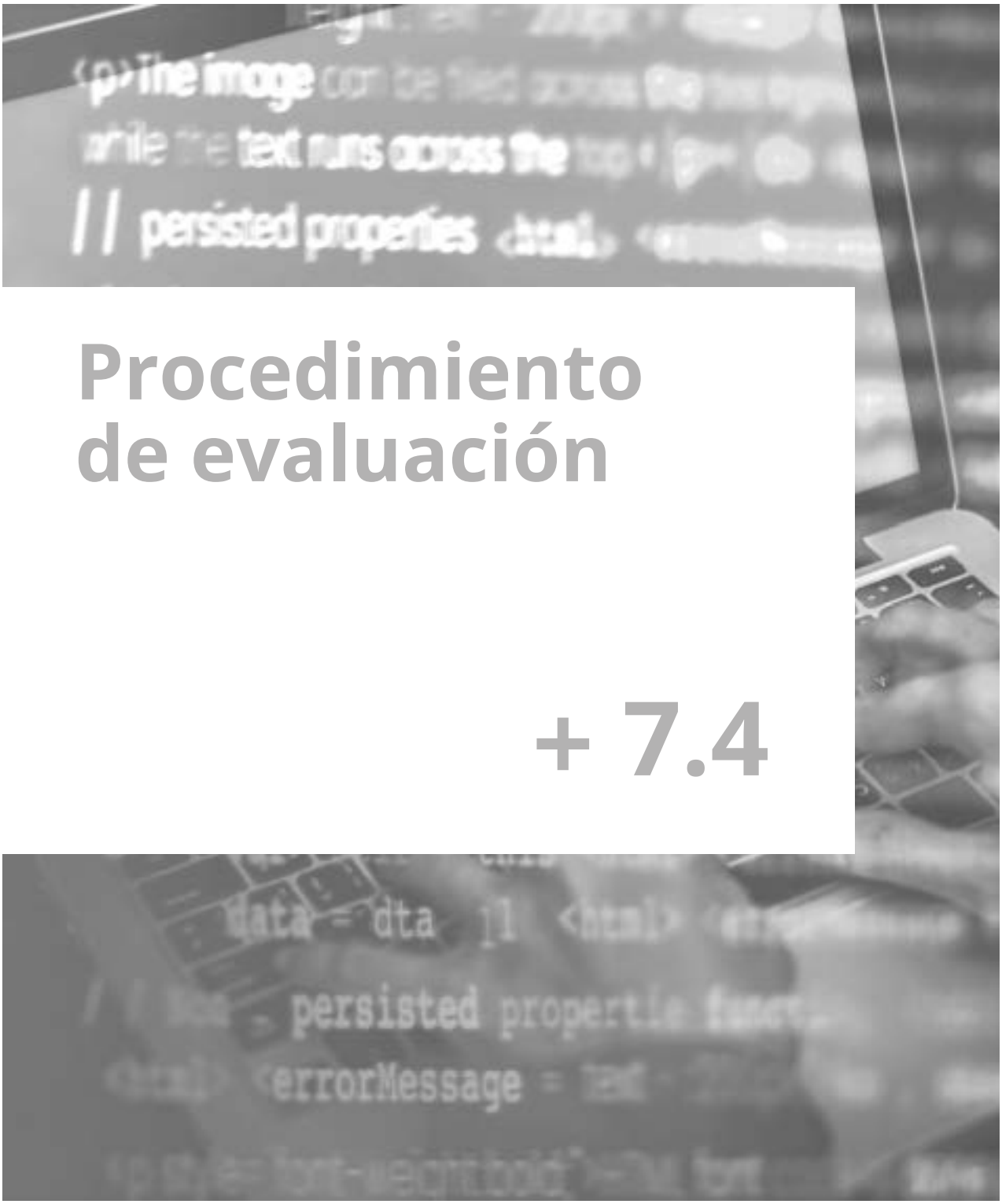
  - **Justificar una experiencia profesional regular y continuada** de, al menos, dos **(2) años en proyectos y/o actividades y tareas** relacionadas con las funciones del RCSEG, y una formación mínima de 300 horas en relación con las materias incluidas en el programa del Esquema.

  - Si no se dispone de la experiencia mínima requerida, será necesario justificar una **formación mínima de 600 horas en relación con las materias incluidas en el programa** del Esquema. En este supuesto, una vez justificada la formación y aprobado el examen, se deberán acreditar, en un período máximo de (5) años, (3) años de experiencia para poder emitir el certificado.

[3] Equivalencias crédito-horas: se establece que un (1) crédito corresponde a diez (10) horas lectivas.

- El Reglamento del Esquema Nacional de Certificación de RCSEG que, a tales efectos, desarrollará el CGE y, en su caso, aprobará el CE, determinará en qué medida podrá valorarse como experiencia que el solicitante posea certificaciones profesionales en materia de auditoría, seguridad, gobierno y/o gestión de riesgos de las TIC proporcionadas por organismos académicos o entidades de reconocido prestigio.

- El Reglamento del Esquema Nacional de Certificación de RCSEG desarrollará cómo se concretará la experiencia profesional a la que se refieren los citados prerrequisitos; y las exigencias en relación con las evidencias documentales, que serán evaluadas por la Entidad de Certificación, y que deberá aportar el solicitante para justificar el modo de acceso. El resultado será comunicado al solicitante.



Procedimiento de evaluación

+ 7.4

El proceso de evaluación está basado tanto en la valoración del conocimiento y experiencia como en el desarrollo profesional.

El proceso de evaluación podrá estar basado en una valoración de competencias que incluya:

Conocimiento

Preguntas teóricas de **tipo test**.

Habilidad

Preguntas prácticas con simulaciones avanzadas y realización de ejercicios sobre laboratorios o plataformas de *cyber-ranges*.

Actitud

Análisis cuantitativo y cualitativo de las distintas posibilidades de realizar correctamente las preguntas y ejercicios de habilidad.

A través de las correspondientes **pruebas de evaluación**, el **candidato deberá evidenciar que posee la competencia adecuada** (experiencia y capacitación, esencialmente); es decir, los conocimientos teóricos, la capacidad profesional y las habilidades personales necesarias para llevar a cabo las funciones correspondientes a la actividad de Responsable de Ciberseguridad (RCSEG), en los términos y condiciones establecidos por el presente Esquema de certificación.

7.4.1. Modo de Acceso 1

Aquellos candidatos que justifiquen documentalmente una experiencia continuada de al menos quince (15) años en actividades relacionadas con la ciberseguridad, la seguridad de la información o responsabilidades conexas, serán evaluados por un Tribunal de Evaluación Específico.

Dicho Tribunal será convocado por la EC con el asesoramiento del CE y estará compuesto por **un representante de cada uno de los miembros del CE**. A su propuesta, podrán estar presentes otros especialistas de los sectores público, privado o académico, con voz, pero sin voto; y que, evaluará la idoneidad y adecuación de las aportaciones documentales presentadas por el candidato que le hayan sido requeridas.

Una vez la documentación presentada por el solicitante se ha considerado satisfactoria, la evaluación presencial consistirá en la defensa por parte del candidato, durante un tiempo no superior a una hora, de un Programa detallado para el análisis, la implantación y el mantenimiento de la ciberseguridad de un sistema de información. Será según la elección del candidato, de suficiente significación y complejidad, para posibilitar que los miembros de Tribunal evalúen los conocimientos teóricos y las capacidades prácticas del candidato, formulando preguntas, cuestiones o aclaraciones sobre lo presentado.

Una vez concluida la defensa y satisfechas las preguntas, el Tribunal, tras la oportuna deliberación, se pronunciará sobre la superación o no de la prueba de competencia por parte del candidato, informando de ello a la EC y remitiéndole la totalidad de los registros de la prueba para que continúe el proceso de certificación como RCSEG.

7.4.2. Modo de Acceso 2

La evaluación de los conocimientos y capacidades técnicas o profesionales se llevará a cabo mediante la realización de dos (2) pruebas independientes, teniendo en cuenta que:

- La evaluación versará sobre los **temas relativos a los conocimientos específicos indicados en el programa** del Esquema, detallado en el Reglamento del Esquema Nacional de Certificación de RCSEG.

- Es requisito para la obtención del Certificado, la **superación de la evaluación global repartida en dos (2) pruebas**, una teórica y otra práctica. La teórica consistirá en 150 preguntas tipo test, de respuesta múltiple. La prueba práctica consistirá en un ejercicio a desarrollar por el alumno en hojas en blanco, a partir de un supuesto práctico determinado o en la realización de ejercicios sobre laboratorios o plataformas de *cyber-ranges*.

- Todos los candidatos dispondrán de **dos (2) convocatorias para cada prueba**. Entre ellas no deberán mediar más de seis (6) meses. De no superar alguna prueba, se requerirá iniciar de nuevo el proceso de solicitud, ya sea en la misma, o en otra EC.

- El Reglamento del Esquema Nacional de Certificación de RCSEG **determinará la naturaleza y el alcance de las pruebas y su valoración**, así como los derechos de los solicitantes en materia de impugnación de resultados y expedición de las Certificaciones. Se precisarán los extremos necesarios para asegurar la custodia de los enunciados de las pruebas, la preservación del anonimato de los ejercicios realizados y la independencia y neutralidad de las EC.

7.4.3. Preguntas teóricas y supuestos prácticos

7.4.3.1. Banco de preguntas centralizado

El **CE elaborará y mantendrá actualizado un banco de preguntas y supuestos prácticos suficientes** para cubrir las necesidades derivadas de la ejecución de las pruebas teóricas y prácticas que estén previstas realizar en un período de tiempo considerado.

Anualmente, el CE revisará dicho banco de preguntas y supuestos prácticos, incluyendo nuevas preguntas y supuestos, y actualizando las existentes. El objetivo es adecuar su contenido a las exigencias derivadas de las nuevas tecnologías, vulnerabilidades, amenazas, métodos de ataque, etc. y a las eventuales actualizaciones legales o normativas.

Asimismo, el CE instará a las EC a desarrollar y proponer al CE preguntas y supuestos prácticos, alineados con los dominios y contenidos del presente Esquema, con la periodicidad que decida el CGE. El CE, a través de sus representantes, aprobará o rechazará, en todo o en parte, la idoneidad de las preguntas y supuestos en base a la verificación de las mismas.

El CE adoptará las decisiones oportunas en cuanto al número de preguntas que deberán conformar el banco mencionado anteriormente, así como la periodicidad de su renovación o actualización y su alcance. El criterio empleado inicialmente para el contenido de las diferentes preguntas del banco será proporcional al peso de cada uno de los dominios en que se ha dividido la prueba teórica.

La salvaguarda de las condiciones de independencia, imparcialidad y armonización de contenidos, así como la garantía de acceso igualitario a las pruebas, exige que las EC se abstengan de hacer públicas las preguntas y supuestos prácticos que hubiesen desarrollado o a las que hubiesen tenido acceso, prohibiéndose su comercialización o puesta a disposición de cualquier modo. El incumplimiento de este precepto podría comportar la retirada de la acreditación a la EC incumplidora.

7.4.3.2. Juegos de preguntas para los exámenes

Para cada convocatoria que organicen las EC, éstas deberán notificarlo al CE, quién les proporcionará **dos (2) juegos de 150 preguntas** cada uno de modo que se asignen juegos distintos a candidatos adyacentes en el aula de examen. Cada uno de los juegos de preguntas estará constituido de forma proporcional al peso de los dominios definidos para el Esquema de Certificación de RCSEG.

Dichas preguntas **se facilitarán de una forma segura que garantice la confidencialidad de las mismas**, y pocos días antes de la fecha establecida para la convocatoria de examen.

7.4.4. Concesión del Certificado

Las EC concederán la certificación a los candidatos que satisfaciendo los requisitos de certificación hayan obtenido el resultado de "APTO", en su proceso de evaluación, ya sea ejecutado por un Tribunal constituido por el CE.

En ambos casos la EC les emitirá un Certificado justificativo, conforme al modelo que se recoge en el Reglamento del Esquema Nacional de Certificación de RCSEG, que se mantendrá vigente durante un período de tres (3) años. Tras dicho período, su titular deberá renovarlo atendiendo a lo dispuesto más adelante.

7.4.5. Mantenimiento

En el supuesto de que durante el período de validez del Certificado se produjesen cambios legales o tecnológicos que, a juicio del Comité de Gestión del Esquema (CGE), hiciesen conveniente una revisión o adaptación significativa del Certificado concedido, se podrán establecer los criterios y medidas adecuadas para mantener la vigencia de dichos certificados que, en todo caso, deberán de ser aprobadas por el Comité del Esquema (CE).

7.4.6. Renovación

La renovación del Certificado requerirá que el candidato justifique y documente adecuadamente:

- Haber participado en un **mínimo de 60 horas de formación recibida y/o impartida** durante el período de validez del Certificado, requiriéndose un mínimo anual de 20 horas en materias objeto del programa del Esquema.

  Como alternativa a la formación recibida, los profesionales certificados podrán cubrir las horas de formación requeridas mediante **su equivalencia en créditos de *Continuing Education*** (CPE y CCE). Tres (3) horas académicas de formación y/o docencia en los ámbitos de la Privacidad, la Protección de Datos de carácter personal y/o la Seguridad de la Información, equivalen a un (1) crédito de *Continuing Education*.

  Asimismo, también **se considerarán las ponencias**, así como la publicación de **artículos académicos y/o publicaciones especializadas** en los ámbitos de la Privacidad, la Protección de Datos de carácter personal y/o la Seguridad de la Información, con la equivalencia de un (1) crédito de Continuing Education. Podrán trasladarse de una anualidad a otra, un máximo de 10 créditos o 30 horas de formación y,

- Al menos, **un año de experiencia profesional continuada y regular en proyectos y/o actividades** y tareas relacionadas con las funciones del RCSEG y/o de la seguridad de la información, evidenciada por tercera parte (empleador o similar).

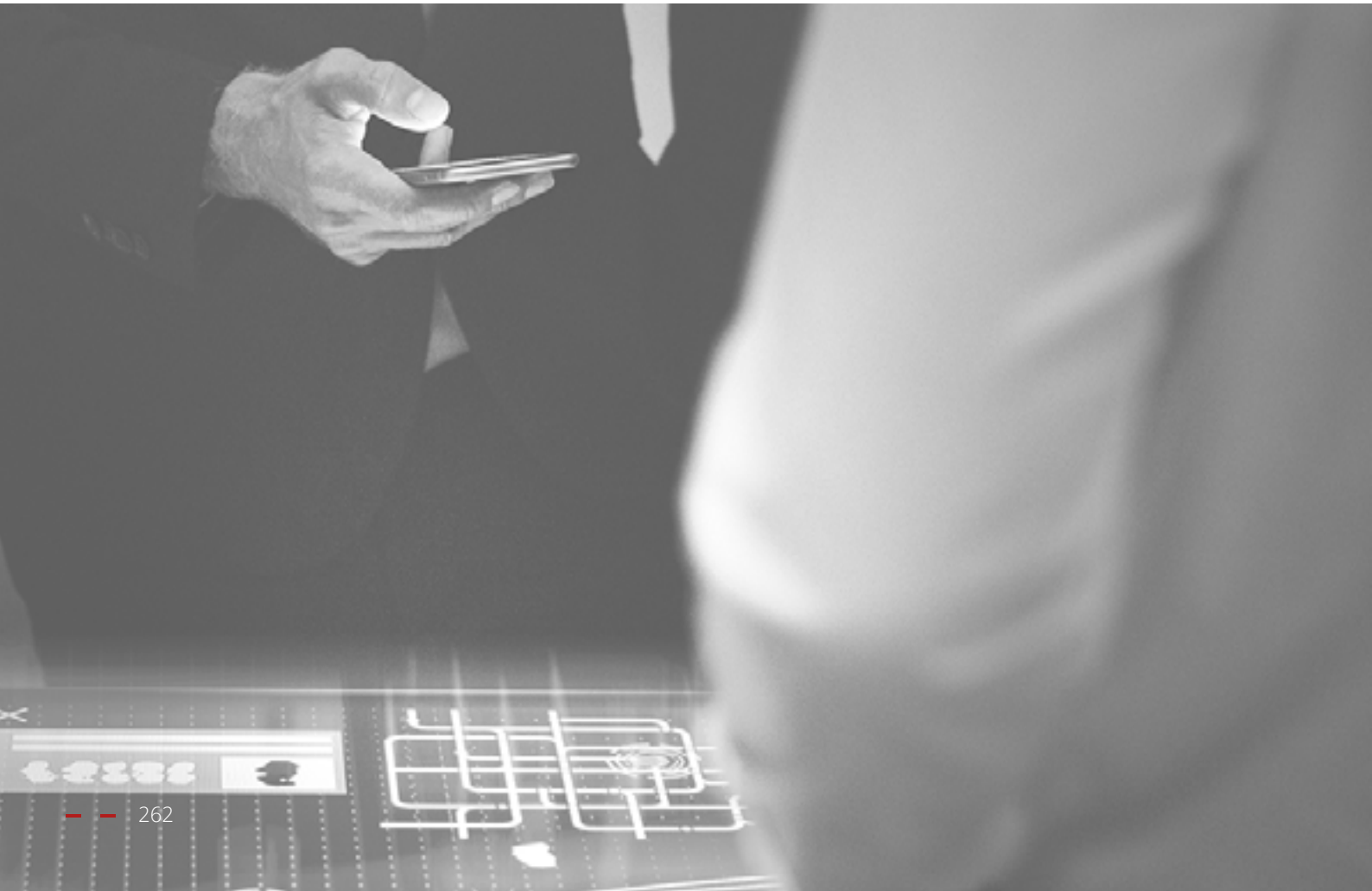
Se valorará la formación impartida con el doble de horas que la formación recibida. Para que la formación recibida se considere válida debe proporcionar una actualización demostrable de los conocimientos objeto del Esquema y sólo se tendrá en cuenta la formación recibida durante el período de vigencia de la certificación. No será válida la formación que se cursó con anterioridad para poder presentarse a los exámenes de certificación. Lo que este requisito pretende es la actualización permanente de los conocimientos de los RCSEG.

Para que el certificado correspondiente a la formación sea tomado en consideración, debe constar la entidad de formación que lo imparte y el título de la formación, fecha y número de horas, temario y formato (presencial u online). En el caso de no poder justificar la formación anual mínima requerida durante alguno de los tres (3) años exigidos, se permite la cumplimentación de esa formación en alguno de los otros dos (2) años restantes. Se considera formación la asistencia a seminarios y congresos siempre que el candidato aporte certificado con la misma información solicitada para un programa de formación.

La EC notificará a la persona certificada el final del período de validez de la certificación con una antelación mínima de tres (3) meses.

La renovación habrá de **solicitarse con anterioridad a la fecha de vencimiento del período de validez del Certificado**. La no recepción por la persona certificada de la comunicación de la EC informando del final del período de validez de la certificación, no eximirá del cumplimiento de lo indicado en este apartado.

La renovación de la certificación comportará la expedición de un nuevo Certificado por parte de la EC con el mismo número personal asignado en la primera certificación. El nuevo Certificado tendrá un **período de validez de tres (3) años** y podrá reflejar la antigüedad total de la certificación.



Suspensión o retirada de la Certificación

+ 7.5

7.5.1. Suspensión temporal o voluntaria

En el caso de que el RCSEG certificado manifieste a la EC que expidió su certificación haber dejado de cumplir los requisitos del Esquema, el Certificado dejará de estar en vigor durante un tiempo no superior a un (1) año.

Para la reactivación de su vigencia, la entidad de certificación realizará las comprobaciones oportunas encaminadas a verificar que las causas que motivaron la solicitud de suspensión han desaparecido, siempre que no haya transcurrido más de un (1) año desde la fecha de suspensión de la certificación y se justifique documentalmente que se está en condiciones de seguir utilizando el Certificado, en los términos establecidos para su renovación en el apartado anterior.

Una vez transcurrido un (1) año de suspensión del Certificado sin que haya sido posible la reactivación de su vigencia, o no hayan desaparecido las causas que motivaron la suspensión, se procederá a la retirada definitiva de la certificación, siendo necesario reiniciar el proceso íntegro a fin de obtener una nueva certificación.

7.5.2. Otros motivos de suspensión temporal

Son **motivos de suspensión de la certificación** por la EC los siguientes:

- La **no presentación** por parte de la persona certificada de RCSEG de **la documentación, registros o de cualquier información que le haya sido requerida** por la Entidad de Certificación de RCSEG para mantenerla, o para investigar una reclamación contra su actuación.

- La realización por parte de la persona de **declaraciones o usos en su condición de RCSEG certificado** que **excedan del alcance de la certificación**, sean engañosas o que, de cualquier manera, perjudiquen o desprestigien el Esquema de Certificación.

- **El uso de la Marca de certificación que haya establecido cada EC de manera no permitida o contraria a las reglas** de su uso, de forma reiterada, tras haber recibido al menos un apercibimiento formal.

- El incumplimiento por la persona certificada de **cualquiera otra de las reglas del Esquema que le afecten**.

Cualquiera de estos incumplimientos podrá dar lugar a la suspensión temporal de la certificación por un período máximo de seis (6) meses. La acumulación de tres (3) incumplimientos podrá suponer la suspensión de la certificación por un período entre seis (6) meses y la mitad del ciclo de vigencia de la certificación, procediendo a su retirada en caso de superar el plazo de vigencia.

7.5.3. Retirada de la certificación

Los motivos de retirada de una certificación ya emitida son los siguientes:

- **Cualquiera de los identificados anteriormente para la suspensión temporal**, en función de su gravedad o su reiteración, como la reiteración en un tipo concreto de incumplimiento que hubiera dado lugar a una suspensión temporal, que implique que no se ha corregido la conducta del RCSEG.
- La **acumulación de más de tres (3) sanciones de suspensión** de la certificación.
- **Ignorar deliberadamente un comunicado de suspensión temporal** y continuar haciendo uso del Certificado como RCSEG, o manifestar a terceros su condición como persona certificada mientras dure dicha suspensión.

Ante la retirada de la certificación, el interesado **deberá destruir o devolver a la EC todas las copias en su poder de la misma**, así como eliminar su mención o referencia en la documentación que elabore a partir de la fecha en que le ha sido notificada.

Los interesados a los que las EC les haya retirado la certificación y deseen obtenerla de nuevo **deberán someterse a un proceso de certificación inicial completo**.

Las EC podrán requerir a estas personas para que, previamente a someterse a la evaluación, evidencien haber subsanado las causas que llevaron a la retirada del certificado anterior sin que ello pueda ser considerado como trato discriminatorio.

Las EC se reservarán el derecho a aceptar una nueva solicitud por parte del profesional sancionado, pudiendo elevar, si lo estiman necesario, consulta previa al Comité de Gestión del Esquema (CGE).

Derechos y obligaciones de los RCSEG certificados

+ 7.6

7.6.1. Derechos

Los titulares de los Certificados tendrán derecho a:

- **Hacer uso de los Certificados** en el desarrollo de su actividad profesional.
- **Beneficiarse de cuantas actividades de divulgación y promoción** lleve a cabo la Entidad de Certificación en relación a los RCSEG certificados.
- **Hacer uso de la Marca de Certificación** que, en relación con el presente Esquema, haya establecido cada EC, que se desarrolla en el Reglamento del Esquema Nacional de Certificación de RCSEG.
- **Reclamar y recurrir cualquier decisión** desfavorable.

7.6.2. Obligaciones

Los titulares de los certificados estarán obligados a:

» **Respetar el Esquema de Certificación de RCSEG** y **todos los procedimientos** aplicables.

» **Cumplir con las obligaciones económicas** derivadas de la certificación.

» **Actuar en su ámbito profesional con la debida competencia técnica**, velando por el mantenimiento del prestigio de la certificación concedida.

» **Colaborar** con la Entidad de Certificación de RCSEG **en las actividades de supervisión de su actuación** necesarias para el mantenimiento y renovación de la certificación.

» **Informar** a la Entidad de Certificación de RCSEG **sobre cualquier situación profesional que pudiera afectar al alcance de la certificación** concedida.

» Informar a la Entidad de Certificación de RCSEG, sin demora, **sobre cuestiones que puedan afectarle** para continuar cumpliendo los requisitos de certificación.

» **No usar el Certificado del Esquema para fines diferentes** que no sean los derivados de la realización de actividades dentro del alcance de la certificación concedida.

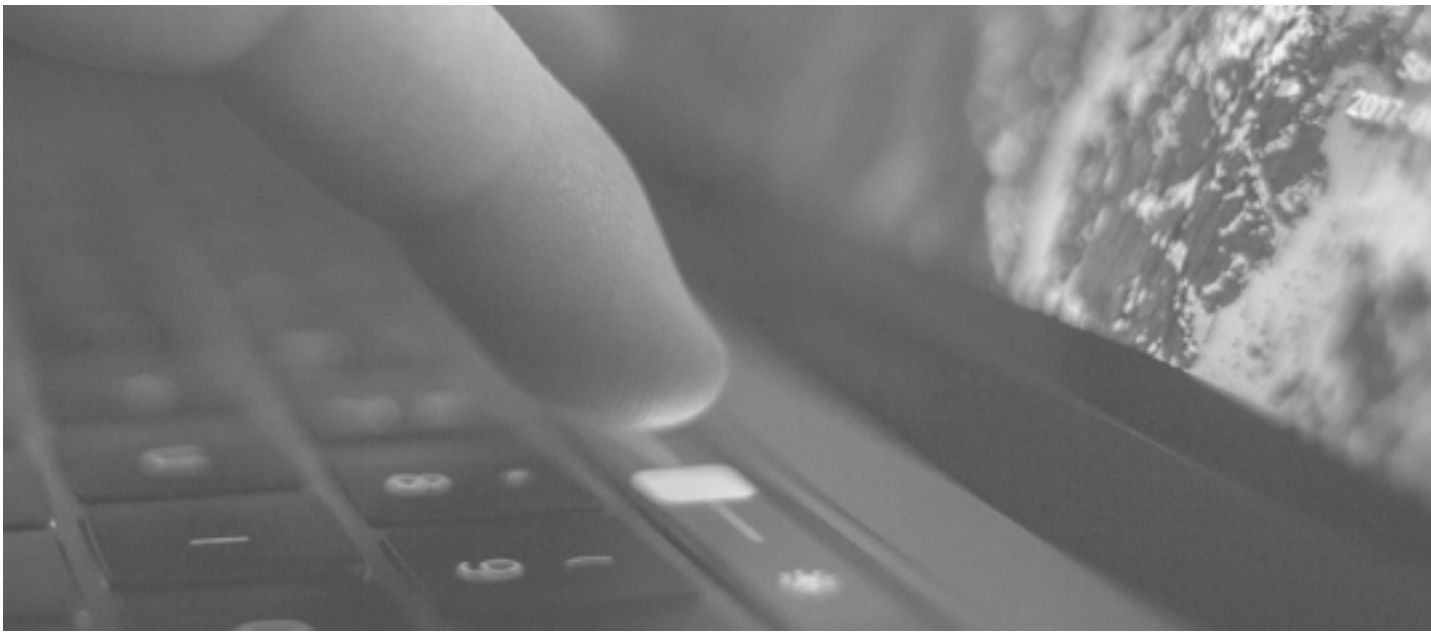
» **No realizar acciones lesivas**, de cualquier naturaleza, ni dañar la imagen y/o los intereses de las personas, empresas, entidades y clientes, incluso potenciales, interesados en la prestación profesional, ni tampoco la del presente Esquema o de las Entidades de Certificación de RCSEG.

» **No tomar parte en prácticas fraudulentas** relativas a la sustracción y/o divulgación del material de examen.

» **Mantener un registro de reclamaciones recibidas** en relación con el alcance de la certificación obtenida.

El incumplimiento de las obligaciones descritas supondrá el inicio del proceso de suspensión o retirada del certificado.

El incumplimiento de las obligaciones descritas supondrá el inicio del proceso de suspensión o retirada del certificado.

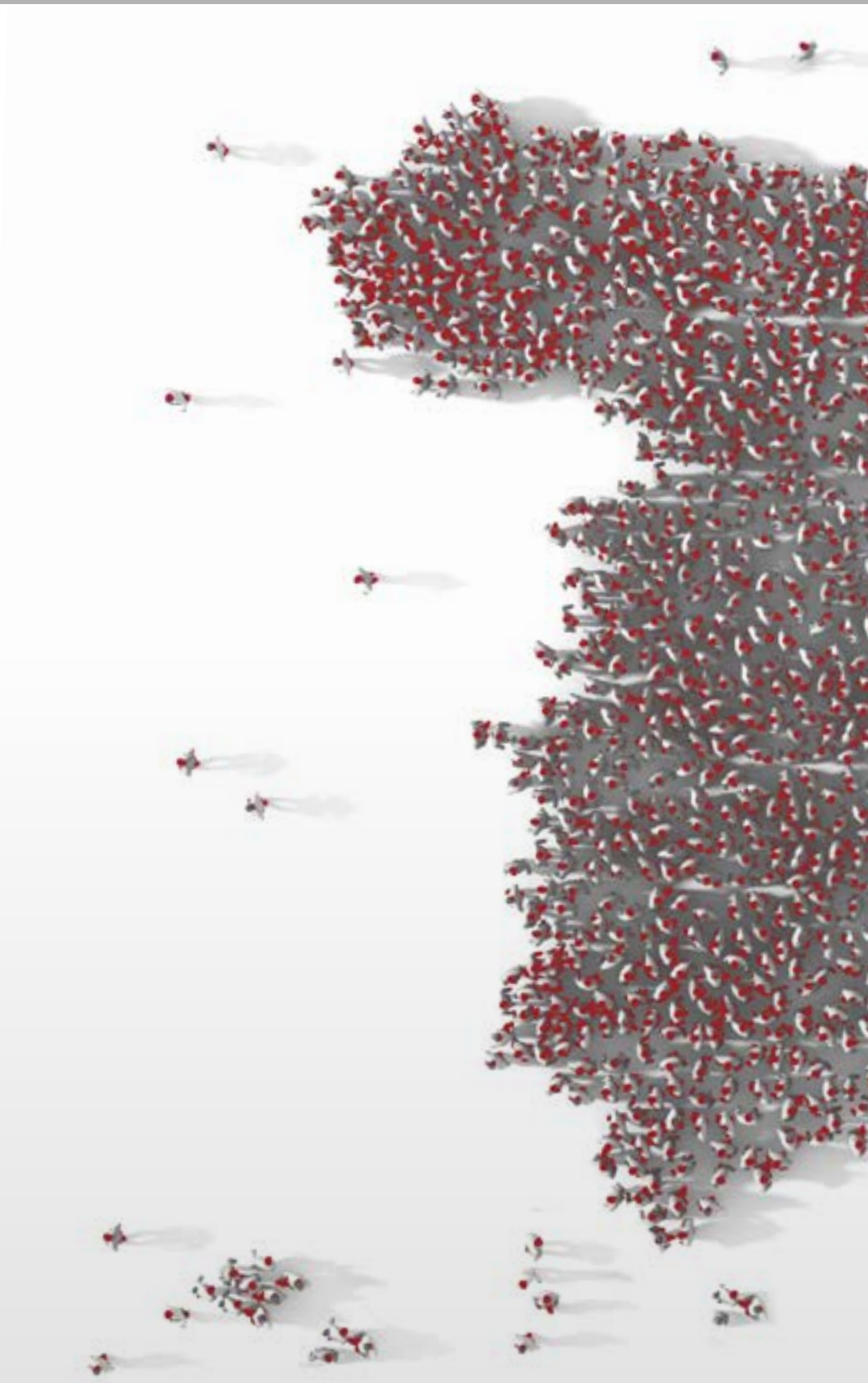


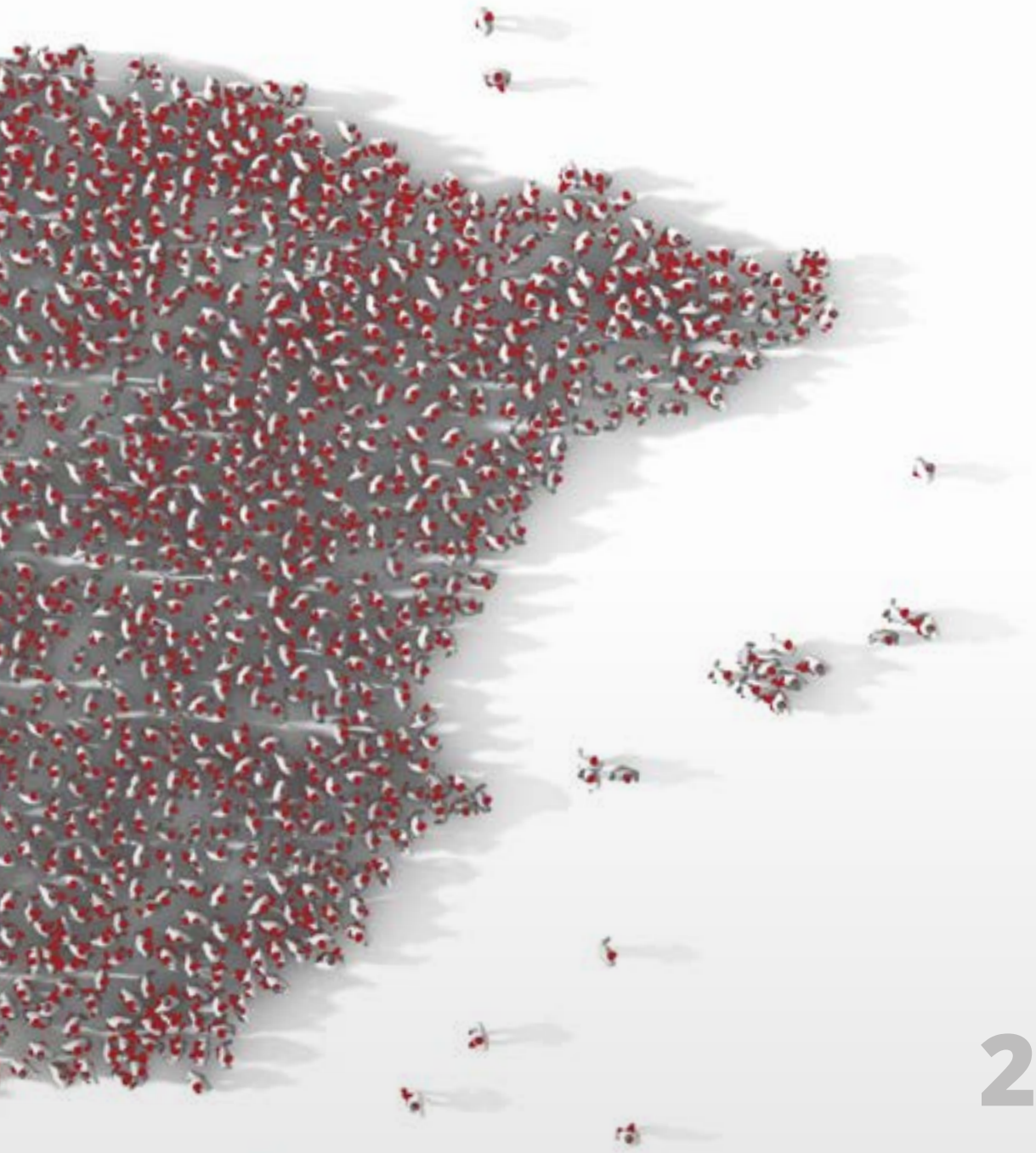
7.6.3. Información sobre RCSEG certificados

Las EC mantendrán un registro actualizado de los RCSEG certificados que incluirá: nombre y apellidos, número de certificado, fecha de concesión inicial, fecha de la última renovación (si es el caso), fecha de caducidad y estado del Certificado (concedido, suspendido, retirado, renovado).

Las EC publicarán en su web, previa información y consentimiento del interesado, la información contenida en dicho registro.

El CE, asesorado por el CGE, podrá decidir en cualquier momento sobre la conveniencia de mantener un registro público centralizado de los RCSEG certificados, que se nutrirá a partir de información que deberán proporcionarle las EC en la forma y plazo que se determine.





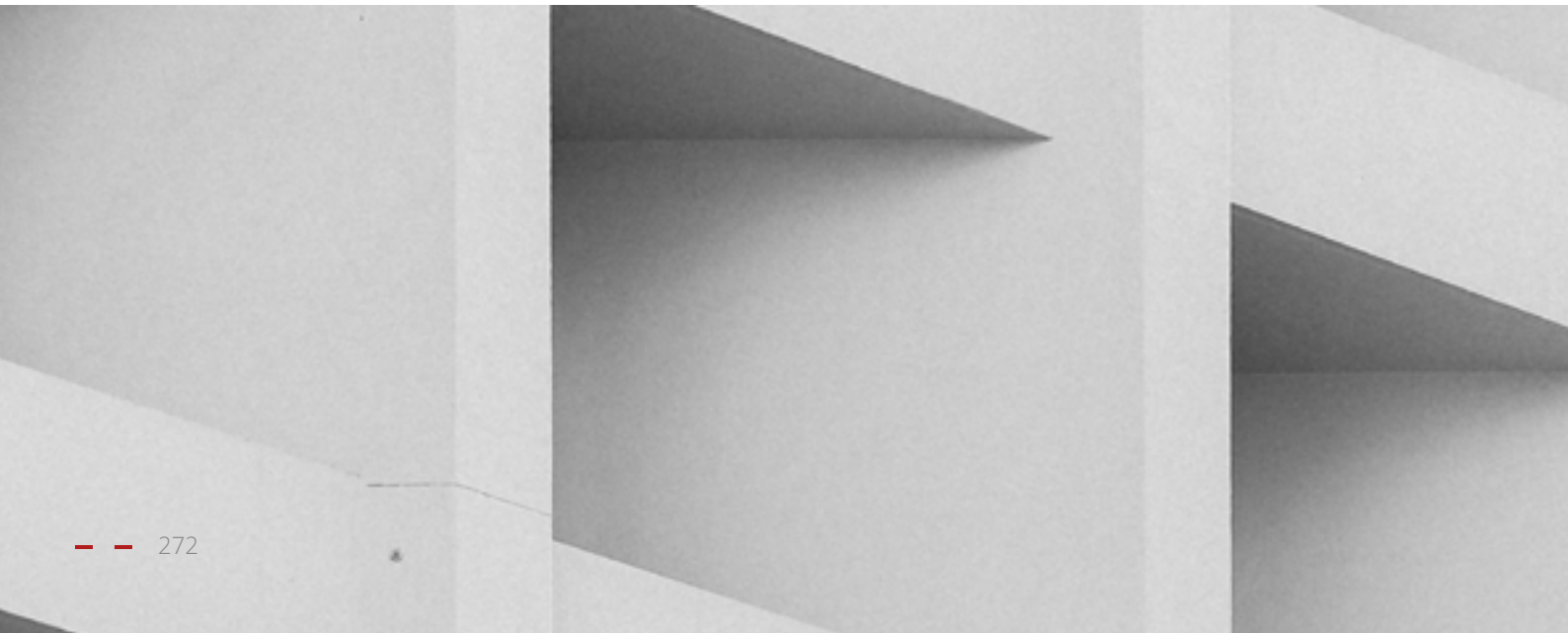
2021

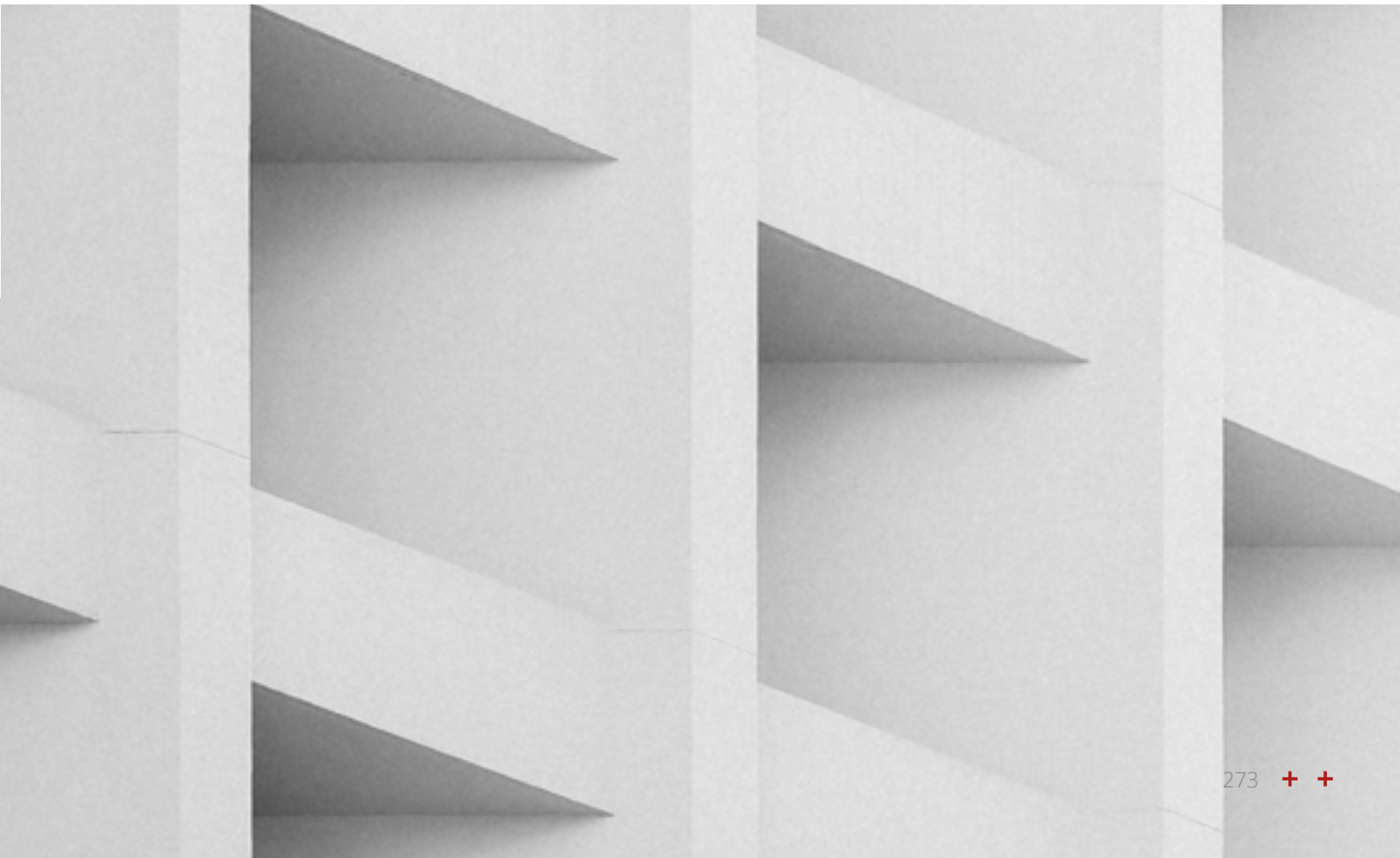
REGLAMENTO DE ESQUEMA NACIONAL DE CERTIFICACIÓN DE RCSEG

FORO NACIONAL DE CIBERSEGURIDAD

Índice

+ Reglamento de Esquema Nacional de Certificación de RCSEG





Acrónimos y terminología

+ 01.

Acrónimos y terminología

/// AEPD	Agencia Española de Protección de Datos.
/// CCN	Centro Criptológico Nacional.
/// CE	Comité del Esquema.
/// CGE	Comité de Gestión del Esquema.
/// CNPIC	Centro Nacional de Protección de Infraestructuras Críticas
/// CSIRT	Computer Security Incident Response Team: Equipo de Respuesta ante Incidencias de Seguridad Informáticas.
/// DPD	Delegado de Protección de Datos.
/// EC	Entidad de Certificación de Responsables de Ciberseguridad o Entidad de Certificación de RCSEG.
/// ENAC	Entidad Nacional de Acreditación.
/// ENS	Esquema Nacional de Seguridad.
/// Esquema de Certificación de RCSEG	Esquema Nacional de Certificación de Responsables de Ciberseguridad.
/// OCC	Oficina de Coordinación de Ciberseguridad.
/// RCSEG	Responsable de Ciberseguridad.
/// SGAD	Secretaría General de Administración Digital.


data-track="click.searchFilters.sort
Meest relevant
<span class="label-selectable-pill hidden-md
</button>

<li class="js_close-drawer">
<button title="Nieuwe inhoud"
class="btn btn-link navbar-btn js_search-filter-sort"
data-val="newest"
data-track="click.searchFilters.sort-recent"
Nieuwe inhoud
<span class="label-selectable-pill hidden-md
</button>

<input type="hidden" name="sort" value="popular" />

<ul class="nav navbar-nav">
<li class="js_close-drawer close-drawer
<button class="btn btn-link navbar-btn dropdown-toggle
<li class="filter-horizontal">
<ul class="filter-content nav buttonize
<li class="js_close-drawer">
title="Meest relevant"
navbar-btn js_search-filter-sort


// persisted properties
<html> <body style="
<html> text - :200px;
<errorMessage
style="color:orange
function
persisted
errorMessage

Objeto

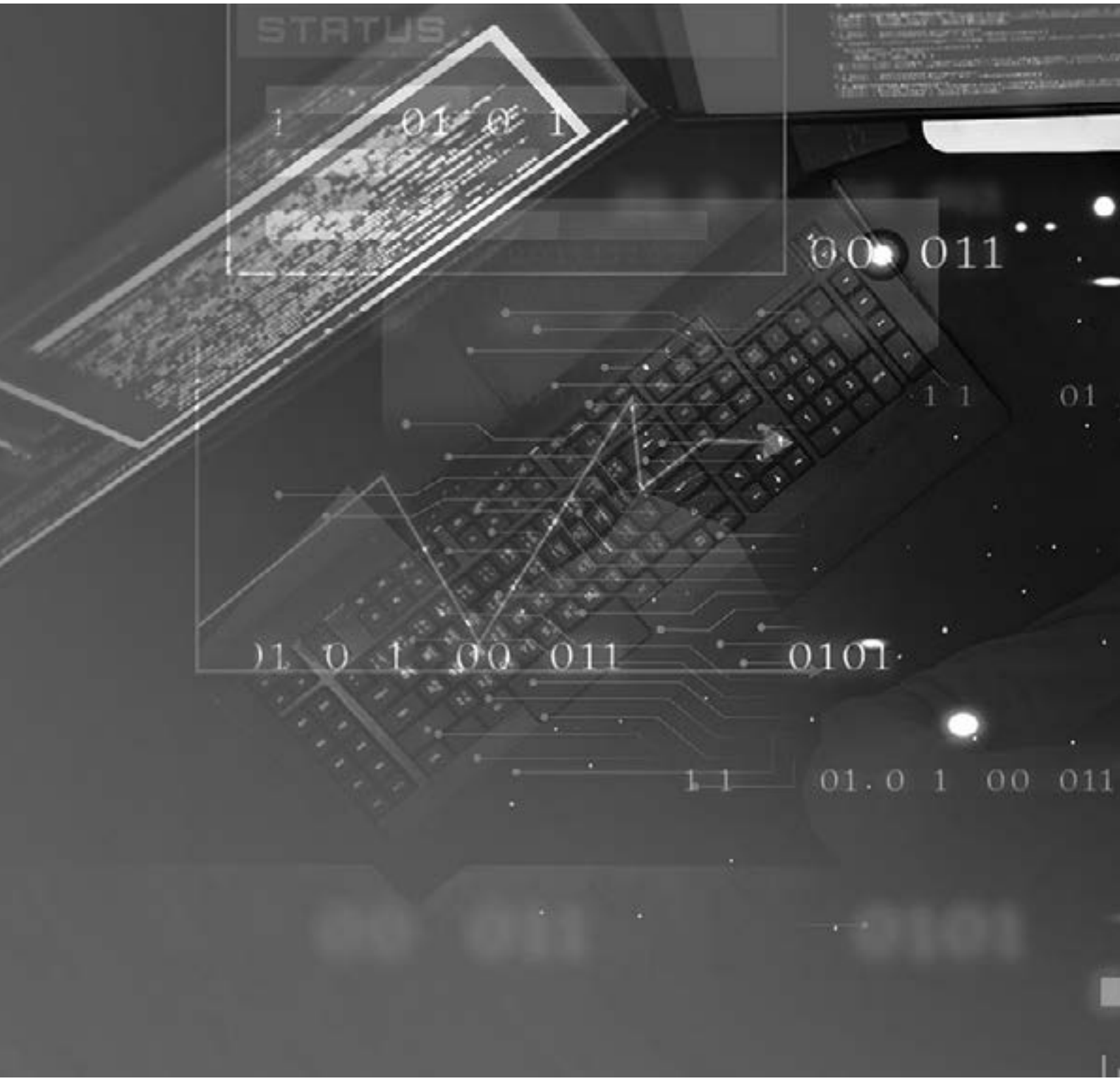
+ 02.

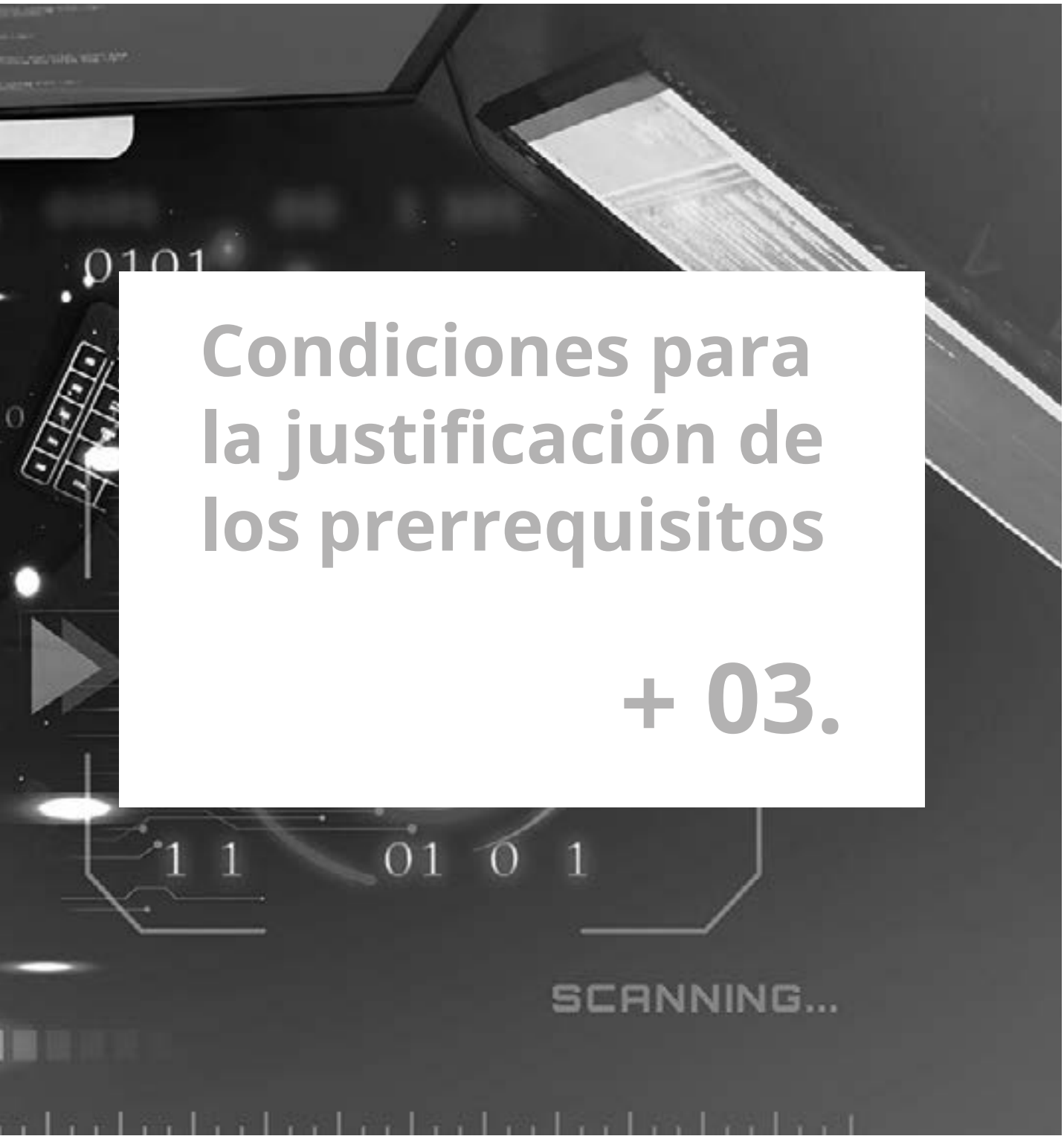
Objeto

El objeto de este documento [ENCRCSEG-02] es establecer el Reglamento del Esquema Nacional de Certificación de RCSEG referenciado en el documento principal del Esquema Nacional de Certificación de Responsables de Ciberseguridad (RCSEG) [ENCRCSEG-01], que regula las condiciones y requisitos que conforman el funcionamiento de dicho Esquema, cuyo referencial de evaluación está basado en la norma ISO/IEC 17024:2012.

Los siguientes epígrafes recogen cada uno de los extremos que deben ser considerados por los diferentes Agentes del Esquema que intervienen en el proceso de Evaluación de aquellos profesionales aspirantes a obtener la Certificación de Responsable de Ciberseguridad, según el dicho Esquema.

Para acomodarse a la realidad y a la regulación vigente en cada momento, el presente Reglamento podrá ser actualizado, previa aprobación del Comité del Esquema, a propuesta del Comité de Gestión del Esquema.


STATUS
00 011
1 1 01
01 0 1 00 011 0101
1 1 01.0 1 00 011



Condiciones para la justificación de los prerrequisitos

+ 03.

Condiciones para la justificación de los prerrequisitos

Los profesionales candidatos a concurrir en los procesos de certificación de RCSEG deberán acreditar los requisitos de formación y/o experiencia profesional que se señalan seguidamente, atendiendo, según proceda, a los dos Modos de Acceso descritos en el documento principal del Esquema [ENCRCSEG-01].

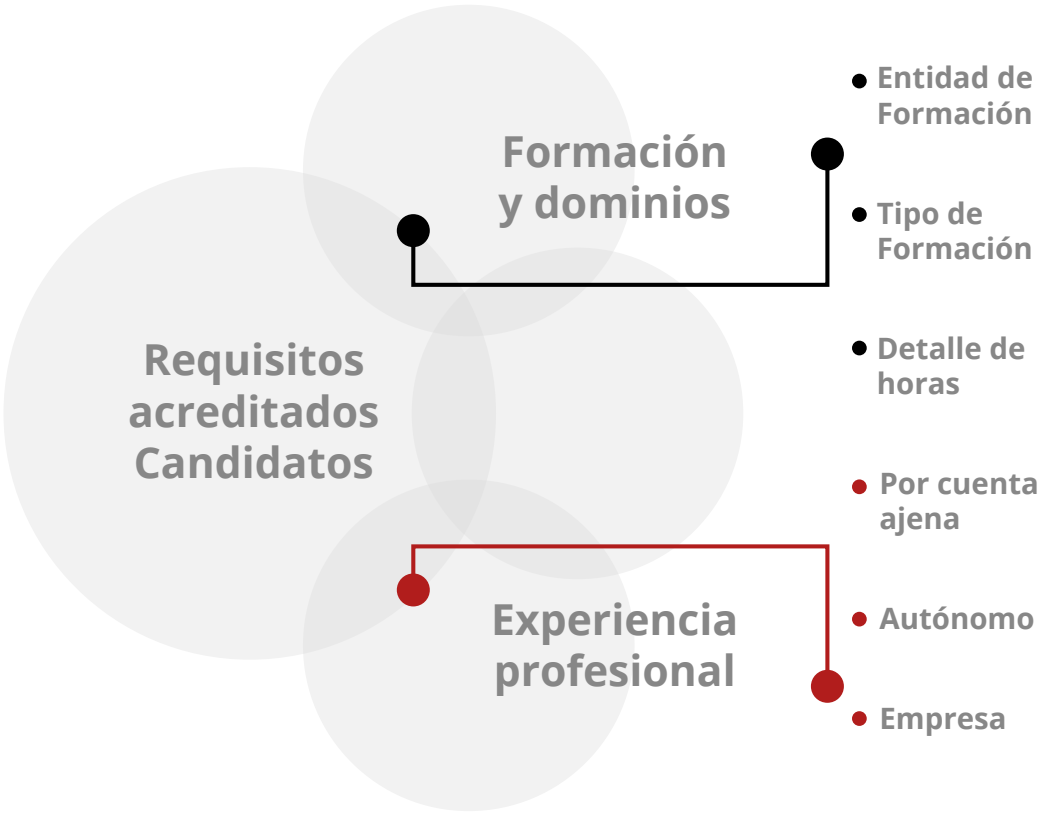
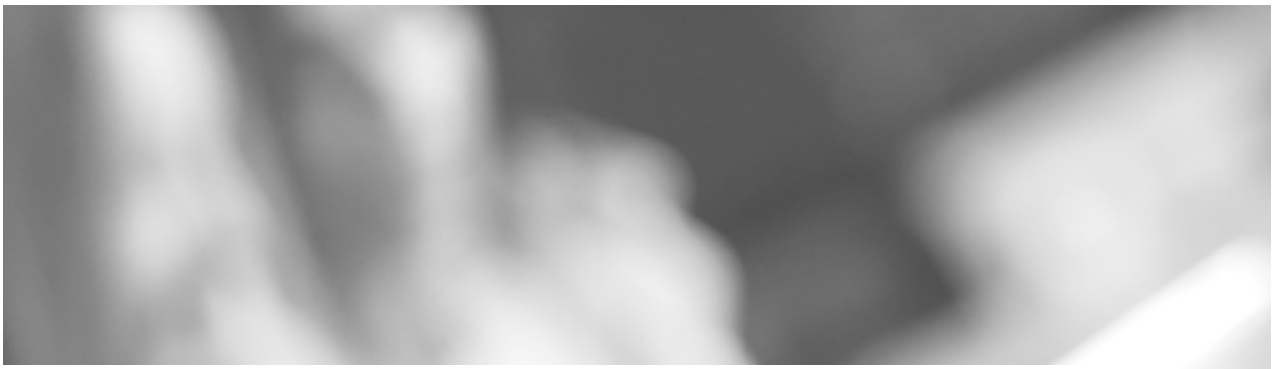


Figura 1.



Formación y dominios

+ 3.1

Si el solicitante ha iniciado el proceso a través del Modo de Acceso 2, deberá aportar el certificado de haber recibido la formación necesaria en relación con las materias objeto del programa del Esquema. Es el requisito para poder presentarse al examen, en el que conste:

- **Entidad de formación de RCSEG (EF)** que ha impartido la formación y ha emitido el correspondiente certificado.

- **Tipo de formación recibida**, atendiendo al siguiente criterio:

  - Cinco (5) o más años de experiencia profesional no requerirán justificar ninguna formación.

  - Tres (3) años de experiencia profesional requerirán justificar haber recibido y superado una formación mínima de 150 horas.

  - Dos (2) años de experiencia profesional requerirán justificar haber recibido y superado una formación mínima de 300 horas.

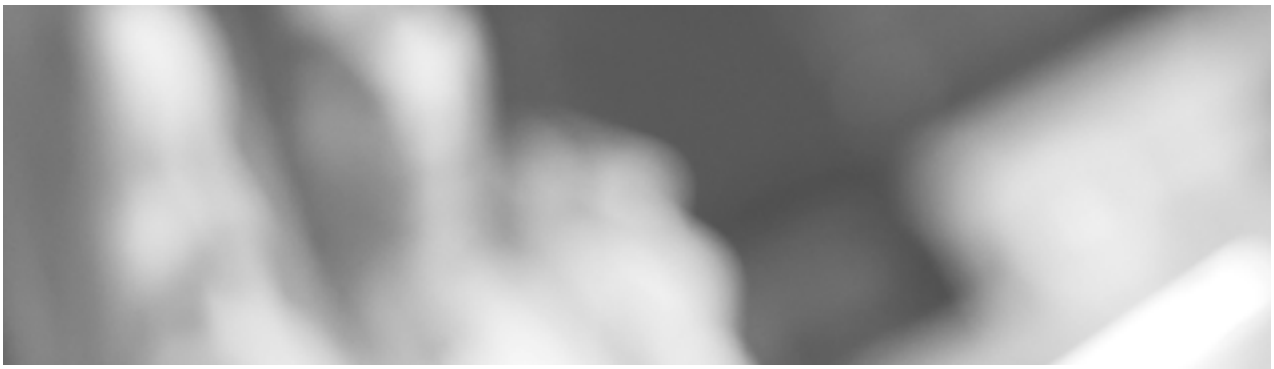
  - Si el candidato no poseyera la experiencia profesional mínima de dos (2) años, será necesario justificar haber recibido y superado una formación mínima de 600 horas.

- **Detalle de la distribución de las horas de formación** del programa conforme al porcentaje establecido para cada uno de los dominios del programa del Esquema. Un programa de formación puede estar formado por varios cursos.

La distribución de horas de formación por dominios -que podrán haber sido impartidas presencialmente o telemáticamente, pero siempre en tiempo real-, será la mostrada en la tabla siguiente.

Dominio	Peso	Descripción	Horas formación	Horas formación	Horas formación
Dominio 1	20 %	Gobierno y gestión de la seguridad	30	60	120
Dominio 2	15 %	Análisis y gestión del riesgo	22,5	45	90
Dominio 3	15 %	Normativa, estándares, buenas prácticas y cumplimiento legal	22,5	45	90
Dominio 4	20 %	Gestión de incidentes, crisis y continuidad de negocio	30	60	120
Dominio 5	20 %	Arquitectura y operativa de ciberseguridad	30	60	120
Dominio 6	10 %	Sistemas industriales e infraestructuras críticas	15	30	60
Total	**100 %**		**150**	**300**	**600**

Sólo se valorará aquella formación que acredite un mínimo nivel de calidad. Y se tendrá en cuenta: que haya sido realizada por organismos académicos o entidades formadoras de reconocido prestigio; o que los formadores sean personas expertas en la materia y que lo acrediten debidamente (mediante su experiencia profesional o mediante certificaciones profesionales en la materia proporcionadas por organismos académicos o entidades de reconocido prestigio).



Experiencia profesional

+ 3.2

El candidato **deberá justificar la experiencia profesional continuada** de, al menos, dos (2), tres (3) o cinco (5), años en funciones relacionadas con la ciberseguridad, desempeñando funciones de CISO, consultor externo de seguridad de la información, auditor de la norma ISO/IEC 27001 o del ENS, etc.

Además de las exigencias documentales que se señalan en los epígrafes siguientes, se valorará disponer de certificaciones profesionales en materia de auditoría, seguridad de la información, gobierno y/o gestión de riesgos de las TIC, proporcionadas por organismos académicos o entidades de reconocido prestigio.

Tales certificaciones, cuyas evidencias documentales de posesión, contenidos y peculiaridades habrán de ser suministradas por el candidato en el momento de realizar la solicitud, serán evaluadas por el Comité de Gestión del Esquema, que podrá tomar la decisión de deducir del tiempo requerido para la experiencia profesional un máximo de seis (6) meses, atendiendo al alcance y significación de la certificación de que se trate. En la documentación que acompañará cada Convocatoria de RCSEG se publicará un baremo precisando los citados extremos.

3.2.1. Profesional por cuenta ajena

El **profesional por cuenta ajena** deberá aportar:

- **Informe de Vida Laboral**, conforme al modelo establecido por la Seguridad Social.
- **Certificado de la(s) empresa(s)** en la(s) que ha venido **desarrollando la actividad que se acredita**, donde consten detalladamente las tareas desempeñadas respecto a las materias relacionadas con seguridad de la información, en relación con el listado de Dominios vigente en el Esquema, fecha de inicio y fecha de finalización de dichas tareas, así como porcentaje de ese tiempo dedicado a otras actividades no relacionadas.

3.2.2. Profesional por cuenta propia (autónomo)

El profesional por cuenta propia (autónomo) deberá aportar:

» **Informe de Vida Laboral** conforme al modelo establecido por la Seguridad Social.

» **Certificado de los clientes**, donde consten, de manera detallada, las tareas desempeñadas respecto a las materias relacionadas con seguridad de la información, en relación con el listado de Dominios vigente en el Esquema, fecha de inicio y de finalización de los servicios prestados, indicando dicho certificado la dedicación efectiva anual.

3.2.3. Profesional de empresa de prestación de servicios o consultoría de ciberseguridad

El profesional empleado de una empresa prestadora de servicios o consultoría de ciberseguridad deberá aportar:

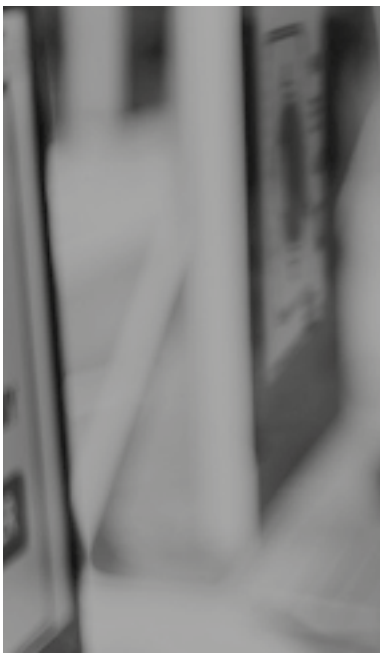
- **Informe de Vida Laboral**, conforme al modelo establecido por la Seguridad Social.

- **Certificado de la empresa** donde consten de forma detallada las tareas desempeñadas respecto a las materias relacionadas con seguridad de la información, nombre del cliente, fecha de inicio y de finalización de los diferentes trabajos realizados, y la dedicación efectiva anual a cada uno de ellos.

Dominios del Esquema de certificación

+ 04.

Dominios del Esquema de certificación



Se muestra seguidamente el temario detallado por Dominios del Esquema de Certificación de Responsables de Ciberseguridad (RCSEG).

Dominio 1
Gobierno y gestión de la seguridad

Objetivo: estándares, estrategia, política de ciberseguridad, gestión, auditorías y terceras partes.

+ La Estrategia Nacional de Ciberseguridad

- Objetivos
- Líneas de Trabajo
- Órganos de Gobierno:
  - Consejo Nacional de Ciberseguridad
  - Foro Nacional de Ciberseguridad

+ Introducción y gestión de ciberseguridad

- Qué es la ciberseguridad
- Fundamentos:
  - Cumplimiento legal y requisitos de negocio.
  - Análisis de riesgos
  - Tipos de controles: organizativos, procedimentales, técnicos y humanos
- Marcos de control:
  - Interrelación con procesos, riesgos globales y cumplimiento (GRC)

+ Consideraciones generales sobre los sistemas de gestión

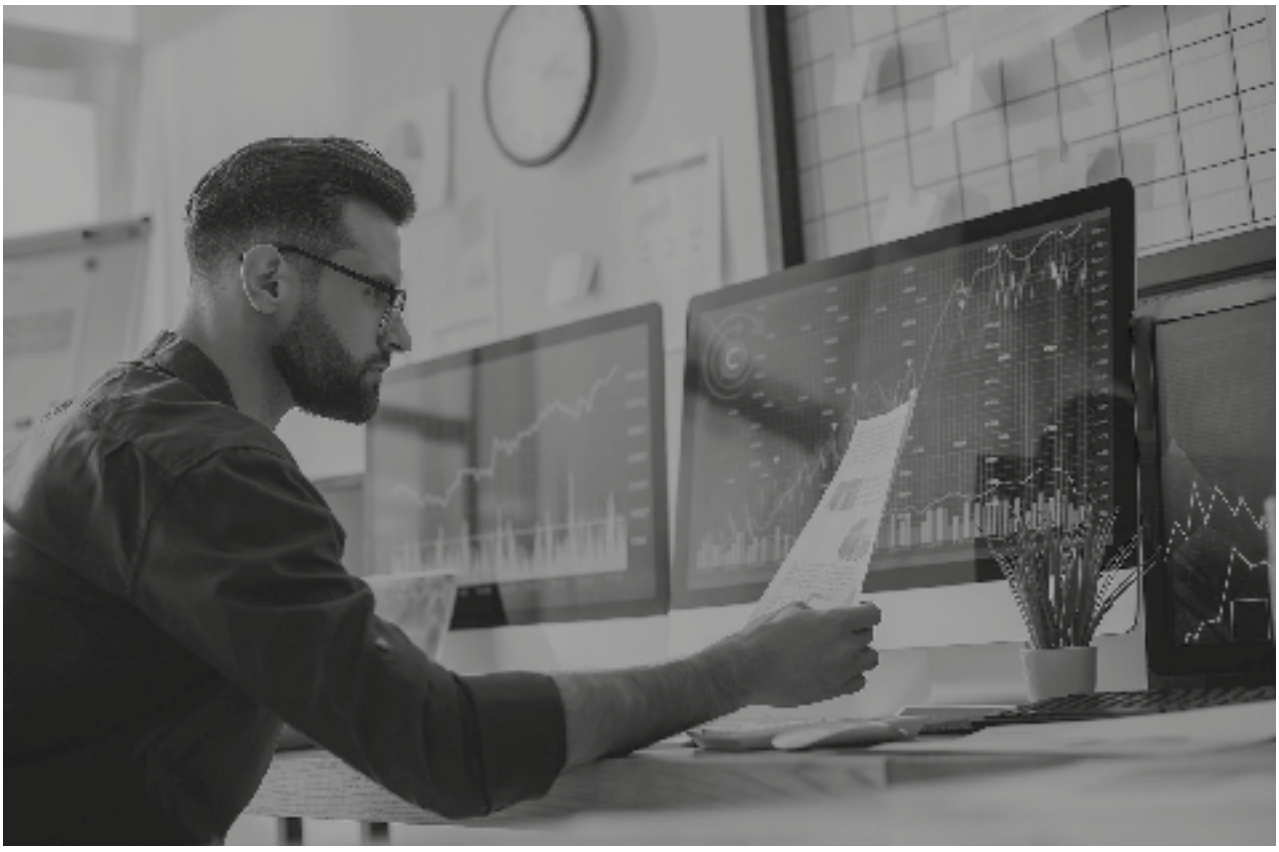
- Sistemas de gestión de seguridad (ISO)

+ Arquitecturas de seguridad

- Introducción a la arquitectura de seguridad y su diseño
- Seguridad en redes
- Seguridad en accesos
- Gestión de identidades
- Gestión de usuarios privilegiados
- Cifrado de información y destrucción segura de información
- Desarrollo seguro
- Seguridad en el ciclo de desarrollo
- Bastionado de equipos
- Monitorización de seguridad
- Respaldo de información
- Estrategias de continuidad
- Protección contra el malware
- Gestión de vulnerabilidades y hacking ético
- Ciberinteligencia, cooperación y capacidad
- Principios de seguridad
- Mínimo privilegio
- Defensa en profundidad
- Aislamiento de entornos críticos

+ La seguridad gestionada. Sistemas de gestión de seguridad de la información aplicados sobre sistemas de información

- Modelos organizativos
  - Roles y responsabilidades
  - Comités de seguridad
  - Función de la organización de seguridad: las tres líneas de defensa
- Modelo de relaciones
  - Internas y con terceros
  - Privado-privado
  - Público-privado
  - Nacionales e internacionales
- Competencias vs Capacidades



+ Responsable de seguridad de la información

- **Estrategia de Seguridad**
  - Modelo de Estrategia (organización, objetivos, alcance, inputs (regulatorios, de negocio...)
  - Marcos de control (¿propio o ajeno? ¿Mixto? Densidad, agilidad, robustez)
  - Seguimiento e indicadores (*Key Performance Indicator* (KPI) + *Key Risk Indicator* (KRI), reporte, validación)
- **Gobierno de ciberseguridad**
  - Misión, Visión y Mandato
  - Modelos de Gobierno.
  - Políticas, Normas y procedimientos (usuarios, infraestructura, dispositivos, procesos, etc.)
  - Estrategia y Plan Director.
  - Plan-Do-Check-Act.
- **Competencias/capacidades**
  - Prevención y asesoramiento.
  - Supervisión
  - Identificación
  - Detección
  - Respuesta y recuperación
  - Coordinación y seguimiento
- **Softskills**
  - Habilidades personales (habilidades propias naturales o adquiridas (hablar en público, presentaciones, empatía, negociación...))
  - Ciencias paralelas (otras cualificaciones o estudios que habilitan palancas)
  - Modelo de relación (relaciones internas y externas, jerarquía, establecer red de contactos, quid pro quo)

+ Procesos de certificación y acreditación

- Requerimientos de seguridad en terceras partes
- Cláusulas de Seguridad
- Acuerdos de Niveles de Servicio de Seguridad
- Certificaciones y acreditaciones [ISO/IEC 27001, *Common Criteria*, Esquema Nacional de Seguridad (ENS)]
- Informes de auditoría (*International Standard on Assurance Engagements* -ISAE 3402 y *Service Organization Control Report* (SOC1 / SOC2)
- Evaluaciones y calificaciones de seguridad
- Normativa y certificación en la nube

+ Ciberejercicios y plataformas de simulación

- Motivación, tipología, marco de ejecución y puesta en valor de un ciberejercicio
- Ciberejercicios (Agencia de Ciberseguridad de la Unión Europea -ENISA, Instituto Nacional de Ciberseguridad de España - INCIBE, Oficina de Coordinación de Ciberseguridad - OCC y sectoriales)
  - Internacionales, nacionales, sectoriales, internos
- Plataformas y herramientas de simulación

+ Cumplimiento y auditoría

- Gestión del marco de control (evaluaciones, evolución, mejora continua, etc.)
- Marcos de control de la Seguridad
- Matrices de controles mapeando diferentes estándares, regulaciones y marcos de referencia
- Auditorías internas y externas de seguridad

- Auditorías de Seguridad: qué son, tipos de auditorías de seguridad (interna, perimetral, forense, test intrusión, de código, etc..), revisión con respecto a normativa interna/externa/estándar referencia/marco de control
- Auditoría documental y Auditoría técnica: evidencias
- Las evaluaciones de seguridad en el marco del ENS: auditorías y certificaciones

+ Concienciación, formación y capacitación del personal

- Concienciación y sensibilización (empleados y niveles directivos)
- Formación y capacitación (equipos de seguridad)

+ La cadena de suministro

- Particularidades de los servicios externalizados respecto al ENS
- Soluciones IaaS, PaaS y SaaS en la nube e implantadas en modo local (híbridas, mixtas y *on-premise*)
- Contratación y seguimiento de los acuerdos con proveedores

+ Requerimientos en especificaciones técnicas para contrataciones

- Seguridad y privacidad desde el diseño
- Riesgos en la cadena de suministro
- Monitorización y supervisión

Dominio 2
Análisis y gestión del riesgo

Objetivo: Principales amenazas tecnológicas y gestión de riesgos en Ciberseguridad.

+ Riesgos de seguridad

- **Modelo de gestión de riesgos**
  - Metodologías
  - Líneas de defensa
- **Análisis de riesgos**
  - Amenazas y vulnerabilidades
  - Identificación de riesgos asociados a los activos
- **Controles de seguridad**
  - Tipos de controles (preventivos, detectivos, reactivos, etc.)
  - ¿Cómo elegir los mejores controles?
- **Gestión de los riesgos**
- Fases de la gestión de riesgos
- **Plan de acción:**
  - Establecer una hoja de ruta basada en el análisis de riesgos
  - Priorización de controles en base a la Mitigación del riesgo, coste y complejidad
  - **Efectividad de los controles**
  - Preparación de los KRI (*Key Risk Indicators*) y revisión
  - Seguimiento del plan de acción
- **Gestión de riesgos continua y dinámica.**
  - Por qué es importante una gestión continua
- **Automatización**
  - Soluciones y herramientas
- **Reporte de los riesgos a los diferentes comités**
  - Comité de riesgos, comité de seguridad y comité de dirección
- **CDM (Cuadro de Mando)**
  - Uso de los indicadores para la construcción de un cuadro de Mando enfocado a cada destinatario

+ Identificación de activos y marco regulatorio

- Identificación del contexto de activos
- Tipologías de activos
- Identificación de activos
  - Agregación de activos
  - Valoración de los activos

+ Vulnerabilidades, amenazas, probabilidades e impactos

- **Conceptos: vulnerabilidad y amenaza**
- **Vulnerabilidades**
  - Ejemplos reales de explotación de vulnerabilidades y sus consecuencias
- **Amenazas**
  - Identificación de amenazas
- **Evaluación del riesgo**
  - Estimación del riesgo cualitativo y cuantitativo
  - Cálculo de probabilidad e impacto
  - Riesgo inherente y efectivo

+ Análisis de riesgos

- Concepto de Riesgo de Ciberseguridad
- Relación con los riesgos corporativos
- Identificación y evolución de fuentes de amenaza
- Apetito de Riesgo de Seguridad

+ Gestión y tratamiento de Riesgos de Seguridad

- Programa de tratamiento de riesgos
  - Estrategias de tratamiento (asumir, reducir, transferir, evitar)

+ Estrategias especiales

- Riesgos de Terceros
- Amenazas híbridas y desinformación
- Ciberseguros
- Teletrabajo

Dominio 3

Normativas, estándares, buenas prácticas y cumplimiento legal

Objetivo: regulaciones y Leyes, Cibercrimen, Infraestructuras Crítica, la prueba digital.

+ Cumplimiento

- Organización y protocolos internos de cumplimiento
- Análisis y gestión de riesgos de cumplimiento y planes de acción
- Figuras y roles en el cumplimiento: responsable de seguridad de la información, Asesoría Jurídica, *Compliance Officer*, *Data Privacy Officer-DPO*, Auditoría interna, etc.
- Visión integral del cumplimiento
  - Matriz de cumplimiento y ranking de controles
- Seguimiento, evaluación y auditoría

+ Requerimientos legales y regulatorios

- Regulación nacional e internacional
  - ENS: Esquema Nacional de Seguridad
  - NIS-NIS2: Seguridad en los sistemas de información y comunicaciones
  - GDPR/RGPD: Reglamento General de Protección de Datos
  - PIC: Protección de Infraestructuras Críticas
  - eIDAS: Sistema Europeo de Reconocimiento de Identidades Electrónicas y Servicio de Confianza
- Regulaciones sectoriales

+ Estándares y marcos de control nacionales e internacionales

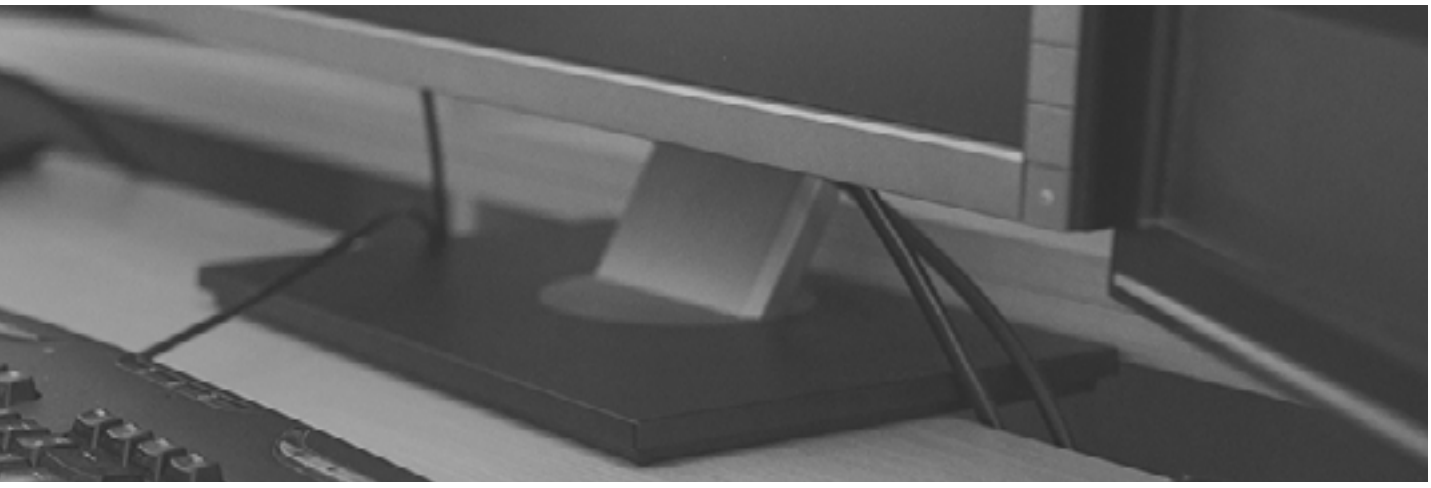
- **Estándares, marcos de referencia y mejores prácticas**
  - ISO y UNE
  - ENS: Esquema Nacional de Seguridad
  - NIST: Instituto Nacional de Estándares y Tecnología
  - SANS: SysAdmin Audit, Networking and Security Institute
  - COBIT: Objetivos de Control para las Tecnologías de la Información y Relacionadas
  - UIT – T x.1205
  - NATO: Organización del Tratado del Atlántico Norte y DoD: Department of Defence
- **Diferentes sistemas de gestión de la seguridad legales y normativos**
  - ENS: Esquema Nacional de Seguridad
  - UNE ISO/IEC 27001:2013 sobre Sistemas de Gestión de Seguridad de la Información (SGSI)
  - Certificaciones Cloud (ISO/IEC 27017:2015 y CSA-STAR de la Cloud Security Alliance)
  - UNE ISO 22301:2019 sobre sistemas de gestión de continuidad del negocio (SGCN)
  - Relaciones y equivalencias entre normas

+ Herramientas de gestión del cumplimiento normativo en seguridad

- Técnicas, metodologías y herramientas del cumplimiento.
- Concienciación
- Formación

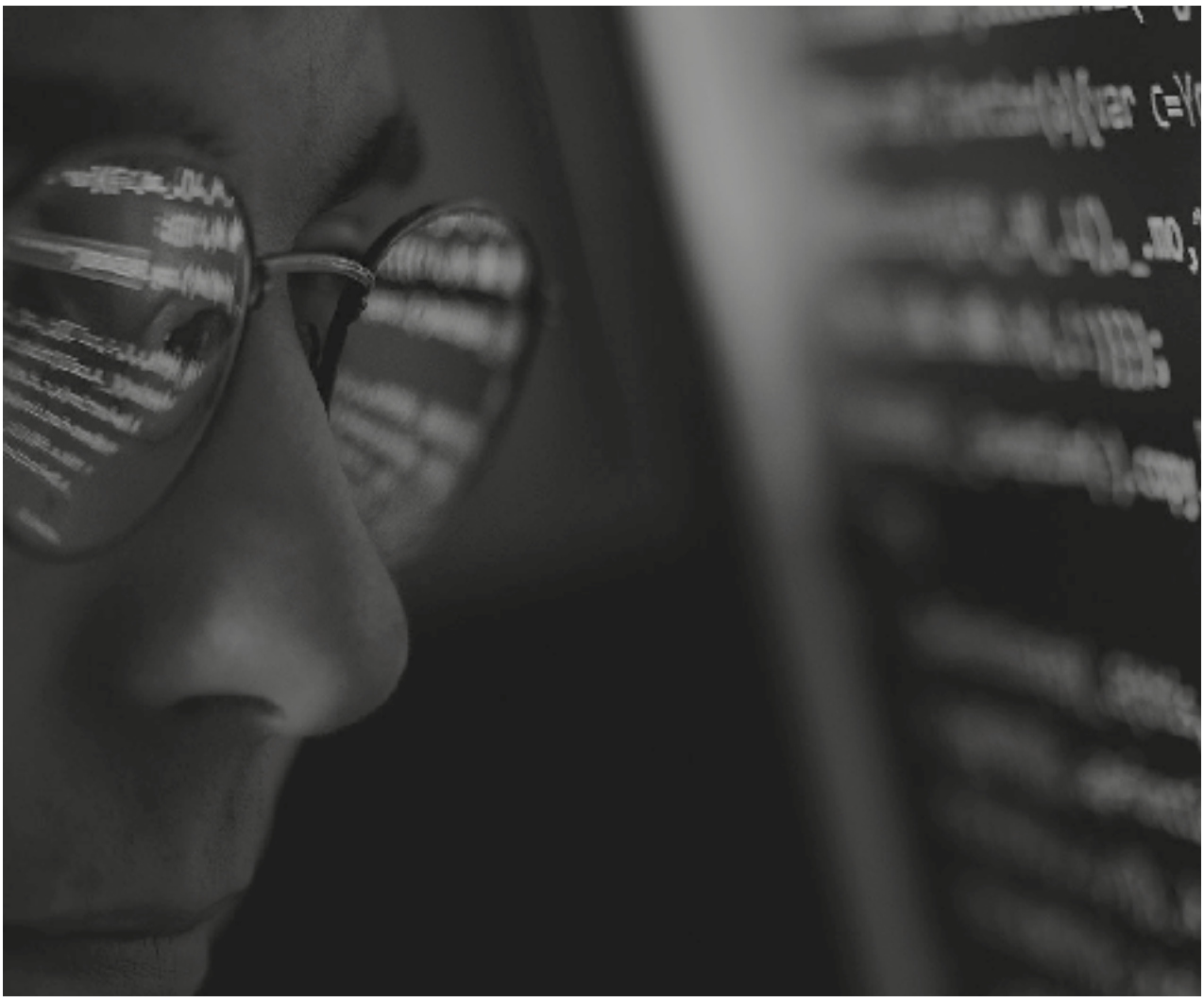
+ Aspectos legales del cibercrimen y delitos informáticos

- La recogida, preservación, presentación y custodia de indicios y evidencias electrónicas
- Regulación del Código Penal y Circular de la Fiscalía. Ejemplos y jurisprudencia
- Investigaciones ante el cibercrimen. Aspectos de jurisdicción y normativa aplicable



Dominio 4
Gestión de incidentes, crisis y continuidad de negocio

Objetivo: **detección, tratamiento, análisis y notificación de brechas. Continuidad y Resiliencia.**



+ Planificación de una gestión de Crisis

- Definición del Plan [decisión y motivación del Plan, alcance (continuidad, reputacional, financiero, recursos humanos, ...), definición y escalado, roles y responsabilidades (Comités)]
- Fases y decisiones [funcionamiento y procedimientos (cómo, cuándo, quién...), comunicación y sus mecanismos, toma decisiones, impacto en terceros, reguladores, clientes]
- Planes de acción y recuperación [definición de medidas ad-hoc, activación de Planes: continuidad, contingencia, etc.; vuelta normalidad, gestión post crisis (causa raíz, lecciones aprendidas, seguros...), ejemplos]
- Simulacros y simulaciones
- Presupuesto
- Plan de Continuidad

+ La gestión de Brechas e incidentes de seguridad

- Incidencias e Incidentes
- Detección de incidentes de seguridad (canales y herramientas)
- Registro y documentación (herramientas, codificación y valoración)
- Estrategias de investigación y remediación
- Investigación temprana, triaje y valoración
- Escalado (grupos de soporte, comité de crisis, continuidad de negocio)
- Análisis, especialización, documentación
- Recuperación
- Lecciones aprendidas
- Estrategias de minimización de situaciones de riesgo

+ Notificación de incidentes y violaciones de seguridad: Regulación, autoridades de control

- Acciones legales y judiciales ante casos de cibercrimen
- Límites legales en la investigación de incidentes de ciberseguridad
- Responsabilidad legal relacionada con el análisis forense
- Notificación de brechas de seguridad y violaciones de datos

+ CERT/CSIRT y SOC

- Estructura, funciones e intercambio de información o indicadores de compromiso

+ Análisis forense y búsqueda de evidencias

- Análisis forense visión general
- Introducción a las metodologías
- Ciclo de vida de un incidente
- Relación entre el análisis forense y la respuesta ante incidentes
- Cadena de custodia
- Adquisición de evidencias
- Clonado
- Forense en Red
- Forense en La Nube
- Forense en Móviles
- Forense de Malware
- Herramientas

+ Gestión de Crisis y Continuidad de Negocio.

- Planes, Protocolos, Ubicaciones
- Comités de Crisis y Roles
- Comunicación y Notificación. Responsables y Portavoces
- Mando y Control
- Información Pasiva y Activa
- Herramientas para Gestionar la Crisis
- Coordinación y Cooperación Interna y Externa
- Toma de Decisiones
- Monitorización y Cierre del Evento, Crisis
- Informes y lecciones aprendidas

Dominio 5

Arquitectura y operativa de ciberseguridad

Objetivo: Tecnologías, Herramientas, Servicios y Capacidades, Infraestructura de seguridad, pentesting, monitorización, gestión de vulnerabilidades, respuesta, desarrollo seguro, etc.

+ Operaciones de ciberseguridad (identificar, proteger, detectar, responder y recuperar)

+ Arquitectura y tecnologías de la ciberseguridad

- Tipologías de arquitectura (On-premise/Cloud)
- Protección de la información
- Data Loss Prevention (DLP)
  - Identificación de datos
  - Detección de fugas de datos
  - Los datos en reposo, en uso y en movimiento
  - Tipologías
- Protección de bases de datos
  - Cifrado
  - Ofuscación de datos
  - Big Data
- Protección de sistemas y servicios
  - Certificación y acreditación de sistemas
  - Bastionado de sistemas
  - Antimalware
  - Cifrado de dispositivos
  - Web
  - Correo electrónico
  - Teletrabajo

- Protección de la infraestructura de seguridad
- Protección del Directorio Activo
- Protección del Cloud
- Protección de redes
- Seguridad en redes
  - Tipologías de red
  - Dispositivos de red (enrutadores, conmutadores, cortafuegos, etc.)
  - Firewall
- Protección de dispositivos Móviles
  - Aspectos específicos
  - MDM: Mobile Device Management
  - BYOD: Bring Your Own Device

+ Monitorización y detección

- **Conceptos esenciales**
  - Elementos
  - Casos de uso
  - MITRE
  - SOC - Security Operation Centre
- **Información de seguridad y gestión de eventos (SIEM)**
  - Capacidades de un SIEM
  - Pasos para realizar una buena monitorización de sistemas
  - Ventajas monitorización de sistemas

+ Análisis y gestión de vulnerabilidades

- Tipologías de vulnerabilidades: tecnologías y aplicaciones
- Gestión de vulnerabilidades: ciclo de vida
  - Tecnologías y aplicaciones
- Detección de vulnerabilidades
  - Interno
  - Externo (programa de recompensas)
  - Hacking ético
- Metodologías de gestión de vulnerabilidades (OWASP)
  - Identificación de vulnerabilidades (CVE)
  - Criticidad de vulnerabilidades (CVSS)
- Herramientas de análisis y gestión

+ Análisis y gestión de malware

- Estado Actual del Malware
- Familias y Tipos
- Herramientas de Análisis
- Técnicas de Análisis:
  - Dinámico
  - Estático
  - Memoria RAM
- Adquisición y custodia de evidencias de Malware
- Laboratorio de Malware

+ APT - Amenazas Persistentes Avanzadas

- Creación de una APT
- Infección por APT
- Mecanismos de protección frente a APT
- Soluciones Anti-APT

+ Pruebas técnicas: Hacking ético y auditorías técnicas

- Objetivos, definición y terminología
- Técnicas y Metodologías: OSSTMM, PTES (*Penetration Testing Execution Standard*) OWASP (Open Web Application Security Project), MITRE ATT&CK, NIST...
- Tipología de pruebas:
  - Alcance, Objetivos y Tipos: caja negra, blanca o gris
  - Requisitos y resultados
  - Limitaciones, exclusiones y periodicidad
  - Competencias auditor: Certificaciones profesionales
- Herramientas: Open-source, comerciales, exploits...

+ Ciberinteligencia y cooperación

- Ciclo de ciberinteligencia y fuentes (internas y externas)
- Relaciones con organismos nacionales e Internacionales
  - Marco nacional, autonómico y local: Centro Criptológico Nacional: CCN-CERT, INCIBE-CERT y Ministerio de Defensa: ESPDEFCERT
  - Marco europeo e internacional: ENISA, FS-ISAC (*Financial Services Information Sharing and Analysis Center*), FIRST (*Forum of Incident Response and Security Teams*)
- Intercambio de información de inteligencia
  - Aspectos legales y regulatorios asociados a intercambio de ciberinteligencia y reporte de ciberincidentes
  - Iniciativas de intercambio de información de inteligencia
  - Plataformas de intercambio
  - Tipos de información a intercambiar

+ Desarrollo seguro

- Introducción y Objetivos
- Conceptos y Definiciones
- Referencias metodológicas y normativas
- Ciclo de vida de desarrollo de software seguro:
  - Requerimientos funcionales, de rendimiento, de calidad y de seguridad del código
  - Directrices de codificación segura
  - Componentes del modelo de seguridad en el desarrollo de aplicaciones
  - Gestión de cambios en el software
  - Integración SecOps y DevOps
- Ciclo de vida de la auditoría de desarrollo de software
  - Tipos de pruebas: de código, de aplicación, funcionales, etc.
  - Subsanación de vulnerabilidades
  - Seguimiento y mejora continua

+ Criptografía

- Introducción y objetivos
- Conceptos y Definiciones
- Tipos de criptografía:
  - Simétrica y asimétrica
  - Curva elíptica, cuántica, etc.
- Procedimientos de gestión y custodia de claves
- Mecanismos criptográficos (PKI (Public Key Infrastructure), HSM (Hardware Security Module), técnicas de ofuscación, etc.)
- Evolución de la criptografía

Dominio 6
Sistemas industriales e infraestructuras críticas

Objetivo: Ciberseguridad específica en los sistemas industriales e infraestructuras críticas (IOT-*Internet of Things*).

+ La Ciberseguridad Industrial (IoT, OT - *Operational Technology*)

- Concepto, similitudes y diferencias
  - IEC 62443 y otras referencias
  - Dependencias de la cadena de suministro
- Sistemas de protección de infraestructuras críticas
  - El Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)
  - Operadores críticos y de servicios esenciales
  - Modelo de relación (colaboración público-privada)
- La Ciberseguridad de los servicios esenciales
  - La Oficina de Coordinación de Ciberseguridad (OCC)
  - La Agencia de Ciberseguridad de la Unión Europea -ENISA
  - *Computer Emergency Response Team* - CERT de referencia (CCN-CERT, INCIBE-CERT)
- Otras organizaciones (Plataforma Tecnológica Española de Seguridad Industrial- PESI, Centro de Ciberseguridad Industrial - CCI, etc.)

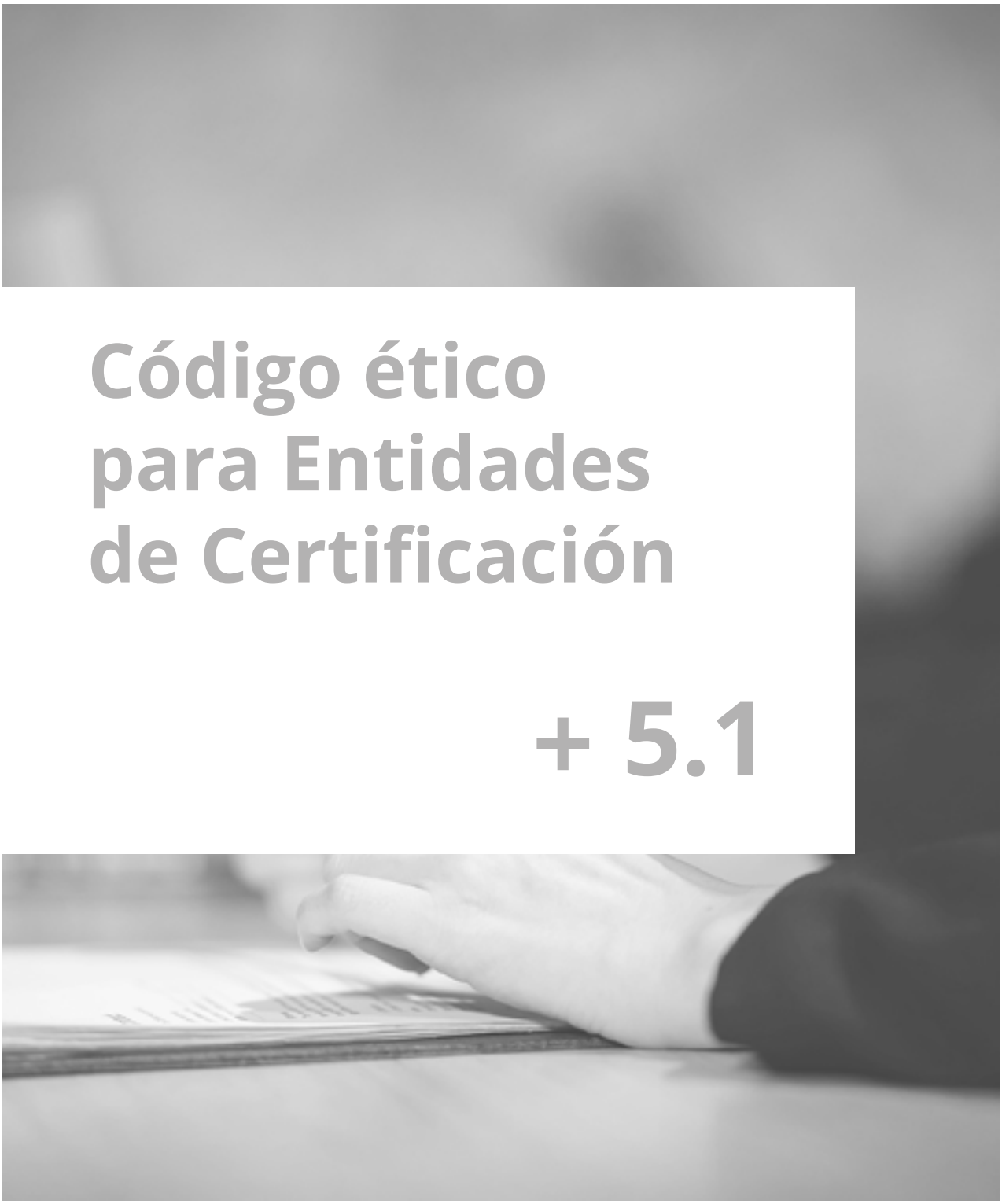
Reglas de uso de la Marca del Esquema

+ 05.

Reglas de uso de la Marca del Esquema

Las Entidades de Certificación establecerán procedimientos para garantizar que ellas mismas, las Entidades de Formación cuyos programas de formación hayan reconocido y los responsables de Ciberseguridad que hayan certificado, usan la Marca del Esquema conforme a las normas y al contrato de uso, recogidas en los epígrafes 4.3.1 y 4.3.2, respectivamente.

Estos procedimientos deben asegurar que dichas normas son conocidas por el personal de las EC, el personal de las EF reconocidas y los RCSEG, que se han de comprometer contractualmente a respetarlas, y que se ejerce el adecuado control de su uso y se toman medidas en caso de una utilización de la Marca que incumpla lo establecido en dichas normas. El Comité de Gestión del Esquema podrá en todo momento solicitar información sobre dichos procedimientos.



Código ético para Entidades de Certificación

+ 5.1

A efectos de justificar cuestiones como la integridad y un elevado nivel de compromiso ético por parte de las entidades interesadas en acreditarse como Entidades de Certificación bajo el Esquema Nacional de RCSEG, dichas entidades han de observar los principios, valores y compromisos que se recogen en el Código Ético para Entidades de Certificación señalado en el epígrafe 6.4 del presente Reglamento.

Dicho Código Ético debe ser aceptado por las entidades interesadas en obtener la acreditación en el momento de solicitarla. Las Entidades de Certificación han de dar visibilidad a sus compromisos éticos mediante la publicación del Código Ético en su página web.

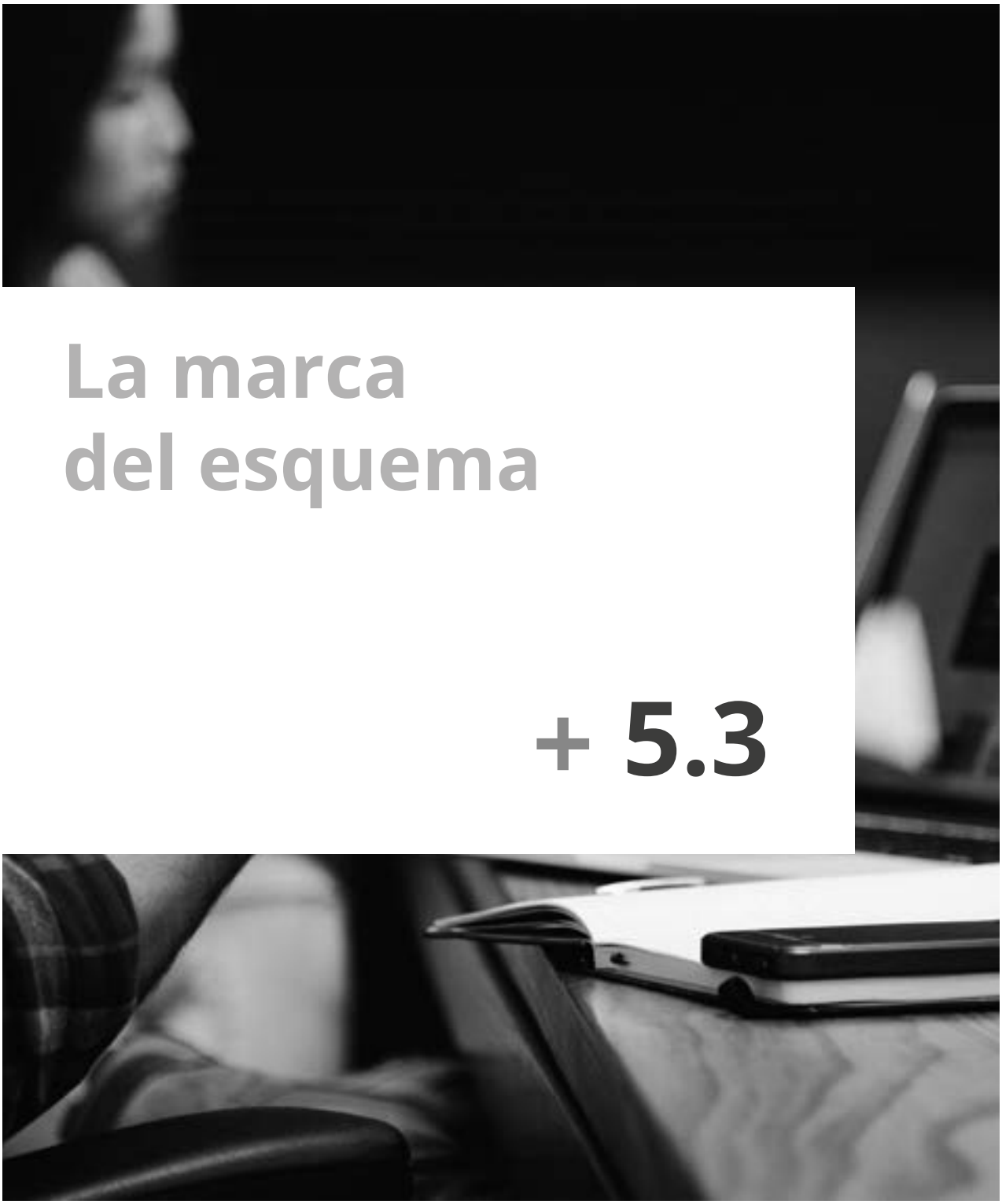
El incumplimiento del citado Código Ético podrá ser causa de resolución del contrato de uso de la Marca (epígrafe 6.3).

Código ético para responsables de ciberseguridad

+ 5.2

A efectos de justificar cuestiones como la integridad y el elevado nivel de ética profesional que implica la función de RCSEG, se ha elaborado y forma parte del Esquema, un Código Ético para responsables de Ciberseguridad, con principios, valores y compromisos que ha de ser aceptado por los candidatos a obtener la certificación con carácter previo a su concesión. El Código Ético se recoge en el epígrafe 6.5. del presente Reglamento.

El incumplimiento del citado Código Ético podrá ser causa de suspensión de la Certificación como RCSEG.



La marca del esquema

+ 5.3

Al objeto de que el mercado sea capaz de identificar la condición de profesional certificado en virtud del Esquema Nacional de Certificación de Responsables de Ciberseguridad, se crea la Marca del Esquema.

La Marca del Esquema es el símbolo usado por los Entidades de Certificación y los profesionales certificados como RCSEG para hacer público este hecho e identificarse como agentes del Esquema. No podrá ser usada por entidades o personas distintas de las descritas, ni tampoco por ninguna entidad interesada en acreditarse como Entidad de Certificación mientras esté en proceso de evaluación.

5.3.1. Normas de uso de la marca del Esquema

Los copropietarios del Esquema concederán licencia para el uso de la Marca, mediante contrato con las Entidades de Certificación, y estará sujeta a las siguientes reglas:

- Se usará siempre claramente asociada al nombre o logotipo del agente autorizado.

- Las Entidades de Certificación podrán emplear la Marca del Esquema exclusivamente en documentos o soportes de tipo publicitario del servicio que presten en el marco del Esquema (folletos, páginas web, etc.), de forma que quede clara su vinculación únicamente con el servicio prestado dentro del Esquema y no con cualquier otro servicio similar que se oferte al mercado.

- Los RCSEG certificados podrán usar la Marca del Esquema exclusivamente en documentos o soportes de tipo publicitario del servicio que presten como responsables de Ciberseguridad (tarjetas de visita, folletos, páginas web, etc.) y no de cualquier otro servicio cuya prestación puedan ofrecer al mercado.

- Las Entidades de Certificación dejarán de emplear la Marca del Esquema cuando finalice o se resuelva el contrato de licencia de uso, así como en caso de suspensión o retirada de la acreditación por parte de ENAC. En estos casos, los profesionales certificados por dichas entidades podrán seguir haciendo uso de la Marca del Esquema hasta la renovación de la certificación, en cuyo caso pasarán a utilizar la de la Entidad de Certificación que proceda a su renovación.

Las Entidades de Certificación son responsables de que, tanto ellas como los RCSEG a los que hayan certificado, usan la Marca del Esquema siguiendo estas normas. En caso de detectar un mal uso de la Marca del Esquema deberán adoptar las medidas oportunas, incluidas la revocación del reconocimiento de los programas de formación y la suspensión o retirada de la certificación.

La infracción de las obligaciones de las Entidades de Certificación respecto a la vigilancia y control del uso de la Marca del Esquema por los RCSEG podrá dar lugar a la resolución del contrato de uso de la Marca del Esquema.

5.3.2
Modelo de contrato de uso de la Marca del Esquema entre los agentes del Esquema

REUNIDOS

De una parte, ...
De otra parte, ...

Reconociéndose mutuamente la capacidad legal necesaria para el otorgamiento del presente contrato,

EXPONEN

I. Que, al objeto de que el mercado sea capaz de identificar la certificación de personas como RCSEG, dentro del Esquema Nacional de Certificación de Responsables de Ciberseguridad (en adelante, Esquema RCSEG), se ha creado la Marca del Esquema Nacional de Responsables de Ciberseguridad (en adelante, Marca del Esquema), inscrita en ..... para las clases..... del Nomenclátor internacional.

II. Que la Marca del Esquema es el símbolo usado por los Agentes del Esquema RCSEG y las personas certificadas para hacer público este hecho.

III. Que la Marca del Esquema es propiedad del Centro Nacional de Inteligencia, a través del Centro Criptológico Nacional (CCN); la Secretaría de Estado de Digitalización e Inteligencia Artificial, a través de la Secretaría General de Administración digital (SGAD); y la Secretaría de Estado de Seguridad, a través de la Oficina de Coordinación de Ciberseguridad (OCC), y solo puede ser usada bajo la responsabilidad de la Entidad de Certificación abajo firmante en las condiciones establecidas en las Normas de Uso publicadas como parte del Esquema RCSEG.

IV. Que la Entidad de Certificación abajo firmante está interesada en operar en el Esquema RCSEG.

V. Que la firma del contrato de uso de la marca es una condición para operar dentro del Esquema RCSEG, debiendo firmarse el mismo con carácter previo a la solicitud de la acreditación a ENAC, a quién deberá aportarse copia de este contrato.

VI. Que ambas partes han acordado proceder a la firma del presente Contrato de uso de la marca con sujeción a las siguientes:

CLÁUSULAS

PRIMERA. Objeto.

Los copropietarios del Esquema RCSEG ceden a la Entidad de Certificación los derechos de uso de la Marca del Esquema en las condiciones establecidas en las Normas de Uso de la Marca recogidas en los epígrafes 6.3 y 6.4 del Reglamento de Solicitantes [ENCRCSEG-02].

SEGUNDA. Condición suspensiva.

El uso de la Marca del Esquema queda condicionado al otorgamiento de la acreditación por ENAC conforme al Procedimiento de Acreditación. La Entidad de Certificación deberá comunicar a los copropietarios del Esquema RCSEG la obtención de la acreditación al objeto de que estos le suministren formalmente el correspondiente archivo de la Marca del Esquema, momento a partir del cual podrá comenzar el uso de la misma.

TERCERA. Responsabilidad de la Entidad de Certificación.

La Entidad de Certificación es responsable de:

a) Ejercer un adecuado control del uso de la Marca del Esquema conforme a las condiciones establecidas en las Normas de Uso de la Marca del Esquema recogidas en el epígrafe 6.3 del citado Reglamento de Evaluación de Solicitantes y en la cláusula 6.4 del Esquema RCSEG, tanto por sí misma como por los RCSEG que certifique, asumiendo las consecuencias establecidas en el Esquema RCSEG en caso de incumplimiento de dicha obligación.

b) Informar a los RCSEG certificados sobre las Normas de uso que les son de aplicación, así como de las consecuencias de un uso incorrecto.

CUARTA. Resolución del contrato.

1. Son causas de resolución del presente contrato:
a) El mutuo acuerdo de las partes.
b) El transcurso del plazo de seis (6) meses desde la solicitud de acreditación a ENAC sin que se haya obtenido la misma, por causas imputables a la Entidad de Certificación.
c) La retirada de la acreditación.

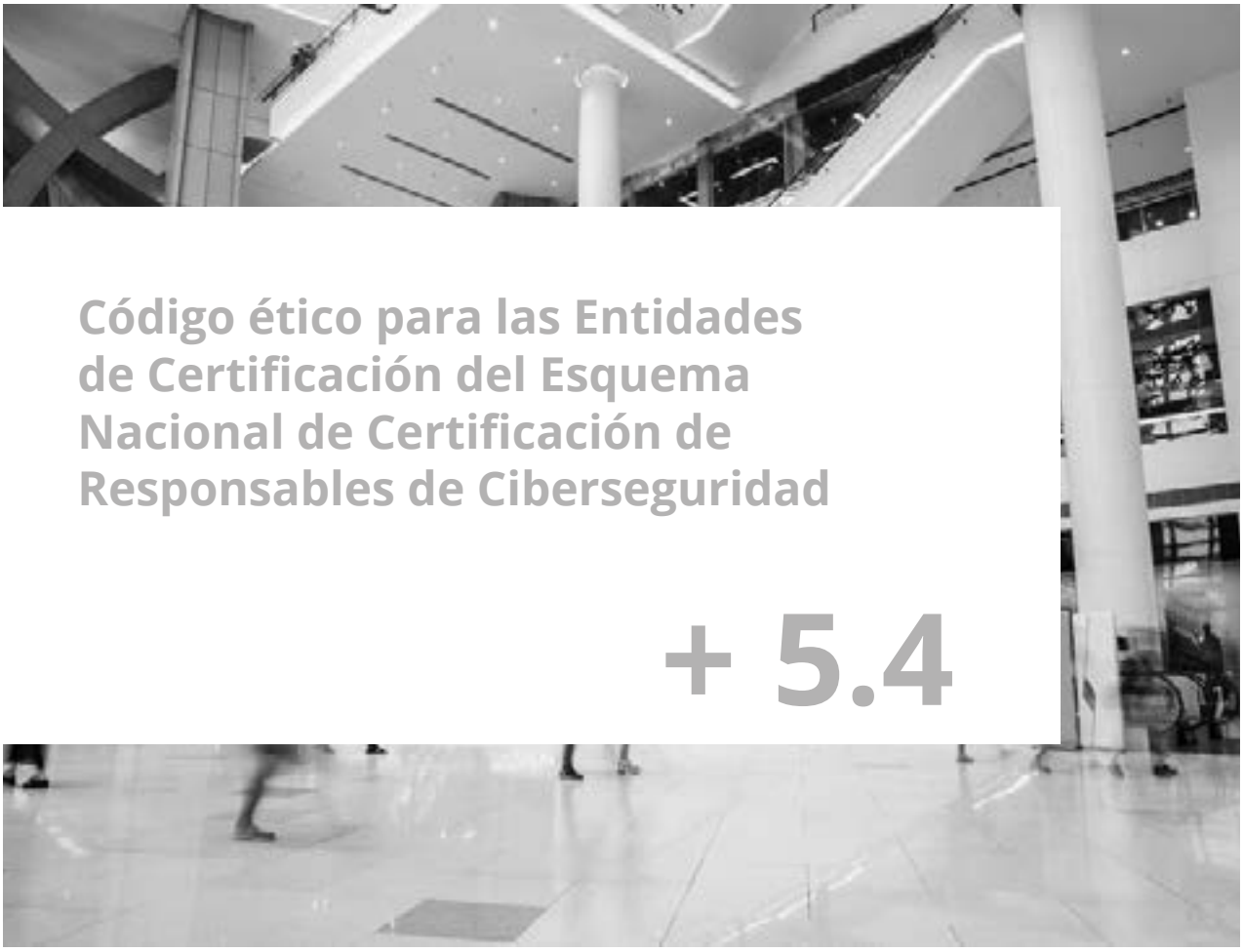
2. Asimismo, podrá dar lugar a la resolución del contrato, motivadamente y previa audiencia de la Entidad de Certificación:
a) La suspensión de la acreditación.
b) El incumplimiento del Código Ético.
c) El incumplimiento por la Entidad de Certificación de su deber de control del uso de la Marca del Esquema respecto de los RCSEG que ha certificado.
d) Cualquier otro incumplimiento de las obligaciones establecidas en el presente contrato.
e) Cualquier otra causa distinta de las anteriores prevista en la legislación vigente que fuera de aplicación.

3. La resolución del contrato implica que la entidad no pueda ofrecer los servicios de certificación dentro del Esquema RCSEG, dando lugar a la extinción de la condición de Agente del Esquema RCSEG y a la indemnización de los daños y perjuicios causados.

4. Resuelto el contrato, los copropietarios del Esquema RCSEG no firmarán un nuevo contrato de uso de la marca con dicha entidad hasta transcurridos dos años, a contar desde la resolución.

QUINTA. Jurisdicción competente.

Las controversias que pudieran surgir entre las partes como consecuencia de la interpretación o ejecución de este contrato serán de conocimiento y competencia del orden jurisdiccional contencioso-administrativo.



Código ético para las Entidades de Certificación del Esquema Nacional de Certificación de Responsables de Ciberseguridad

+ 5.4

En el **Anexo I del presente Reglamento se contiene el Código Ético** que deberán suscribir todas las Entidades de Certificación del Esquema Nacional de Certificación de Responsables de Ciberseguridad, durante su proceso de acreditación por parte de ENAC.

Código ético para las responsables de ciberseguridad del Esquema Nacional de Certificación de Responsables de Ciberseguridad

+ 5.5

El **Anexo II del presente Reglamento de Evaluación de Solicitantes** contiene el Código Ético que todos los profesionales Responsables de Ciberseguridad certificados conforme al Esquema Nacional de Certificación de Responsables de Ciberseguridad deben suscribir durante el proceso de certificación realizado por la Entidad de Certificación de que se trate.

Procedimiento de selección y designación de evaluadores

+ 06.

Procedimiento de selección y designación de evaluadores

El evaluador es el profesional con conocimientos y experiencia profesional equivalente o superior al candidato a certificarse como RCSEG, y con capacidad para evaluar la ejecución de las pruebas, teóricas y prácticas que habrán de desarrollar los candidatos en su proceso de evaluación, así como las alegaciones que pudieran presentar dichos candidatos durante su realización.

Su labor no puede comprometer los principios de independencia e imparcialidad que rigen las tareas de evaluación y de certificación. Se considera que un evaluador cumple las condiciones si está certificado bajo el presente Esquema RCSEG.

Los evaluadores pueden ser personal propio de la entidad o contratado, en cuyo caso, para cuantas cuestiones puedan surgir respecto al incumplimiento de sus compromisos con relación al Esquema RCSEG, se ajustarán a lo indicado en el contrato.

El procedimiento de selección define los criterios relativos a la selección y mantenimiento de las empresas o personas contratadas.

1. Requisitos de los evaluadores

Los evaluadores candidatos deberán cumplir los siguientes requisitos.

- **Titulación universitaria de licenciado, ingeniero o grado en informática, telecomunicaciones o tecnologías de la información.**
- **Experiencia profesional continuada de, al menos, cinco (5) años en el ámbito de la Seguridad de la Información**

2. Méritos

Se valorarán los siguientes méritos:

2.1. Méritos preferentes.

2.1.1. Titulación universitaria superior a la de grado: ostentar el título de doctor o poseer un posgrado o máster en el ámbito de la ciberseguridad.
2.1.2. Experiencia docente en títulos relacionados con la ciberseguridad, especialmente en el ámbito universitario.
2.1.3. Estar en posesión de certificaciones vigentes relacionadas con la ciberseguridad.

2.2. Méritos adicionales.

Se valorarán también los siguientes méritos:

2.2.1. Publicación de libros, artículos o ponencias relacionados con la ciberseguridad.
2.2.2. Premios o reconocimientos recibidos, en materia de ciberseguridad.
2.2.3. Participación en comités nacionales o internacionales de normalización relacionados con la ciberseguridad.
2.2.4. Experiencia específica en el puesto de responsable de ciberseguridad.

3. Incompatibilidades y exclusiones

Podrán ser excluidos parcial o totalmente del proceso de evaluación aquellas personas que pudieran ver comprometida su independencia e imparcialidad por cualquier circunstancia profesional, familiar o personal.

4. Funciones del evaluador

El evaluador es responsable de:

- Evaluar de manera imparcial y confidencial la documentación presentada por los candidatos y las pruebas a que se sometan. La valoración del examen se hará sin conocer la identidad del candidato, salvo en el caso del Modo de Acceso 1.

- Emitir un informe con el resultado de la evaluación.

Además, le corresponde:

- Informar a la Entidad de Certificación de cualquier relación profesional, familiar o de otro tipo que pueda afectar a la objetividad e imparcialidad de su labor de evaluación.

- Valorar la recusación motivada de cualquier candidato para su traslado a la Entidad de Certificación.

5. Procedimiento de selección

La Entidad de Certificación evaluará las candidaturas de los evaluadores y resolverá comunicando su decisión al candidato.

6. Comité de selección

La Entidad de Certificación creará un órgano interno sujeto a la normativa interna y del Esquema para realizar la selección de los evaluadores.

7. Registros y procedimientos de trabajo

Se mantendrán archivados los currículums de todos los evaluadores en los que se conserven los registros sobre titulación, formación y experiencia que demuestren su adecuada competencia técnica.

Asimismo, se distribuirán de forma controlada a los evaluadores copias de aquellos documentos del sistema de gestión, basado en la norma ISO 17024, que sean de aplicación a su actividad y, en especial, todos los procedimientos y formatos aplicables a la actividad de evaluación.

Modelo de informe de los resultados de las pruebas teóricas de los solicitantes

+ 07.

Modelo de informe de los resultados de las pruebas teóricas de los solicitantes

La prueba teórica tipo test se considerará superada con un resultado igual o superior al 75 % de las respuestas correctas con, al menos, el 50 % en cada uno de los dominios.

Dominio	Puntuación Mínima	Puntuación Obtenida
1. Gobierno de la seguridad	X	
2. Análisis y gestión del riesgo	X	
3. Normativa, estándares, buenas prácticas y cumplimiento legal	X	
4. Gestión de incidentes, crisis y continuidad de negocio	X	
5. Operativa de ciberseguridad	X	
6. Sistemas industriales e infraestructuras críticas	X	

PUNTUACION MÍNIMA PARA SER APTO	113
PUNTUACIÓN OBTENIDA	[ ]
RESULTADO	APTO [ ] / NO APTO [ ]

Derechos de los solicitantes

+ 08.

Derechos de los solicitantes

En el momento de la comunicación a los aspirantes de los resultados de las Pruebas de Evaluación de cada Convocatoria de RCSEG, el Comité de Gestión del Esquema publicará el procedimiento para permitir a los solicitantes la impugnación de tales resultados, incluyendo un formulario online para el ejercicio de tal derecho.

El Comité de Gestión del Esquema dispondrá de un plazo no superior a un mes para decidir sobre la reclamación planteada, comunicando al solicitante su decisión, que cerrará la vía administrativa, pudiéndose interponer recurso por la vía regulada en la legislación en materia contencioso-administrativa.

Los sistemas de información que alojen el sistema de gestión del proceso completo de Certificación de RCSEG (solicitud y documentación anexa, custodia de los enunciados de las pruebas, evaluación, impugnaciones y certificaciones) estarán bajo la responsabilidad del Centro Criptológico Nacional y dispondrán de la Certificación de Categoría Alta del Esquema Nacional de Seguridad (RD 3/2010, de 8 de enero), de conformidad con lo señalado en la Disposición adicional primera de la Ley Orgánica 3/18, de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales.

Modelo de documento justificativo de la Certificación

+ 09.

Modelo de documento justificativo de la Certificación

Cada Entidad de Certificación (EC) podrá disponer libremente de su propio formato de Certificación de Conformidad con el presente Esquema, que deberá mostrar, al menos, el contenido siguiente:

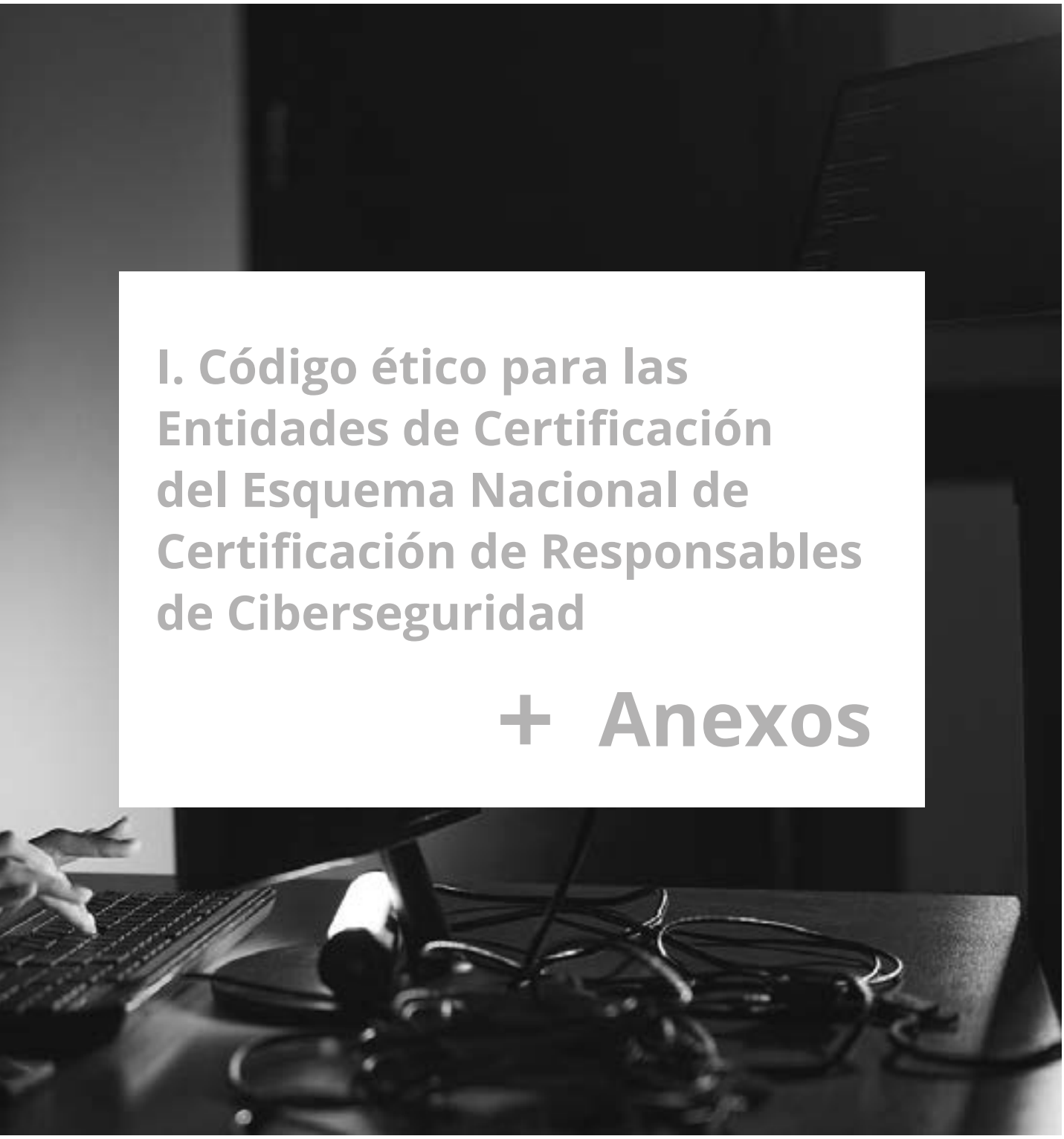
- *Logotipo de la Entidad Certificadora de RCSEG.*
- *Sello o marca del Esquema común a todos los agentes del Esquema.*

NOTA: Sería equivalente a los certificados emitidos en el ENS, o en la certificación de Delegado de Protección de Datos, que consta el sello del esquema y el logotipo de la EC.

- *Identificación de la Entidad Certificadora de RCSEG.*
- Texto: *"**Certificado de Conformidad con el Esquema Nacional de Certificación de Responsables de Ciberseguridad (RCSEG)**".*
- Texto: *"«Entidad Certificadora" certifica que el candidato reseñado, ha sido evaluado y encontrado conforme con las exigencias del Esquema Nacional de Certificación de Responsables de Ciberseguridad (RCSEG)».*

- *«Nombre, apellidos y DNI de la persona objeto de la certificación».*
- Texto: *"Número de certificado: «número de certificado»".*
- Texto: *"Fecha de certificación de conformidad inicial: «día» de «mes» de «año»"*.
- Texto: *"Fecha de renovación de la certificación de conformidad: «día» de «mes» de «año»".* (si procede)
- Texto: *"Fecha de caducidad de la certificación de conformidad: «día» de «mes» de «año»".*
- Texto: *"Fecha: «Localidad (la que corresponda)», «día» de «mes» de «año»".*
- Firma: *Nombre y Apellidos del responsable competente de la Entidad de Certificación de RCSEG.*
- Firma del responsable de la Entidad de Certificación de RCSEG.
- Nombre completo/razón social de la Entidad de Certificación y página web.
- Dirección postal/electrónica.
- Código Postal, Provincia, País.

Los textos que aparecen entre paréntesis angulares se adaptarán a los aspectos concretos de la certificación expedida.



I. Código ético para las Entidades de Certificación del Esquema Nacional de Certificación de Responsables de Ciberseguridad

+ Anexos

Código ético para las Entidades de Certificación del Esquema Nacional de Certificación de responsables de ciberseguridad

Preámbulo

El presente Código Ético constituye una declaración expresa de los valores y principios que, basados en la normativa aplicable y en los requisitos del Esquema Nacional de Certificación de Responsables de Ciberseguridad (Esquema RCSEG, en adelante) deben presidir y guiar el comportamiento de aquellas entidades y empresas (en adelante, entidades interesadas) que soliciten de la Entidad Nacional de Acreditación (ENAC) la acreditación para ser Entidades Certificadoras (en adelante, EC) de RCSEG, conforme al Esquema RCSEG, en el ejercicio y desempeño de su actividad profesional.

El presente Código Ético recoge un conjunto de principios y valores (legalidad, integridad, honorabilidad, competencia leal, profesionalidad, responsabilidad, imparcialidad, transparencia y confidencialidad) que provienen de las obligaciones que establecen las distintas normativas que son de aplicación a la actividad de las entidades que solicitan la acreditación de EC a ENAC, así como de las recogidas en el Esquema RCSEG.

Su observancia se fundamenta en la diligencia debida para su cumplimiento con la finalidad de proporcionar confianza y garantía de un comportamiento absolutamente responsable con la legalidad vigente en sus relaciones con empleados, proveedores, clientes y cualesquiera terceros con los que se relacionen, tanto de ámbito público como privado, incluyendo la sociedad en general.

El objetivo del presente Código es procurar un comportamiento profesional por parte de las entidades interesadas: de sus directivos, empleados, apoderados, representantes y colaboradores, que se aleje de conductas y hechos contrarios a los principios y valores que recoge.

El presente Código Ético, que las entidades interesadas vienen obligadas a suscribir con carácter previo a la presentación de la solicitud de acreditación, implica el compromiso de actuar conforme a sus principios y valores durante el procedimiento de acreditación como EC por ENAC y durante el ejercicio de su actividad como EC una vez que como tal hayan sido reconocidas.

Para que el Código sea efectivo y proporcione confianza y seguridad a los que se relacionen o hayan de relacionarse con las entidades interesadas de un comportamiento ético, éstas han de proceder a su difusión entre directivos, empleados, apoderados, representantes y colaboradores; establecer procedimientos y estructuras para la comunicación y gestión de reclamaciones; y para la supervisión y control de su observancia, funciones que, en su caso, también podrán ser realizadas por el Comité del Esquema (CE) o, por delegación de éste, por el Comité de Gestión del Esquema (CGE), en garantía de su buen funcionamiento.

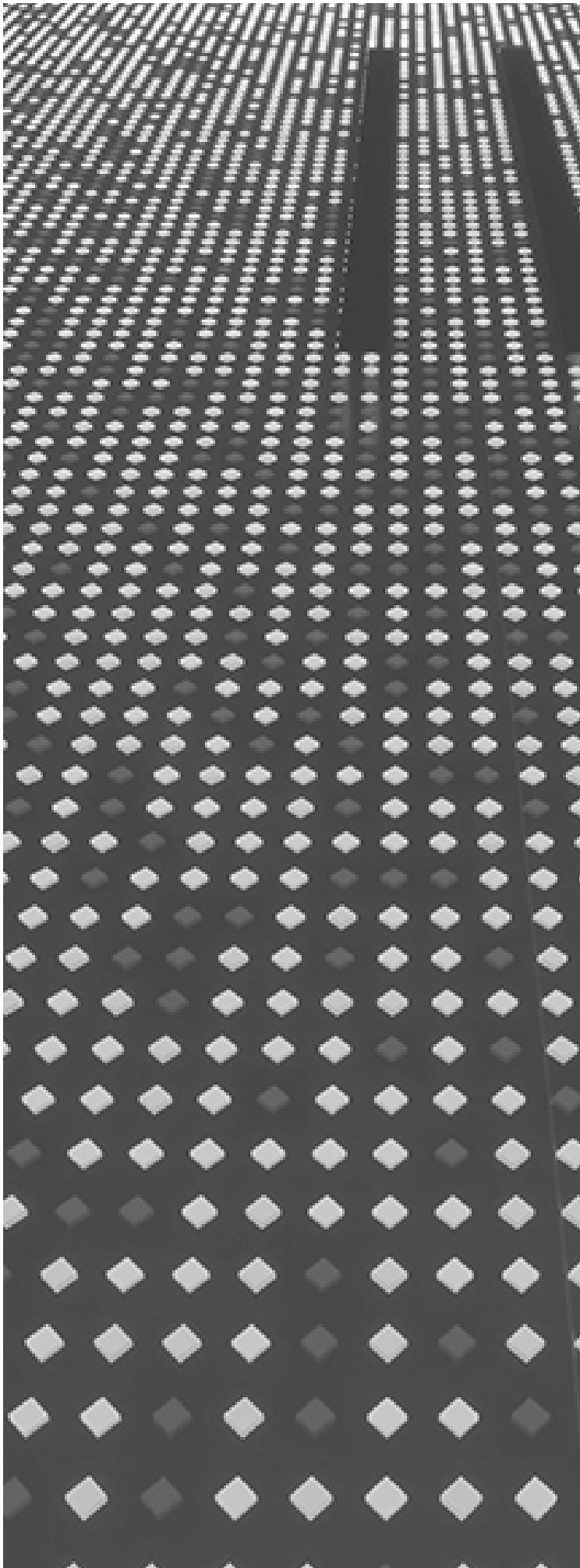
Artículo I. Ambito de aplicación

Los principios y valores contenidos en el presente Código Ético son de obligada observancia y cumplimiento para las entidades que soliciten de la Entidad Nacional de Acreditación (ENAC) ser acreditadas para constituirse como Entidades de Certificación con arreglo al Esquema RCSEG, así como por sus directivos, empleados, apoderados, representantes y colaboradores, desde el mismo momento de presentación de la solicitud y durante el ejercicio de su actividad como EC en el marco del Esquema RCSEG. Será de aplicación para todas las sociedades que formen parte de las entidades interesadas, incluyendo sus directivos, empleados, apoderados, representantes y colaboradores.

Artículo II. Principios de actuación

Las entidades interesadas y sus sociedades, sus directivos, empleados, apoderados, representantes y colaboradores, en el ejercicio de sus actividades, se comportarán con sujeción a los siguientes principios:

» **Legalidad:** las entidades interesadas cumplirán estrictamente con la legislación y la normativa vigente en cada momento, y especialmente con lo establecido en el Esquema RCSEG, al objeto de evitar que se lleve a cabo cualquier actividad ilícita y, en particular, las prácticas o declaraciones que de cualquier manera supongan un perjuicio para ENAC, los copropietarios del Esquema, el Esquema RCSEG o a cualquiera de sus actores.



Las entidades interesadas se comprometen a adoptar las medidas necesarias para que sus directivos, empleados, apoderados, representantes y colaboradores conozcan la normativa aplicable, incluidos los principios y valores del Código Ético y los puedan observar.

- **Integridad:** las entidades interesadas desarrollarán sus actividades en todo momento con ética profesional, de manera honrada, profesional y de buena fe, evitando los conflictos de intereses.

- **Honorabilidad:** las entidades interesadas no deberán haber sido objeto de sanción en cualquiera de los ámbitos de su actividad y ejercicio profesional durante los tres (3) años anteriores a la presentación de la solicitud de acreditación, ni ser sancionadas durante su desempeño como EC.

- **Competencia leal:** las entidades interesadas desarrollarán su actividad profesional de manera leal, sin permitir comportamientos engañosos, fraudulentos, o maliciosos.

- **Responsabilidad en el desarrollo de sus actividades profesionales:** las entidades interesadas asumirán las actividades de colaboración que le requieran los copropietarios del Esquema RCSEG y demás autoridades públicas, así como el resto de las entidades del Esquema RCSEG para su correcto desarrollo y mantenimiento, evitando cualquier conducta que perjudique su reputación.

- **Imparcialidad:** las entidades interesadas actuarán con objetividad en sus relaciones con terceros, sin aceptar presiones o influencias que pudieran cuestionar su integridad profesional, o la de sus directivos, empleados, apoderados, representantes y colaboradores.

- **Transparencia:** las entidades interesadas actuarán con transparencia en el ejercicio de su actividad profesional, en concreto en el ámbito del Esquema RCSEG que exige:

  - Informar a todas las partes interesadas de forma clara, precisa y suficiente de todos los aspectos que confluyen en el ejercicio profesional como EC, siempre y cuando los mismos no estén sujetos al régimen de confidencialidad, en cuyo caso tendrán carácter reservado y no podrán ser divulgados.

  - Facilitar a todas las partes interesadas con claridad, precisión y suficiencia toda la información relevante sobre el proceso de certificación y sobre el estado de la acreditación.

- **Confidencialidad:** las entidades interesadas respetarán y guardarán la necesaria protección y reserva de la información a la que pudiera tener acceso por razón de su actividad como EC, salvaguardando los derechos legítimos de todas las partes interesadas. Dicha información no será utilizada para su beneficio ni de su personal, ni revelada a partes inapropiadas.

Artículo III. Relaciones con el personal de la organización

En sus relaciones con sus empleados, directivos y colaboradores, las entidades interesadas:

- Pondrán los medios necesarios para comunicar y difundir el Código Ético entre todos sus empleados.
- Evitarán las situaciones que puedan dar lugar a conflictos de intereses con las actividades de la organización.
- Establecerán procedimientos que permitan la notificación de conductas contrarias al presente Código Ético y al Esquema RCSEG.
- Vigilarán que el personal a su cargo no lleve a cabo actividades ilícitas ni conductas contrarias al presente Código Ético y al Esquema RCSEG.
- Asumirán la responsabilidad de la actuación de sus directivos, empleados apoderados, representantes y colaboradores en cuanto a las actividades relacionadas con el Esquema RCSEG.

Artículo IV. Relaciones con colaboradores externos, y proveedores

Las entidades interesadas:

- Establecerán unas relaciones basadas en el respeto a la legalidad vigente, el Esquema RCSEG, el comportamiento ético, la lealtad, la buena fe, la confianza, respeto y transparencia.

- Actuarán con imparcialidad y objetividad en los procesos de selección de colaboradores, aplicando criterios debidamente documentados de competencia y calidad, evitando en todo momento la colisión de intereses.

- Garantizarán documentalmente una absoluta independencia con las entidades que presten formación a los candidatos a obtener la certificación.

- Darán a conocer el contenido del presente código deontológico.

Artículo V. Relaciones con clientes

En sus relaciones con los clientes, las entidades interesadas:

- Darán a conocer el contenido del presente Código Ético.
- Actuarán de forma ética, íntegra, de buena fe y profesional, teniendo como objetivo la consecución de un alto nivel de calidad en la prestación de sus servicios, buscando el desarrollo de unas relaciones basadas en la confianza, seguridad y en el respeto mutuo.
- Salvaguardarán siempre la independencia, evitando que su actuación profesional se vea influida por vinculaciones económicas, familiares y de amistad con los clientes, o de sus relaciones profesionales al margen de la actividad de las EC, no debiendo aceptar regalos o favores de cualquier naturaleza de parte de estos o de sus representantes.
- No efectuarán ni aceptarán, directa ni indirectamente, ningún pago o servicio de más valor ni distinto al establecido para el servicio proporcionado.
- Pondrán en conocimiento del cliente cualquier situación que pueda dar lugar a un conflicto de intereses en la prestación de sus servicios antes de asumir un encargo profesional.

- No realizarán ninguna actividad promocional (publicidad, material informativo u otra) que pueda inducir a los clientes a una incorrecta interpretación del significado de la Acreditación bajo el Esquema RCSEG, o a unas expectativas que no respondan a la situación real.

- No ofrecerán la formación requerida en el Esquema RCSEG ni publicitarán, en su página web o en otros medios, cursos relacionados con el Esquema RCSEG.

- No realizarán ofertas, descuentos u otros beneficios a los candidatos a obtener la certificación como RCSEG por provenir de programas de formación determinados.

Artículo VI. Relación con las autoridades y organismos públicos

Las relaciones con las instituciones, organismos y Administraciones Públicas (estatal, autonómicas y locales) y, especialmente, con los copropietarios del Esquema RCSEG, se desarrollarán bajo el principio de máxima colaboración y escrupuloso cumplimiento de sus resoluciones.

Las comunicaciones, requerimientos y solicitudes de información que las entidades interesadas reciban de autoridades y organismos públicos deberán ser atendidas con diligencia, en los plazos establecidos para ello.

Artículo VII. Control de aplicación del código

Las Entidades de Certificación y las Entidades de Formación permitirán el acceso al registro de las reclamaciones relacionadas con el presente Código Ético a ENAC y a los copropietarios del Esquema RCSEG y colaborarán plenamente con cualquier actuación o investigación sobre su cumplimiento.

Artículo VIII. Aceptación e interpretación del código ético

El Esquema RCSEG exige a las entidades interesadas un alto nivel de compromiso en el cumplimiento del presente Código Ético. Las entidades interesadas se comprometen a la suscripción y aplicación del presente Código ético que forma parte del Esquema RCSEG.

Cualquier duda que pueda surgir sobre la interpretación o aplicación del presente Código Ético deberá consultarse con los copropietarios del Esquema RCSEG, quienes tienen la obligación de fomentar el conocimiento y cumplimiento de este Código Ético e interpretarlo en caso de duda.

Artículo IX. Incumplimiento del código ético

La falta de adhesión al presente Código Ético o el incumplimiento de alguno de los compromisos que implica supondrán la resolución del contrato de uso de la Marca del Esquema.

II. Código ético para responsables de ciberseguridad del Esquema Nacional de Certificación de Responsables de Ciberseguridad

+ Anexos

Código ético para responsables de ciberseguridad del Esquema Nacional de Certificación de Responsables de Ciberseguridad

Preámbulo

El presente Código Ético constituye una declaración expresa de los valores, principios y normas que deben guiar la conducta de las personas certificadas como Responsables de Ciberseguridad (RCSEG certificados), conforme al Esquema Nacional de Certificación de Responsables de Ciberseguridad (Esquema RCSEG, en adelante), en el ejercicio de sus funciones o tareas, y en sus relaciones con otros empleados, como con clientes, proveedores, instituciones públicas y privadas, colaboradores externos y la sociedad en general.

El presente Código Ético recoge, por tanto, un conjunto de compromisos de integridad, imparcialidad, legalidad, confidencialidad y transparencia que habrán de suscribir ineludiblemente, así como conocer y difundir, quienes pretendan desarrollar su actividad profesional como RCSEG certificados con arreglo al presente Esquema.

De este modo, a través del presente Código Ético, se persigue prevenir la comisión de comportamientos contrarios a los criterios que contiene, al tiempo que se diseñan mecanismos de seguimiento y control que garanticen su íntegro cumplimiento por parte de todas aquellas personas que desempeñen su labor profesional como RCSEG certificados por el Esquema RCSEG.

Los criterios de conducta recogidos en este Código Ético no pretenden contemplar la totalidad de situaciones o circunstancias con las que los mencionados profesionales se pueden encontrar, sino establecer unas pautas generales de conducta que les orienten en su forma de actuar durante el desempeño de su actividad profesional.

El Comité del Esquema RCSEG, el Comité de Gestión del Esquema RCSEG, así como las Entidades de Certificación del Esquema RCSEG deberán velar por el cumplimiento y aplicación del presente Código, para lo que cual promoverá su difusión no solo entre los profesionales, sino en empresas y administraciones públicas y la sociedad en general, en relación con el ejercicio de la profesión de responsable de Ciberseguridad.

En la redacción de este Código se ha tenido en cuenta la especificación europea *Common Guidelines on Statements of Professional Ethics* elaboradas en el marco de la iniciativa *European IT Profesionalism Framework*.

Alcance de la responsabilidad profesional

La responsabilidad profesional en que puede recaer el responsable de Ciberseguridad en el desempeño de su cometido profesional es de tres clases:

1. Penal

Por delitos y faltas que se cometan en el ejercicio de la profesión, según las normas penales vigentes.

2. Civil

Cuando actuando con mala fe (dolo civil), negligencia o impericia inexcusable cause daños en los intereses de un cliente sea del ámbito público o privado (retrasos en la ejecución del trabajo encomendado, actividad inoportuna o inadecuada).

3. Disciplinaria

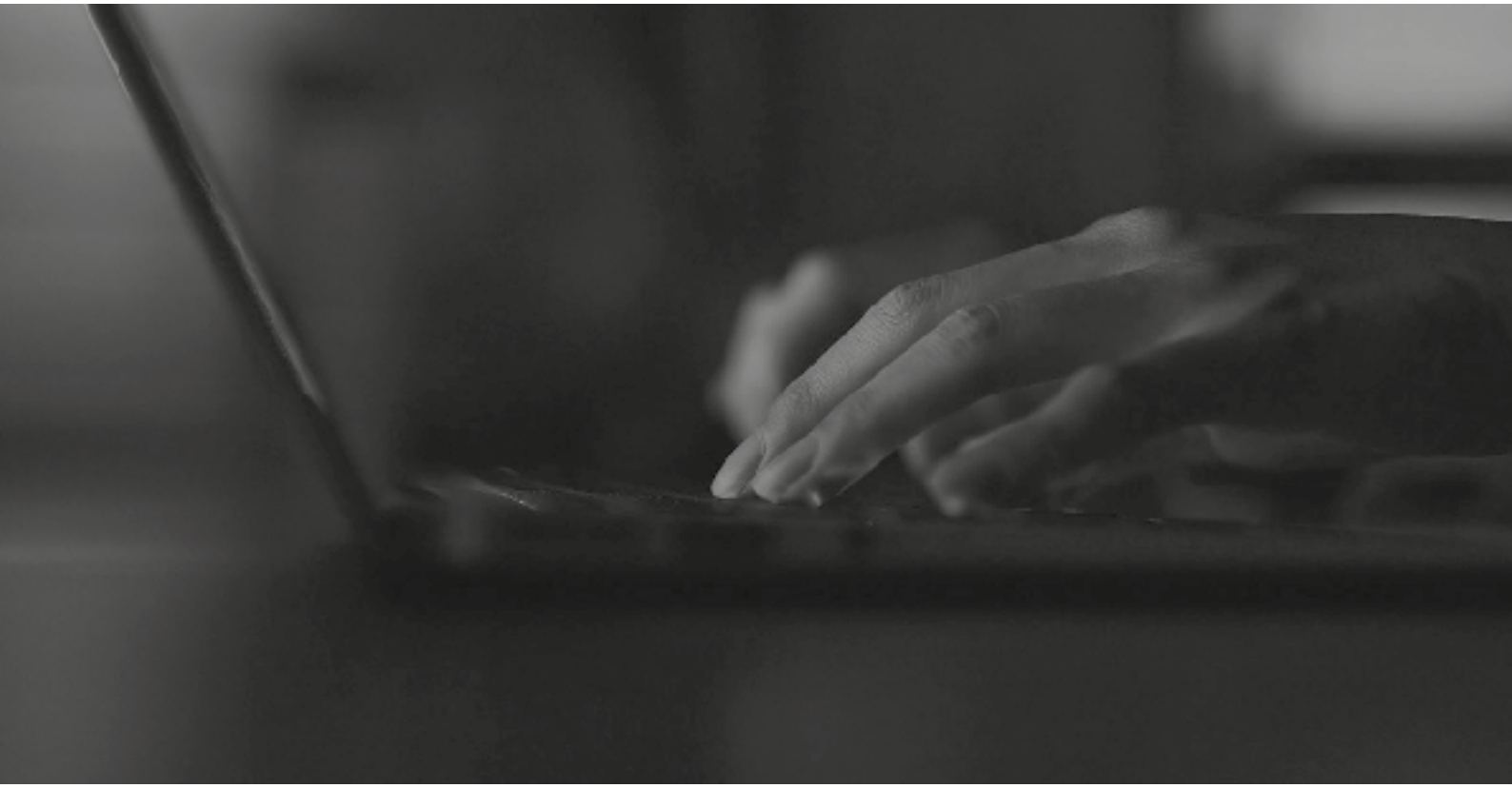
Cuando infrinja deberes estatutarios de la profesión o normas de ética profesional.

Artículo I. Ámbito de aplicación

Los principios, valores y criterios contenidos en el presente Código Ético son de obligado cumplimiento para los RCSEG certificados por las Entidades de Certificación acreditadas por la Entidad Nacional de Acreditación (ENAC) con arreglo al Esquema RCSEG.

Todos los actores del Esquema RCSEG están obligados a conocer, cumplir, difundir y velar por el cumplimiento de los artículos del presente Código Ético. Cualquier incumplimiento de lo dispuesto en este Código deberá ser comunicado a los organismos pertinentes sin demora, de forma puntual.

El incumplimiento del presente Código Ético se considerará como falta leve, grave o muy grave según lo dispuesto en la normativa que resulte de aplicación, incluyendo la laboral o de función pública y, como tal, podrá conllevar la iniciación del correspondiente expediente disciplinario.



Artículo II. Principios generales

Los responsables de Ciberseguridad certificados en su actividad profesional conforme al Esquema RCSEG llevarán a cabo todas sus actuaciones con sujeción a los siguientes principios:

1. Honradez

El responsable de Ciberseguridad ha de ser moralmente íntegro, veraz, leal y diligente, tanto consigo mismo como en relación con los demás.

2. Independencia

La independencia actual y moral del responsable de Ciberseguridad, que permanentemente deberá preservar, es condición esencial para el ejercicio de la profesión y constituye la garantía de que los intereses de los destinatarios de sus servicios serán tratados con objetividad.

3. Lealtad

El responsable de Ciberseguridad debe ser moralmente íntegro, veraz, leal y diligente en el desempeño de su función. El responsable de Ciberseguridad mantendrá siempre una actitud respetuosa, leal, de colaboración y solidaria con los compañeros de profesión, clientes y demás profesionales y observará la mayor deferencia en sus relaciones profesionales, evitando posiciones de conflicto. En las relaciones o colaboraciones interprofesionales debe respetar los principios, metodologías y decisiones que tienen, como propias y específicas, las demás profesiones, aunque conservando en todo caso la libertad de interpretación y aplicación de los propios fines y objetivos.

4. Dignidad

El responsable de Ciberseguridad debe actuar conforme a las normas de honor y de dignidad en la profesión. Debe ejercer la profesión con una conducta irreprochable, guiada por la responsabilidad y la rectitud.

5. Legalidad

El responsable de Ciberseguridad debe cumplir y velar por el cumplimiento de todo el ordenamiento jurídico de aplicación en su trabajo, así como por el cumplimiento de las normas corporativas, advirtiendo a las partes involucradas de aquellos aspectos que no cumplan la legalidad vigente y denunciando aquellas actuaciones que supongan un riesgo potencial para la sociedad.

6. Intereses del cliente

El responsable de Ciberseguridad debe velar por la satisfacción de los intereses del cliente, incluso cuando estos resulten contrapuestos a los suyos propios. Si se viera en una situación de insuperable contradicción con sus valores éticos o morales podrá no aceptar el trabajo acogiéndose a la objeción de conciencia.

7. Libertad del cliente

El responsable de Ciberseguridad intentará, en la medida de lo posible, no proponer soluciones que puedan suponer una situación de 'cliente prisionero'. Asimismo, el responsable de Ciberseguridad ha de reconocer el derecho del cliente a elegir con libertad a quien contrata y, por lo tanto, no poner trabas frente a una posible voluntad de cambio de profesional por parte del cliente.

8. Secreto profesional

El responsable de Ciberseguridad tiene el derecho y el deber de guardar el secreto profesional de todos los hechos y noticias que conozca por razón de su actuación profesional, solo con excepciones muy limitadas, que se justifiquen moral o legalmente.

9. Igualdad y función social

El responsable de Ciberseguridad debe tener presente en todo momento el carácter de su cometido como servicio a la sociedad, velando por la igualdad tanto social como de género y ha de promover el conocimiento general de la profesión y su aportación al bien público. El responsable de Ciberseguridad procurará la mayor eficacia de su trabajo en cuanto a conseguir una óptima rentabilidad social y humana de los recursos disponibles.

10. Adecuación de la tecnología

El responsable de Ciberseguridad debe proponer la solución tecnológica que más se adecúe a las necesidades funcionales y tecnológicas del cliente y a su disponibilidad presupuestaria, evitando la imposición de tecnología.

11. Formación y perfeccionamiento

El perfeccionamiento profesional y la continua puesta al día de sus conocimientos técnico-científicos y las mejores prácticas profesionales es una obligación del responsable de Ciberseguridad, al permitirle garantizar la prestación de unos servicios de calidad a los usuarios. Del mismo modo, el responsable de Ciberseguridad debe participar en el desarrollo, uso y regulación de estándares profesionales.

12. Libre y leal competencia en el ejercicio de la profesión

El responsable de Ciberseguridad no puede proceder a la captación desleal de clientes, debiendo respetar en todo momento lo dispuesto en las normas que tutelen la leal competencia y absteniéndose de cualquier práctica de competencia ilícita e informando cuando sea posible a un órgano competente o colegio profesional de cualquier conocimiento real de fraude en concursos o de selección, en especial en los referentes a las Administraciones Públicas.

13. Remuneración

El responsable de Ciberseguridad promoverá y velará en lo posible por la remuneración justa de su trabajo, evitando aceptar aquellos que supongan un menoscabo del prestigio de la profesión o incurran en competencia desleal.

14. Incompatibilidades

Además de cuando esté legal o reglamentariamente establecido, se entenderá situación de incompatibilidad cuando exista colisión de derechos o conflicto de intereses que puedan colocar el ejercicio de la función profesional en una posición equívoca, o que implique un riesgo para su independencia.

15. Respeto a la naturaleza y medio ambiente

El respeto y la conservación de la naturaleza y el medio ambiente han de estar entre las preocupaciones de los responsables de Ciberseguridad en todos los aspectos del ejercicio de su actividad. Los responsables de Ciberseguridad certificados deberán observar una conducta ecológica en el desempeño de su profesión, debiendo actuar y abogar por y para una defensa de la naturaleza, encaminada a la protección y mejora de la calidad de la vida, así como al respeto, disfrute y conservación de un medio ambiente adecuado.

16. Trabajo en equipo

El responsable de Ciberseguridad cuando participe de un trabajo de equipo, de forma conjunta con otras profesiones, deberá actuar con pleno sentido de responsabilidad en el área concreta de su intervención. Asimismo, contribuirá con sus conocimientos y experiencia al intercambio de información técnica al objeto de obtener la máxima eficacia en el trabajo conjunto.

17. Responsabilidad civil

El responsable de Ciberseguridad, cuando proceda, deberá tener cubierta su responsabilidad profesional, en cuantía adecuada a los riesgos que implique.

18. Investigación y docencia

El responsable de Ciberseguridad como investigador no dará a conocer de modo prematuro o sensacionalista nuevos datos insuficientemente contrastados, no exagerará su significado, ni los falsificará o inventará, ni plagiará publicaciones de otros autores y en general no utilizará con poca seriedad y rigor los datos obtenidos. El responsable de Ciberseguridad, cuando en su ejercicio profesional desarrolle actividad docente, tiene el deber de velar por la buena calidad de enseñanza de la profesión, haciendo especial mención de los principios éticos y deontológicos, consustanciales con la misma.

Artículo III. Obligaciones en relación con la profesión

El responsable de Ciberseguridad certificado está obligado, en relación con la profesión, a:

- Acometer su trabajo solo si está cualificado por su formación y experiencia previas, aceptando las responsabilidades del mismo y manteniendo en todo momento un alto grado de objetividad profesional.
- Atribuirse únicamente aquellos niveles de competencia de los que disponga.
- Trabajar únicamente con información obtenida por medios legales y éticos, haciendo uso de la misma exclusivamente para los fines autorizados.
- Tratar a los agentes con los que se relacione en su actuar profesional con el debido respeto y consideración del ámbito de las peculiares competencias de cada uno, pero no permitirá que sean invadidas las áreas específicas de su responsabilidad.
- Tratar a los agentes con los que se relacione en su actuar profesional con el debido respeto y consideración del ámbito de las peculiares competencias de cada uno, pero no permitirá que sean invadidas las áreas específicas de su responsabilidad.
- Promover en público el reconocimiento de la profesión, abstenerse de emitir opiniones contrarias a la buena reputación de la profesión y contrarrestar informaciones falsas o equívocas con respecto a la profesión.

Artículo IV. Obligaciones en relación con sus compañeros de profesión

El responsable de Ciberseguridad certificado está obligado, en relación con sus compañeros de profesión:

- Sin perjuicio de la crítica técnica y metodológica que estimen oportuna en el ejercicio de su profesión, el responsable de Ciberseguridad no desacreditará a sus compañeros ni a otros profesionales que trabajan con sus mismas o diferentes técnicas y hablarán con respeto de las metodologías y los métodos o sistemas de desarrollo que gozan de credibilidad técnica y profesional.
- Revisará el trabajo de otros de forma objetiva y adecuadamente documentada, ofreciendo críticas desde el punto de vista constructivo.
- Reconocerá el trabajo de otros y nunca se atribuirá méritos ajenos.
- Consultará las opiniones de otros profesionales cuando las circunstancias del proyecto le sitúen fuera de las áreas de competencia personales.
- Promoverá el desarrollo profesional de sus compañeros, especialmente de los nuevos profesionales.
- Los conflictos relativos a la profesión entre responsables de Ciberseguridad certificados que no sean constitutivos de delito o falta deberán ser resueltos de la forma más discreta posible. Si la naturaleza del conflicto o la discrepancia de las partes no hiciera posible la resolución se elevaría al Comité de Gestión del Esquema por si se considerase oportuna su intervención antes de recurrir a otras instancias.

Artículo V. Obligaciones en relación con el cliente

El responsable de Ciberseguridad certificado está obligado, en relación con el cliente, a:

- **Actuar con la debida competencia profesional y dedicación al proyecto encomendado**, de la mejor manera posible según sus capacidades. Asimismo, no deberá aceptar mayor número de encargos que aquellos que pueda atender debidamente, ni que superen la capacidad, medios y conocimientos de que disponga.

- **No aceptar** un proyecto **si existe el riesgo de violación del secreto profesional o si supone intereses contrapuestos o una competencia desleal**. No se podrá aceptar un proyecto de un cliente si conlleva la utilización de información obtenida con anterioridad de un cliente distinto, sin el expreso consentimiento de este. El responsable de Ciberseguridad certificado debe informar de la existencia de conflictos de interés o de la posibilidad de que surjan en el futuro, y de que no se realizará el trabajo sin el consentimiento del cliente.

- **Informar veraz y honestamente al cliente** de la viabilidad del proyecto encargado, tanto en su naturaleza funcional como en los costes. No llevará adelante un proyecto a cualquier coste.

- **Facilitar la autonomía del cliente**, ofreciéndole toda la información necesaria y adecuada que le facilite la toma de decisiones sobre el proyecto, según su criterio.

- **Informar cumplidamente a su cliente** de todas aquellas situaciones que puedan afectar a la calidad de su trabajo.

- **Cumplir los objetivos de plazo y presupuesto**, notificando anticipadamente los posibles desvíos en relación a los objetivos y justificando los mismos.

- **Utilizar los recursos del cliente** implicados en un proyecto de forma **adecuada y autorizada**.

- **Fomentar y asegurar la calidad y seguridad de los sistemas, servicios y productos elaborados**. Deberá asimismo garantizar una vida razonable al proyecto acorde a la naturaleza del mismo.

- **Fundar en elementos objetivos las opiniones, informes y documentos** que emita, sin ocultar o desvirtuar los hechos de manera que puedan inducir a error.

- **Aclarar las relaciones que guarda con cualquiera de las partes** cuando emita juicio profesional que sirva de base a terceros para tomar decisiones (obligación de sostener un criterio imparcial y libre de conflicto de intereses).

- nformar al cliente en caso de que los requisitos del proyecto **supongan un conflicto ético**.

Artículo VI. Obligaciones en relación con el secreto profesional

El responsable de Ciberseguridad certificado está obligado, en relación con el secreto profesional, a:

- **Sujetarse al secreto profesional**, como depositario que es de información confidencial, que constituirá un derecho y una obligación de la profesión y que deberá ser respetado incluso después de haber finalizado la prestación de sus servicios, debiendo ser escrupuloso en el cumplimiento de la legislación vigente.

- **No revelar datos o informaciones** de carácter reservado o privado que procedan de un cliente y que haya obtenido por razón de su profesión.

- **Hacer respetar el secreto profesional** a su personal y a cualquier persona que colabore con él en su actividad profesional de forma directa o indirecta, haciendo extensible esta obligación de secreto profesional en la misma forma en que el profesional está obligado, incluso después de haber terminado la relación laboral.

- Únicamente quedarán dispensados de guardar el secreto profesional, previa autorización del presidente del Comité del Esquema RCSEG, aquellos responsables de Ciberseguridad certificados que se encuentren en alguna de las siguientes situaciones:

  - Dispensa de esta obligación por los titulares de la información o autorizados expresamente por éstos para su divulgación.
  - Necesidad de divulgación para evitar un daño propio o de un tercero. En cualquier caso, el deber de secreto continuará siendo aplicable respecto de aquella información cuya divulgación no impida la lesión.
  - Existencia de una ley que autorice la cesión o comunicación de la información a terceros.
  - Existencia de un requerimiento, mandato u orden de autoridad administrativa o judicial que resulte de obligado cumplimiento.

- El responsable de Ciberseguridad certificado que se vea perturbado en el mantenimiento del secreto profesional deberá comunicarlo al Comité de Gestión del Esquema RCSEG.

Artículo VII. Obligaciones en relación con su equipo de trabajo

El responsable de Ciberseguridad certificado está obligado, en relación con el equipo de profesionales o trabajadores que tenga bajo su dirección, gestión u organización, a:

NOTA: Este artículo 7 se refiere a las obligaciones de un RCSEG en relación a su equipo, con independencia que forme parte de él, o no, algún otro RCSEG certificado.

- **Proporcionar las condiciones de trabajo adecuadas**, ajustándose en todo momento a la legalidad vigente y estableciendo procedimientos activos de prevención de prácticas deleznables como el acoso laboral, moral o sexual de los trabajadores.

- Evitar en todo momento la asignación de tareas propias de la profesión a una persona **sin la capacidad adecuada**, evitando en todo momento el intrusismo profesional.

- **Aceptar las responsabilidades del trabajo de socios y subordinados** bajo su dirección profesional. En todo caso, la relación con los colaboradores deberá estar presidida por el respeto mutuo y la calidad en la dirección (extraído del art. 8).

- Establecer o alentar por unas **remuneraciones justas** y en sintonía con la normativa vigente y los convenios colectivos.

- Promover y nunca coartar la f**ormación permanente de los miembros de su equipo** en nuevas estrategias, tecnologías, protocolos de trabajo y actuación que permitan un mejor ejercicio de la profesión y una evolución constante de la calidad de los proyectos.

- Respetar el principio de la l**ibertad de asociación y el derecho a la negociación** colectiva.

- Vigilará que el personal a su cargo **no lleve a cabo actividades ilícitas** ni conductas contrarias al presente Código Ético. (Extraído del art. 8)

Artículo VIII. Relaciones con el personal de la organización

En sus relaciones con el resto de los empleados, directivos y colaboradores de la organización, el responsable de Ciberseguridad certificado:

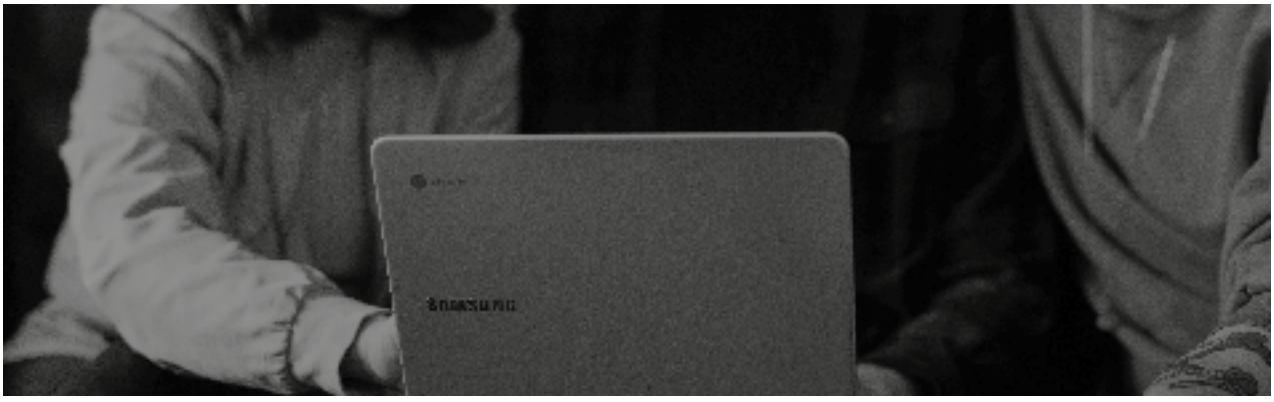
NOTA: En relación a su posible equipo ya se trata en el artículo 7 anterior. Aquí es respecto al resto de personal de la empresa, por lo que se trasladan párrafos de este artículo al anterior, donde tienen mejor encaje.

- Deberá **tratar de forma justa y respetuosa** al resto de empleados o directivos de su organización.

- **Asumirá la responsabilidad de su actuación y la de sus colaboradores**, promoviendo su desarrollo profesional a través de la motivación, la formación y la comunicación.

- Deberá **rechazar cualquier manifestación de acoso** físico, psicológico, moral o de abuso de autoridad, así como cualquier otra conducta contraria a generar un entorno de trabajo agradable, saludable y seguro.

- **Proporcionará siempre toda la información necesaria** para el adecuado seguimiento de la actividad, sin ocultar errores o incumplimientos, y procurando subsanar las carencias que se detecten.



Artículo IX. Relaciones con colaboradores externos y proveedores

En sus relaciones con los colaboradores externos y proveedores, el responsable de Ciberseguridad certificado:

- Establecerá unas **relaciones basadas en la confianza, respeto, transparencia y el beneficio mutuo**.

- **Actuará con imparcialidad y objetividad** en los procesos de selección de este personal, aplicando criterios de competencia, calidad y coste, evitando en todo momento la colisión de intereses.

La contratación de servicios o compra de bienes se deberá realizar con total independencia de decisión y al margen de cualquier vinculación personal, familiar o económica, que pueda poner en duda los criterios seguidos en la selección.

Artículo X. Colaboración con las Entidades de Certificación

Los responsables de Ciberseguridad certificados colaborarán plenamente con cualquier investigación formal sobre infracciones de este Código iniciada por las Entidades de Certificación o para resolver casos específicos de reclamación y/o quejas.

A tales efectos, deberán mantener un registro de todas las reclamaciones presentadas contra ellos, por la actividad desarrollada en el ámbito de validez de la Certificación que les ha sido otorgada y permitir a la Entidad de Certificación el acceso a estos registros.

En el plazo de diez (10) días desde la recepción de la reclamación, deberán enviar una comunicación escrita y copia de la reclamación a la Entidad de Certificación.

Artículo XI. Relación con las autoridades y Administraciones Públicas

Las relaciones con las instituciones, organismos y Administraciones Públicas, estatales, autonómicas y locales, especialmente con los propietarios del Esquema RCSEG, se desarrollarán bajo criterios de **máxima colaboración y escrupuloso cumplimiento de sus resoluciones**.

Las comunicaciones, requerimientos y solicitudes de información deberán ser atendidos con diligencia, **en los plazos establecidos para ello**.

Artículo XII. Desempeño de otras actividades profesionales

Los responsables de Ciberseguridad certificados no realizarán actividades competitivas directas o indirectas contra los copropietarios del Esquema RCSEG y/o la(s) Entidad(es) de Certificación.

A tales efectos, comunicarán a su organización el ejercicio de cualquier otra actividad laboral, profesional o empresarial, remunerada o no, que tenga lugar dentro o fuera del horario de trabajo, o su participación significativa como socio en sociedades o negocios privados, a efectos de evaluar si resultan compatibles con el desarrollo de su actividad o con los fines u objetivos propios de la organización.

Artículo XIII. Aceptación e interpretación del Código Ético

Los responsables de Ciberseguridad certificados tienen el deber de conocer y cumplir el presente Código Ético y habrán de suscribirlo. El Esquema RCSEG exige a los profesionales certificados un alto nivel de compromiso en el cumplimiento de este Código Ético.

Cualquier duda que pueda surgir sobre la interpretación o aplicación del presente documento deberá consultarse con la Entidad de Certificación, quien tiene la obligación de fomentar el conocimiento y cumplimiento del Código e interpretarlo en caso de duda, pudiendo elevar consultas, de estimarse necesario, al Comité de Gestión del Esquema.

Artículo XIV. Incumplimiento del Código Ético

El incumplimiento de alguno de los principios, valores y criterios contenidos en este Código puede acarrear una investigación de la conducta del titular de la certificación y, en última instancia, medidas disciplinarias por parte del correspondiente organismo de certificación que pueden suponer la suspensión o retirada de la certificación.


START UP

III. Competencias y habilidades requeridas al puesto de Responsable de Ciberseguridad

+ Anexos

Competencias y habilidades requeridas al puesto de Responsable de Ciberseguridad

El perfil profesional de esta sección para el director o responsable de Seguridad de la Información se ha obtenido a partir del Marco Europeo de Competencia Electrónica (European e-Competence Framework[1]), concretamente de la norma europea CEN EN 16234-1:2019 (e-Competence Framework (e-CF))[2] y de ESCO (European Skills, Competences, Qualifications and Occupations) [3,4].

[1] http://www.ecompetences.eu/

[2] https://www.ecompetences.eu/get-the-e-cf/

[3] ESCO (European Skills, Competences, Qualifications and Occupations), perfil profesional del director/a de Seguridad de las TIC: https://ec.europa.eu/esco/portal/occupation

[4] ESCO es un proyecto de la Comisión Europea, dirigido por la Dirección General de Empleo, Asuntos Sociales e Inclusión (DG EMPL) que proporciona una clasificación europea multilingüe de capacidades, competencias, cualificaciones y ocupaciones con el objetivo de apoyar la movilidad laboral en Europa y forma parte de la estrategia Europa 2020.

Título del perfil	Perfil del director o responsable de seguridad de la información		
Descripción	Dirige y gestiona la política de seguridad de la información de la organización.		
Misión	Define la estrategia de seguridad de la información y gestiona la implementación en toda la organización. Incorpora la protección proactiva de la seguridad de la información evaluando, informando, alertando y concienciando a toda la organización.		
Entregables	**Responsable de:**	**Encargado de:**	**Colabora con:**
	Política de seguridad de la información.	Base de conocimiento o información. Estrategia de seguridad de la información.	Política de gestión de riesgos. Nueva solución y propuesta de integración de negocios críticos.
Funciones	-Definir la estrategia y las normas de seguridad digital - Contribuir al desarrollo de la política de seguridad de la organización - Gestiona las auditorías de seguridad - Evaluar los riesgos, amenazas y consecuencias - Establecer planes de prevención - Informar y sensibilizar a la dirección general - Promover una cultura de concienciación sobre la seguridad entre todos los usuarios y profesionales de la tecnología de la información - Auditar y asegurar que se apliquen los principios y normas de seguridad de la SI		
e-Competences (e-CF)	A.7. Supervisión de las tendencias tecnológicas		Nivel 4
	D.1.Desarrollo de la Estrategia de Seguridad de la Información		Nivel 5
	E.3.Gestión de riesgos		Nivel 4

Título del perfil	Perfil del director o responsable de seguridad de la información	
	E.8. Gestión de la seguridad de la información	Nivel 4
	E.9.Gobernanza del SI	Nivel 5
Área KPI	Eficacia de la política de seguridad	
Conocimientos esenciales según ESCO (código 2529.1)	- Ciberseguridad - Estrategia de seguridad de la información - Legislación sobre seguridad de las TIC - Normas de seguridad de las TIC - Resiliencia organizativa - Riesgos de seguridad de la red de TIC - Sistemas de ayuda para la toma de decisiones - Técnicas de auditoría	
Habilidades esenciales según ESCO	- Aplicar gestión de riesgos de las TIC - Aplicar gobernanza empresarial - Controlar las tendencias en tecnología - Dirigir ejercicios de recuperación ante desastres - Garantizar el cumplimiento de las normas organizativas de las TIC - Garantizar el cumplimiento de los requisitos legales - Garantizar la confidencialidad de la información - Gestionar los requisitos de seguridad de las TIC - Gestionar planes de recuperación ante catástrofes - Mantener plan de continuidad de operaciones - Utilizar sistemas de apoyo a decisiones	

Nótese que los conocimientos esenciales se especifican en los dominios por lo que no se desarrollarán en esta sección para cada competencia.

Competencia A.7: Vigilancia de las tendencias tecnológicas

Investiga los últimos avances tecnológicos en materia de TIC para comprender la evolución de las tecnologías. Fomenta y explora fuentes internas y externas (incluidas, por ejemplo, actividades de investigación, patentes, actividades de puesta en marcha, comunidades digitales) en busca de ideas y oportunidades innovadoras. Diseña soluciones innovadoras para la adopción o integración de tecnologías y/o ideas existentes o nuevas en productos, aplicaciones o servicios existentes o para la creación de otros nuevos.

En el nivel de dominio 4 de la competencia, se incluye:

- **Valida las tecnologías nuevas y emergentes**, junto con un conocimiento experto del negocio, para prever y articular soluciones para el futuro.
- Crea los **procesos de seguimiento de las tendencias** en toda la organización.

En concreto, las habilidades que se han identificado en esta competencia y nivel son:

- **Controlar las tendencias en tecnología**

Competencia D.1: Desarrollo de la Estrategia de Seguridad de la Información

Define y hace aplicable una estrategia organizativa formal, un alcance y una cultura para mantener la seguridad de la información frente a las amenazas externas e internas. Analiza la estrategia empresarial y tecnológica junto con las tendencias del panorama de las amenazas para anticipar posibles vulnerabilidades y requisitos de mitigación de riesgos. Realiza un seguimiento de las expectativas legales, reglamentarias y sociales relacionadas con la seguridad de los servicios y los datos sensibles. Proporciona la base para la gestión de la seguridad de la información, incluida la identificación de funciones y la responsabilidad. Utiliza normas definidas para crear objetivos de integridad, disponibilidad y privacidad de la información.

En concreto, para el nivel 5, proporciona un liderazgo estratégico para integrar la seguridad de la información en la cultura de la organización. En este nivel, se han identificado las siguientes habilidades:

Aplicar gobernanza empresarial, por ejemplo:

- Asesorar en materia de ciberseguridad a los responsables de los Servicios y a los responsables de la Información de las organizaciones. Así como a la Dirección y, en general a las partes interesadas, como proveedores en la cadena de suministro.
- Capacidad para relacionar la naturaleza y contexto de los Servicios con los riesgos de ciberseguridad inherentes a su actividad, para poder desarrollar una estrategia de ciberseguridad que sea consecuente con los mismos.
- Capacidad y compromiso para responsabilizarse de la determinación de la Declaración de Aplicabilidad, como muestra de conformidad para impulsar y supervisar todas las medidas de seguridad que resulten de aplicación.
- Capacidad para elaborar o supervisar la elaboración de políticas, normas y procedimientos internos relacionados con la seguridad de los sistemas de información que soportan los servicios y la información que éstos manejan.

Garantizar el cumplimiento de los requisitos legales, por ejemplo:

- Aplicar adecuadamente la normativa jurídica y de cumplimiento que se vaya promulgando o modificando, relacionada con la ciberseguridad, asesorando asimismo en su aplicación a la organización.
- Capacidad de organización y análisis para clasificar e interpretar, respecto a la organización donde presta sus servicios, las diferentes guías que publique el CCN y otras organizaciones, así como los demás actores involucrados en la ciberseguridad.

Competencia E.3: Gestión de riesgos

Implementa la gestión de riesgos en los sistemas de información mediante la aplicación de la política y el procedimiento de gestión de riesgos definidos por la empresa. Evalúa el riesgo para la actividad de la organización, incluidos los recursos web, en la nube y móviles. Documenta el riesgo potencial y los planes de contención.

El nivel de dominio 4 de la competencia E.3 incluiría:

- **Lidera la definición y aplicación de una política de gestión de riesgos** teniendo en cuenta todos los posibles condicionantes, incluidos los técnicos, económicos y políticos.

- **Delega las asignaciones**.

En concreto, las habilidades que se han identificado en esta competencia y nivel son:

- **Aplicar gestión de riesgos de las TIC**, por ejemplo:
  - Identificar, en colaboración con los responsables de los Servicios y la Información, los posibles riesgos de seguridad, calcular su valor y consensuar las acciones de mitigación para aquellos que se consideren inaceptables en base al umbral de riesgo establecido en la organización.
  - Dirigir y gestionar la realización de las sucesivas nuevas iteraciones del análisis de riesgos.

Competencia E.8: Gestión de la seguridad de la información

Gestiona la política de seguridad de la información y los sistemas teniendo en cuenta las amenazas técnicas, humanas, organizativas y de otro tipo, en consonancia con la estrategia empresarial y de TI, y reflejando la cultura de riesgo de la organización. Despliega y gestiona los recursos operativos y especializados (por ejemplo, análisis forense, inteligencia de amenazas y detección de intrusiones) necesarios para garantizar la capacidad de gestionar los incidentes de seguridad, y formula recomendaciones para la mejora continua de la política y la estrategia de seguridad.

Específicamente, para el nivel 4, dirige la integridad, la confidencialidad y la disponibilidad de los datos almacenados en los sistemas de información y cumple con todos los requisitos legales. En concreto, las habilidades que se han identificado en esta competencia y nivel son:

+ **Dirigir ejercicios de recuperación ante desastres**, por ejemplo:

» Diseñar y probar los planes de respuesta ante incidentes de ciberseguridad.

+ **Garantizar la confidencialidad de la información**, por ejemplo:

» Colaborar con el DPD, caso de que se produzca una violación de datos personales, según dispone el art. 33 RGPD.

+ **Gestionar los requisitos de seguridad de las TIC**, por ejemplo:

» Conocer y gestionar los informes procedentes de controles y amenazas, verificando la idoneidad de la protección y su ajuste de ser necesario.

» Interpretar informes forenses, reflexionar sobre las lecciones aprendidas, definir planes de acción y hacer seguimiento de su aplicación.

» Verificar, junto al responsable del Sistema, que se efectúe el mantenimiento (gestión de versiones y parches de seguridad) de los componentes del sistema, así como su mantenimiento de hardware.

Gestionar planes de recuperación ante catástrofes.

» Elaborar y supervisar planes de contingencia y formación.

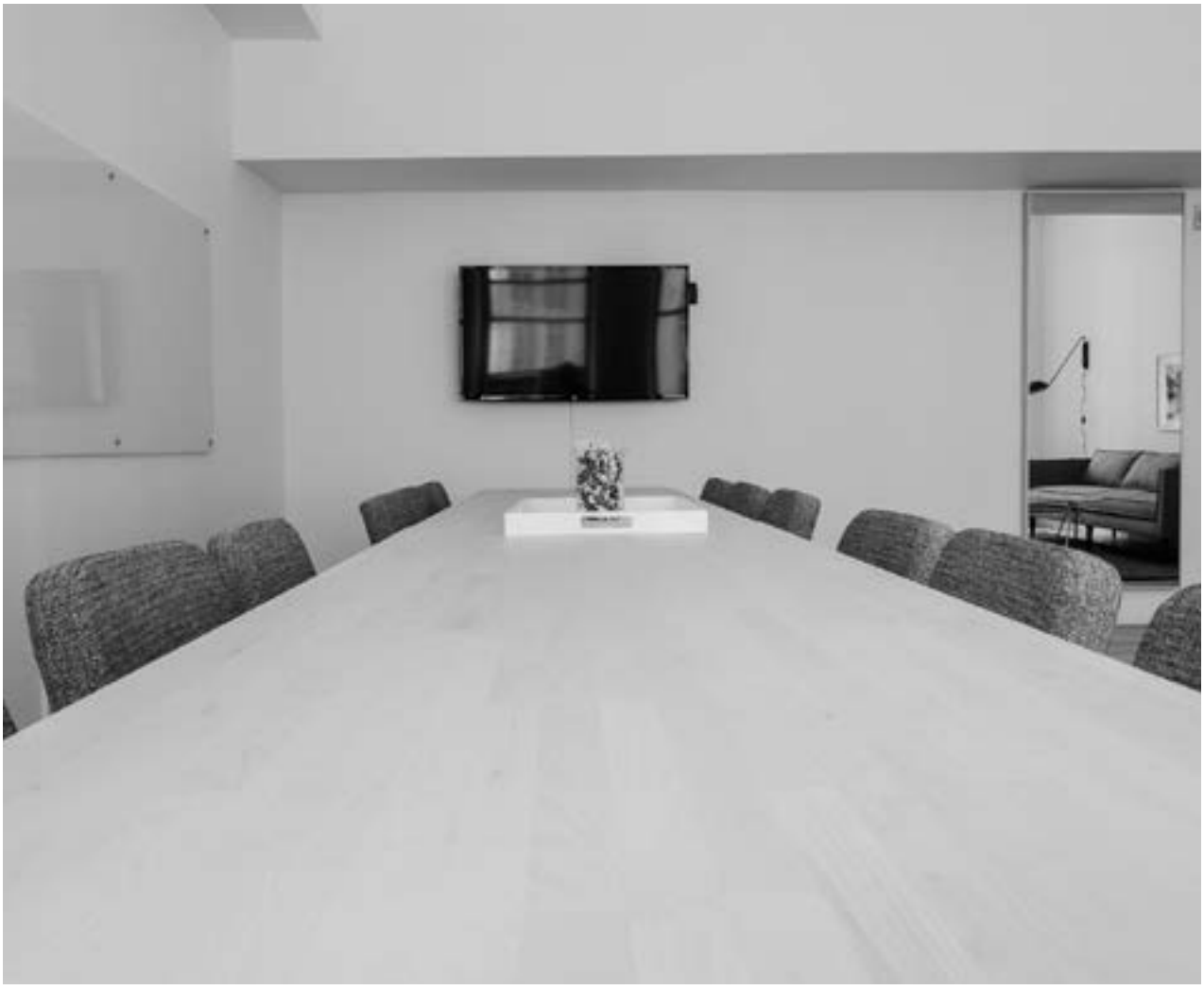
Mantener plan de continuidad de operaciones.

» Gestionar los diferentes incidentes de seguridad que se produzcan en la organización.

» Definir el alcance e impacto ocasionado por un determinado ciberincidente.

» Coordinar la respuesta ante una crisis de ciberseguridad, incluyendo la coordinación con el CSIRT de referencia hasta su resolución y vuelta a la normalidad.

» Analizar y gestionar los informes sobre la actividad de los usuarios, a ser posible apoyándose en herramientas automatizadas, con el objetivo de detectar conductas sospechosas.



Competencia E.9: Gobernanza del SI

Define, despliega y controla la gestión de los sistemas y servicios de información y los datos de acuerdo con los imperativos de la empresa. Tiene en cuenta todos los parámetros internos y externos, como la legislación y el cumplimiento de las normas del sector, para influir en la gestión de riesgos y el despliegue de recursos con el fin de lograr un beneficio empresarial equilibrado.

En el nivel 5 la competencia E.9 incluiría:

- Define y alinea la estrategia de gobierno de la SI incorporándola a la estrategia de gobierno corporativo de la organización.

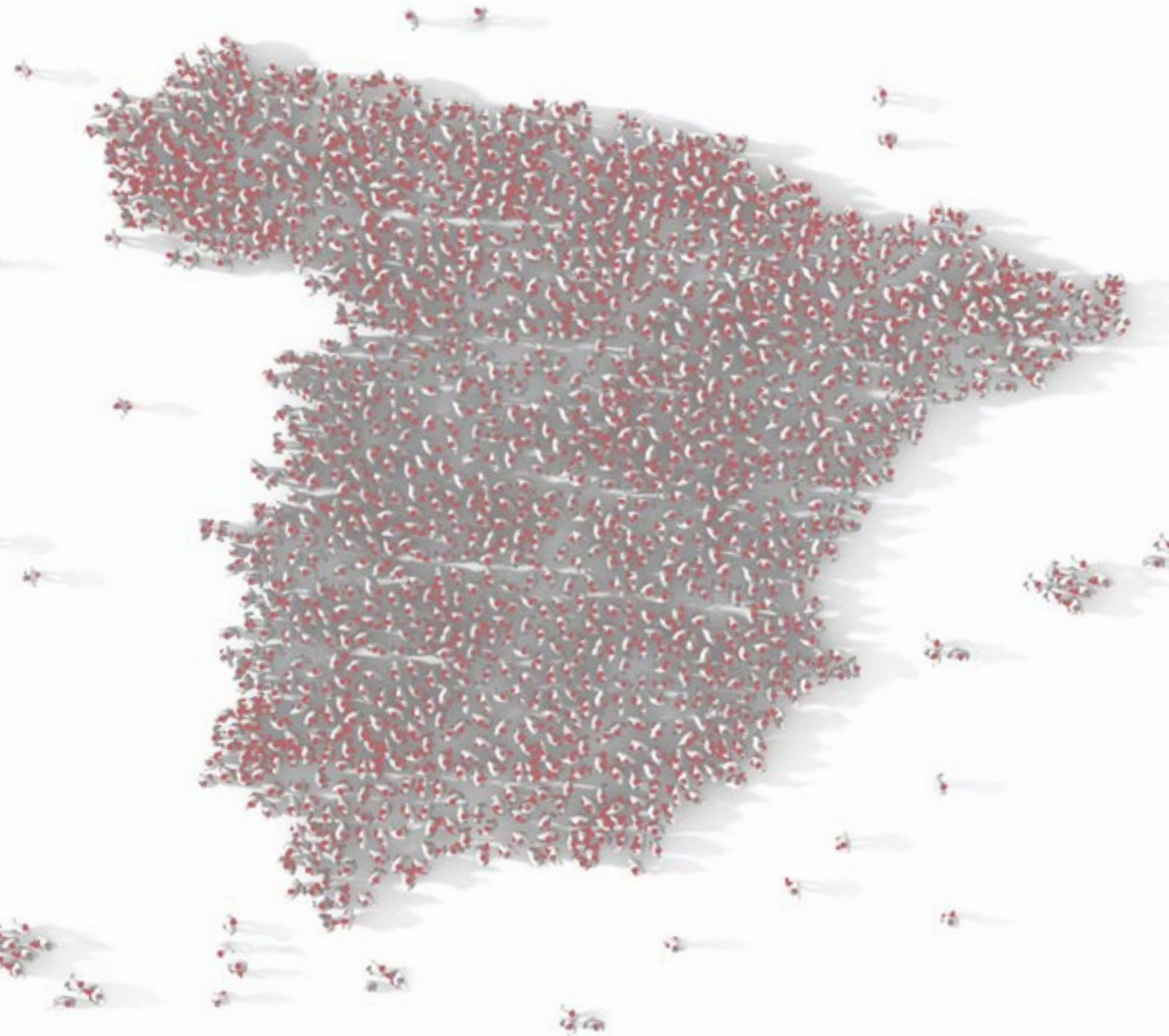
- Adapta la estrategia de gobierno de la SI para tener en cuenta nuevos acontecimientos significativos derivados de cuestiones jurídicas, económicas, políticas, empresariales, tecnológicas o medioambientales.

En concreto, las habilidades que se han identificado en esta competencia y nivel son:

- Garantizar el cumplimiento de las normas organizativas de las TIC, por ejemplo:
  - Analizar e interpretar los contratos y acuerdos de prestación de servicio de proveedores externos, como pueden ser prestadores de servicios de Cloud, verificando que sean acordes con los requisitos de seguridad de la organización y de los sistemas de información que se apoyen en ellos.
  - Analizar las valoraciones en las cinco dimensiones de la seguridad de los servicios y de la información que estos manejan, efectuadas por sus responsables, asesorándolos con criterio respecto a las mismas.
  - Capacidad de decisión para convocar reuniones extraordinarias del Comité de Seguridad, cuando así lo aconsejen las circunstancias.
  - Capacidad para elaborar o supervisar las diferentes métricas e indicadores relacionados con la seguridad.

+++

FORO NACIONAL DE CIBERSEGURIDAD



FORO NACIONAL DE CIBERSEGURIDAD