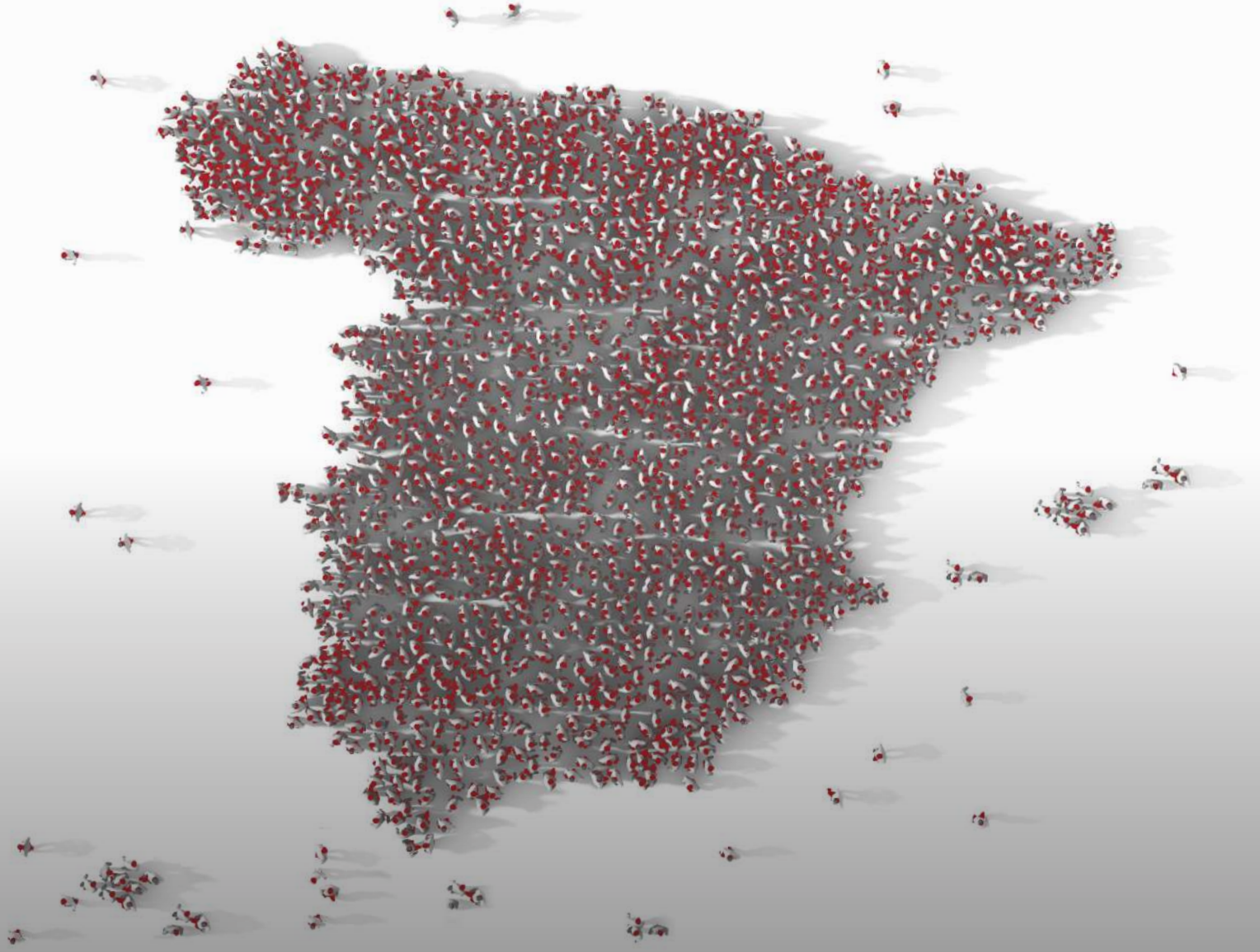
FORO NACIONAL DE CIBERSEGURIDAD



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.

Motor de la colaboración público-privada | Foro Nacional de Ciberseguridad +

Índice

+ Informe global de trabajos realizados

Motor de la colaboración público-privada | Foro Nacional de Ciberseguridad +

Antecedentes

+ 01.

Antecedentes

El modelo de ciberseguridad español integra a diferentes actores en un ecosistema común, ampliamente regulado y especializado, donde se fomenta la colaboración, cooperación y coordinación de todos ellos, entendiendo la ciberseguridad como una Política de Estado bajo el paraguas de la Seguridad Nacional.

La Estrategia Nacional de Ciberseguridad (ENCS) aprobada por el Consejo de Seguridad Nacional en abril de 2019, apunta a la **colaboración público-privada** como elemento clave e impulsa a la materialización de dicha colaboración a través del **Foro Nacional de Ciberseguridad**, un lugar donde integrar a representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones, organizaciones sin ánimo de lucro, entre otros, a fin de potenciar y crear sinergias público-privadas.

La creación del Foro fue aprobada por el Consejo de Seguridad Nacional el 21 de febrero de 2020, como grupo de trabajo del Consejo Nacional de Ciberseguridad. Su constitución se llevó a cabo el 22 de julio de 2020.

La composición del Foro, se determinó con el objetivo de **aglutinar la mayor representatividad** posible de organismos públicos y privados y de la sociedad en el ámbito de la ciberseguridad. Presidido por el Departamento de Seguridad Nacional, consta de dos vicepresidencias a cargo del Centro Criptológico Nacional y el Instituto Nacional de Ciberseguridad (INCIBE) y está compuesto, además de por los organismos públicos con competencia en la materia, por **15 organizaciones representantes de la sociedad civil y el sector privado**: la Cámara de Comercio de España, la CEOE, CEPYME, Asociación de Autónomos ATA, CRUE Universidades, la Asociación Española de Usuarios de Telecomunicaciones AUTELSI, la red española de Equipos de Respuesta a Ciberincidentes CSIRT.es, medios de comunicación especializados, como Ediciones CODA y Editorial Borrmart, Fundación ESYS, Asociación Internacional de Auditores ISACA, Asociación empresarial para el Fomento de la Seguridad de la Información (ISMS Forum), Red de Excelencia Nacional de Investigación en Ciberseguridad y los *think tanks* Thiber y el Real Instituto Elcano.

La creación del Foro fue aprobada por el Consejo de Seguridad Nacional el 21 de febrero de 2020, como grupo de trabajo del Consejo Nacional de Ciberseguridad

Trabajos realizados

+ 02.

Trabajos realizados

Las primeras líneas de trabajo del Foro, aprobadas por el Consejo Nacional de Ciberseguridad, se han centrado en el estudio y propuesta de iniciativas dirigidas al aumento de la cultura de ciberseguridad; el apoyo a la industria e I+D+i y la formación y talento en ciberseguridad, acciones todas ellas alineadas con medidas recogidas en la ENCS. Para su ejecución se crearon tres grupos de trabajo en formato de coliderazgo público-privado.

1

El grupo de cultura de ciberseguridad, co-liderado por el **Departamento de Seguridad Nacional**, la asociación **ISMS Forum** y la **Fundación Borreda**, que ha elaborado un **Informe sobre La Cultura de ciberseguridad en España**.

2

El grupo de apoyo a la industria e I+D+i, co-liderado por el **Instituto Nacional de Ciberseguridad** (INCIBE) y la **Cámara de Comercio de España**, que ha elaborado el **Informe sobre industria e investigación españolas en ciberseguridad**.

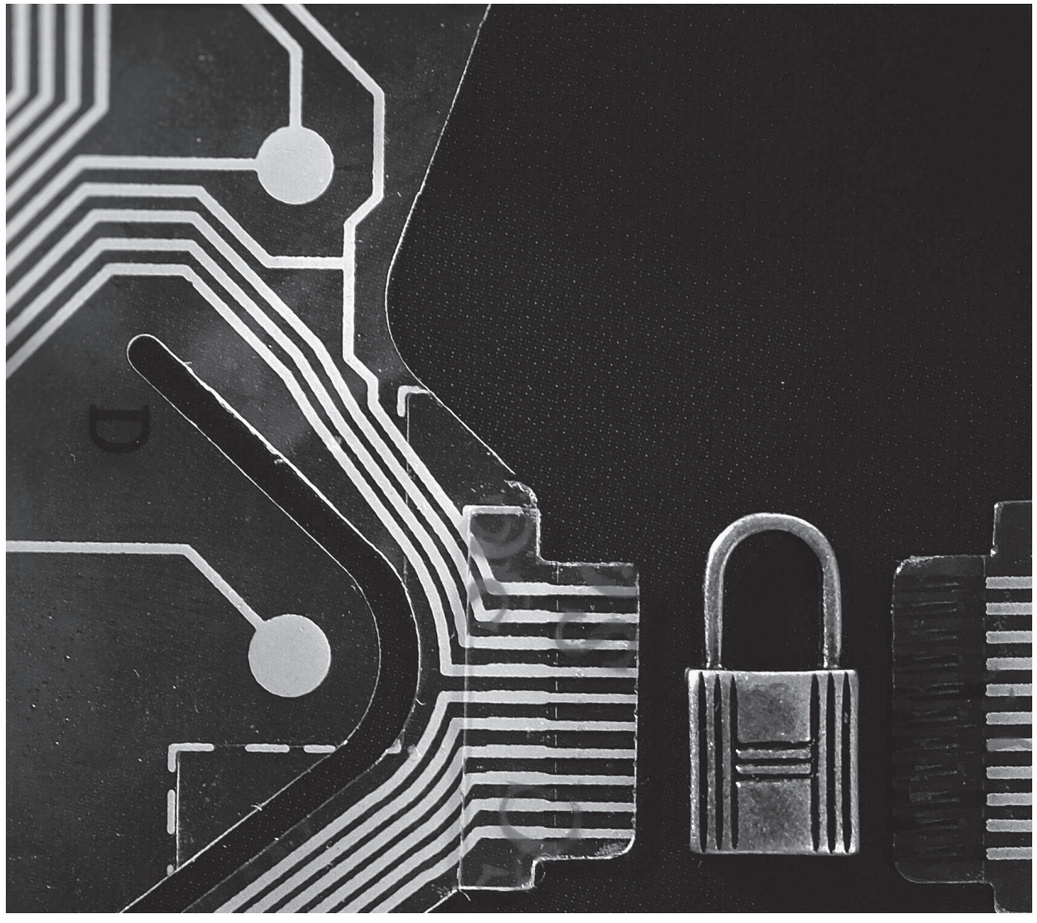
3

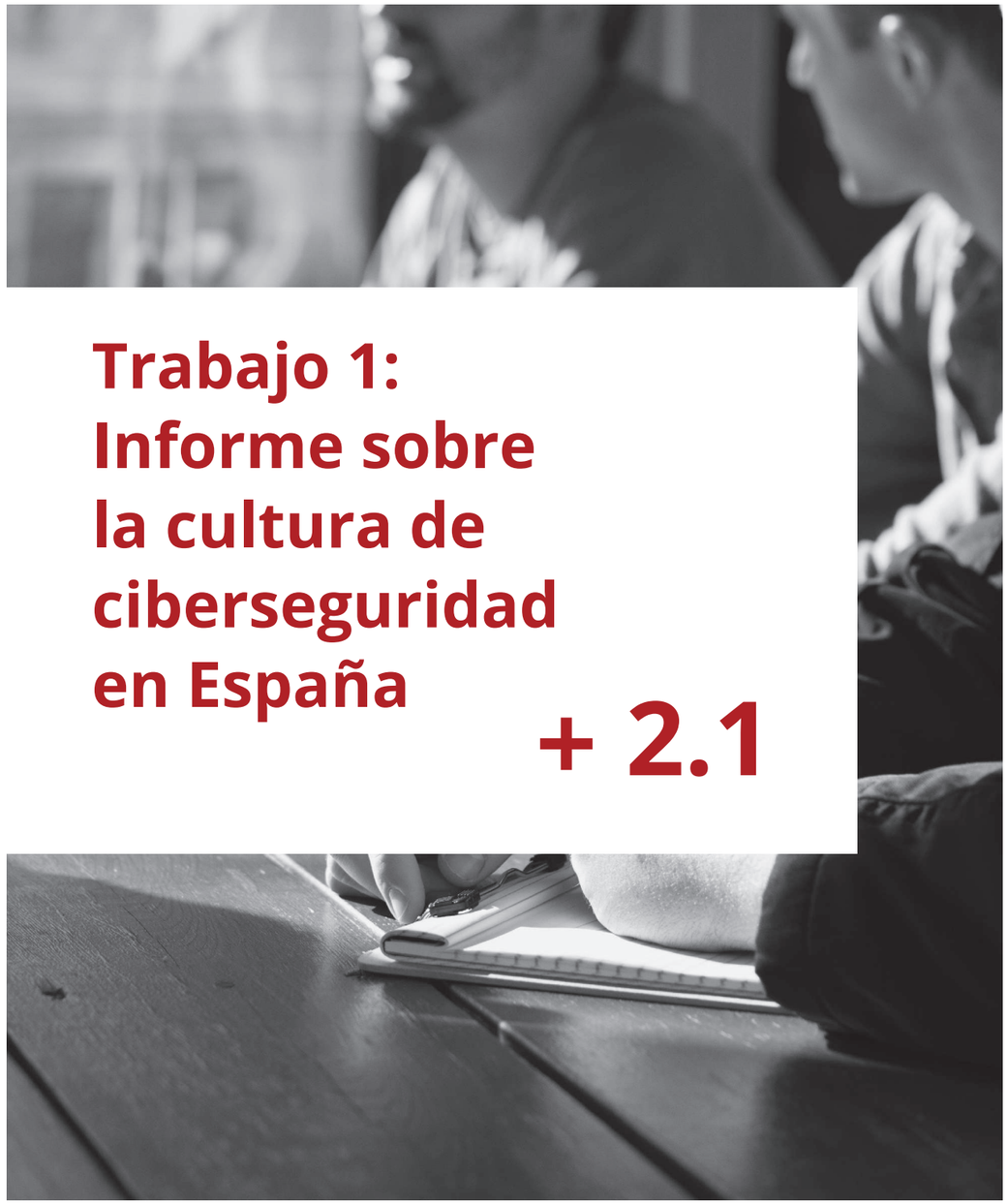
El grupo de formación, capacitación y talento en ciberseguridad, co-liderado por el **Centro Criptológico Nacional** y la **CRUE TIC**, que se ha encargado de elaborar un **Esquema nacional de certificación de responsables de ciberseguridad**.

A petición de una asociación sectorial y con el apoyo del Mando Conjunto del Ciberespacio, se ha creado un nuevo grupo que está diseñando el esquema de estudio para identificar las necesidades y retos de la **colaboración público-privada en materia de ciberdefensa**. El objetivo que se persigue con dicho trabajo es contar con un conocimiento más amplio y analizar las capacidades actuales y necesidades genéricas de la ciberdefensa nacional, a fin de avanzar en propuestas o áreas de desarrollo de I+D+i.

Por último, El Real Instituto Elcano, como miembro del foro, ha impulsado la creación de un nuevo grupo de trabajo sobre Regulación que, coliderado con el Ministerio del Interior, tiene como objetivo instaurar un procedimiento reglado de interacción en los ámbitos de regulación de alto impacto, transversales y sectoriales de ciberseguridad que permita al sector privado colaborar con el público desde el inicio del proceso hasta su conclusión y seguimiento para superar las limitaciones del mecanismo de consulta pública vigente.

A continuación, se presenta un resumen ejecutivo de cada trabajo realizado.





Trabajo 1: Informe sobre la cultura de ciberseguridad en España

+ 2.1

Trabajo 1: Informe sobre la cultura de ciberseguridad en España

Elaborado por el Grupo de Trabajo 1 de cultura de ciberseguridad.

2.1.1. ¿Por qué este informe?

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, 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.

La Estrategia Nacional de Ciberseguridad (ENCS) de 2019 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.

Puesto que la ciberseguridad es una responsabilidad compartida, las Administraciones Públicas deben mantener una coordinación eficaz con el sector privado, la ciudadanía y la sociedad civil.

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.

Con este fin, el Foro Nacional de Ciberseguridad creó el Grupo de Trabajo de cultura de ciberseguridad, que decidió comenzar sus trabajos mediante un 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.

2.1.2. ¿Qué entendemos por cultura de ciberseguridad?

El Informe define la **cultura de ciberseguridad**, *como 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 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.

2.1.3. ¿Cuáles son los objetivos del Informe?

El Informe tiene **4 objetivos principales:**

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.

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.

Este objetivo consta a su vez de ocho ejes, que coinciden con las medidas recogidas por la ENCS:

» 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.

» Potenciar actuaciones encaminadas al incremento de la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional.

» Impulsar iniciativas y planes de alfabetización digital en ciberseguridad.

- 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.
- 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.
- 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.
- Promover la concienciación y formación en ciberseguridad en los centros de enseñanza, adaptada a todos los niveles formativos y especialidades.
- 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.

Estos ejes de acción identifican posibles áreas donde se pueden realizar mejoras que puedan ayudar a 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 la 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 el impulso de la alfabetización digital.

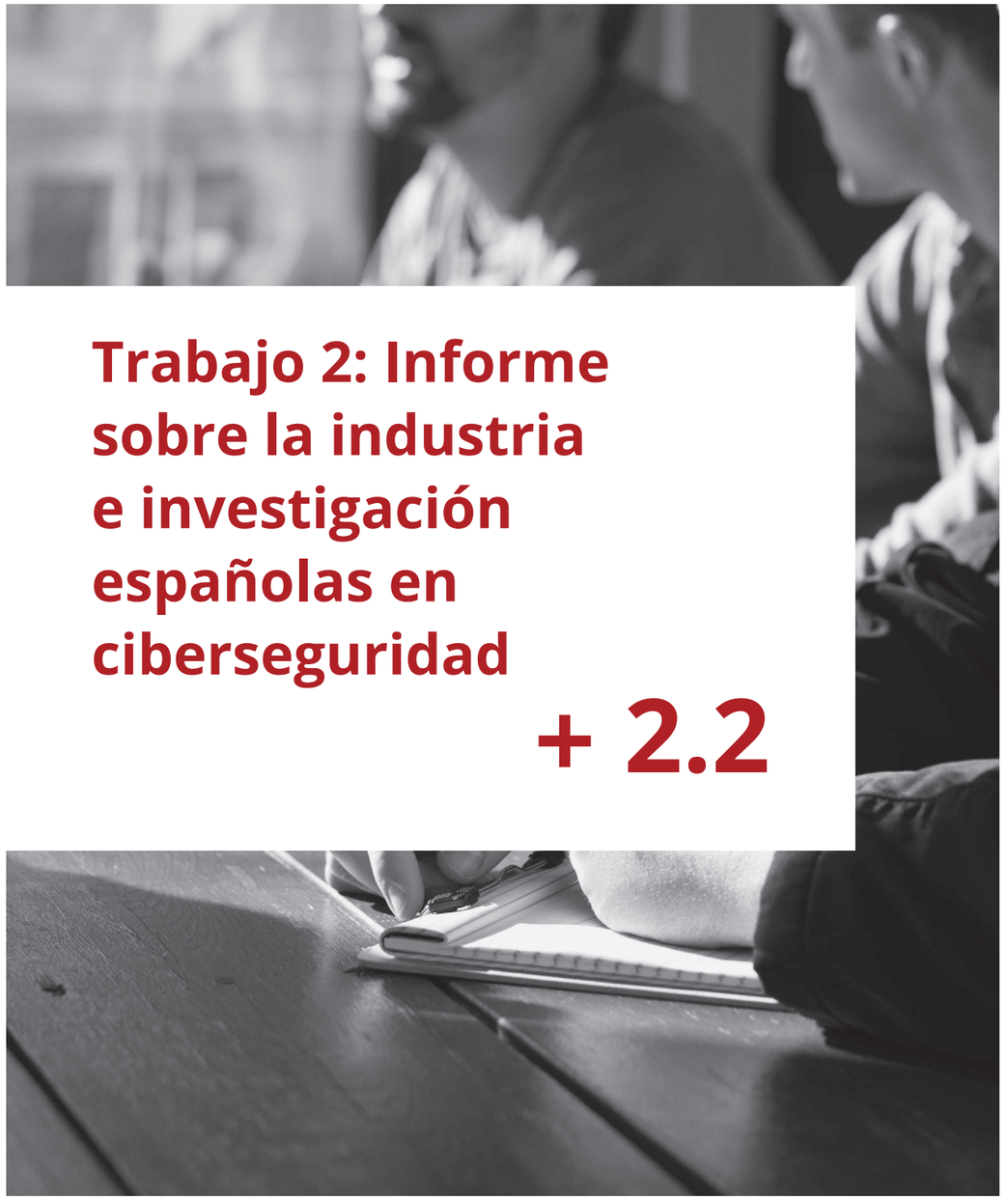
Sin duda, la medida más importante es la necesidad de contar con una visión global y exacta del estado de la cultura de ciberseguridad en la sociedad, así como del impacto de las iniciativas recogidas y de las futuras campañas. Este cuadro de mando sería parte de un **Observatorio para la elaboración 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 medición de la cultura de ciberseguridad en España.

2.1.4. Conclusiones

El proceso de digitalización y transformación digital de nuestra sociedad se ha visto acelerado por la pandemia de la 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, en consecuencia, es imprescindible conocer los riesgos a los que se está expuesto. Por este motivo, 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 elaborado 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 con la sociedad en general, e incrementar la coordinación, eficacia y eficiencia de las actuales iniciativas, con el convencimiento que una mayor cultura de ciberseguridad que nos hará más fuertes y resilientes ante los desafíos que tenemos que afrontar.



Trabajo 2: Informe sobre la industria e investigación españolas en ciberseguridad

+ 2.2

Trabajo 2: Informe sobre la industria e investigación españolas en ciberseguriad

Elaborado por el Grupo de Trabajo 2 de apoyo a la industria e I+D+i.

El ecosistema español de ciberseguridad ha venido desarrollándose durante los últimos veinte años a partir de unas sólidas bases legislativas y con el liderazgo de organismos gubernamentales, centros tecnológicos, universidades y compañías usuarias y proveedoras del sector privado. 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 analizasen indicadores específicos de la industria e investigación, la posición descendería en el ranking: los resultados de la red de investigación no están siendo transferidos a la industria, la utilización de tecnología española y europea es escasa, y la penetración en el mercado nacional de pymes especializadas con excelentes productos y servicios es insuficiente.

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 (FNCS) puede contribuir a eliminar dichos silos e impulsar el trabajo conjunto de todos los actores.

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.

2.2.1. ¿Cómo mejorar el conocimiento aplicado de ciberseguridad?

La base de la mejora se encuentra en una adecuada medición, orientada a precisar los siguientes puntos:

Quién
Cadena de valor global de la ciberseguridad

Qué
Taxonomía de las competencias en ciberseguridad

Cómo y cuánto
Barómetro de ciberseguridad en la industria e investigación

Dónde
Observatorio integral de la ciberseguridad

El estudio de la cadena de valor completa, con inclusión y categorización de nuevos actores y roles, permitirá un mayor conocimiento del ecosistema, de las capacidades disponibles y contribuirá a la eliminación de las barreras entre los mismos.

La propuesta de cadena de valor incluye una tipificación de los actores por roles (decisores, facilitadores, conocedores, desarrolladores, apoyos y clientes), por tamaño y por función en la cadena de valor.

La desconexión entre industria e investigación constituye el eslabón más débil entre los dos grandes ámbitos de la cadena de valor global. Se debe 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.

Disponer de una taxonomía común y alineada con los criterios europeos permite la categorización de los productos y servicios del mercado, los dominios de aplicación, investigación y conocimiento. Además, facilita el mapeado equilibrado de las diferentes entidades que investigan, prestan y demandan servicios de ciberseguridad.

La realidad actual es que no existe una taxonomía única de ciberseguridad. La investigación considera oportuno trabajar con la taxonomía JRC creada por la Comisión Europea, contra la que se coteja la comunidad de I+D+i internacional. Por su parte, la industria habitualmente se mapea en los productos y servicios de ciberseguridad de la taxonomía ECSO, que se ha convertido en referencia a nivel europeo.

Para incrementar la madurez del ecosistema y evitar el gap existente a nivel nacional y europeo, es crítico consensuar una taxonomía común aplicable a I+D+i e industria, que podría basarse en una evolución de la planteada en el Informe. Se propone continuar con estos trabajos y realizar un piloto para verificar su validez.

La medición del nivel de madurez de la industria e investigación debe materializarse en forma de barómetro que recopile los indicadores clave, bien sea para un análisis específico (Barómetro de industria e investigación) o como componente de un barómetro más amplio (Barómetro Integral de la Ciberseguridad).

El barómetro debe identificar los indicadores necesarios para medir la madurez de los componentes identificados en la taxonomía anterior y en cada uno de los actores de la cadena de valor, y es imprescindible para medir y conocer la situación actual en España, compararnos con Europa y observar su evolución.

Para la elaboración y seguimiento del Barómetro Integral de la Ciberseguridad se propone la creación de un Observatorio de la Ciberseguridad, en base a la colaboración público-privada y en el que participen todos los actores de la cadena de valor global, especialmente investigación e industria.

2.2.2. ¿Cuáles son los retos de ciberseguridad de las pymes?

El colectivo de las pymes no es ajeno al aumento en frecuencia y gravedad de los incidentes de seguridad.

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, por lo que es necesario que éstas se incorporen a los proyectos asociados a su ejecución a través del Plan de Recuperación, Transformación y Resiliencia.

El reducido tamaño medio de las empresas españolas puede suponer un reto a la hora de abordar las necesidades digitales de la empresa y, particularmente, las referidas a la ciberseguridad. La adaptación y personalización a las circunstancias concretas de la pyme debe estar en la base de todas las acciones.

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:

Seis propuestas para dar respuesta a los retos de la ciberseguridad de las pymes españolas

- **Elevar el nivel de sensibilización de las pymes** acerca de la existencia de riesgos de ciberseguridad.
- **Reforzar las competencias digitales en ciberseguridad de las pymes**, a través de capacitación y herramientas.
- **Hacer una prospectiva de programas internacionales de apoyo a la ciberseguridad en las pymes.**
- **Definir métricas comunes, estandarizadas y centralizadas para la medición del nivel agregado de ciberriesgo sobre las pymes en España.**
- **Construir una matriz que permita categorizar las pymes en función de características como tamaño, sector, nivel de madurez digital y alfabetización del capital humano, criticidad de la información y situación económica de la pyme.** El objetivo último es adaptar y personalizar los contenidos y herramientas de ciberseguridad a las circunstancias concretas de la empresa.
- **Promover el desarrollo y favorecer la difusión en el mercado de productos y servicios de ciberseguridad con la capilaridad adecuada para llegar a pymes y autónomos.**

Para implementar y ejecutar las propuestas y hacerlo de la forma más eficiente posible es recomendable utilizar las instituciones ya existentes. Para ello, es necesario contar con la participación coordinada de las entidades y organismos que tienen una destacada cercanía con las pymes españolas.

2.2.3 ¿Cómo mejorar la colaboración público–privada en este ámbito?

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.

Se propone la creación de un ecosistema de industria e investigación en ciberseguridad (EI2C) en conexión con el resto de los ecosistemas. 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. Su implantación debe coincidir con la operatividad de la Red y Comunidad de Centros Nacionales de Coordinación de la UE.

Competencialmente, el EI2C debe especializarse 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.

Para asegurar su funcionamiento y capacidad de atracción, es necesario dotar al EI2C de un conjunto de instrumentos, de una agenda de investigación y de un buen sistema de gobernanza.

Los instrumentos son necesarios para estimular la participación de los distintos actores de la comunidad de industria e investigación (decisores, facilitadores, conocedores y desarrolladores) y evitar su desplazamiento a otros ecosistemas europeos o tecnológicos donde se ofrezcan mejores incentivos.

En particular, se considera necesario crear un presupuesto nacional de ciberseguridad para desarrollar las medidas previstas en la ENCS. Su creación, cuantía y finalidad deben figurar en el Plan Nacional de Ciberseguridad.

La definición de una agenda estratégica de investigación e innovación es fundamental para incrementar la autonomía tecnológica e industrial nacional y coordinar las prioridades y programas públicos y privados. Dentro de ella, se deben definir las capacidades tecnológicas e industriales de ciberseguridad críticas para la seguridad nacional y los instrumentos para desarrollarlas. Su elaboración debería figurar en el Plan Nacional de Ciberseguridad.

Finalmente, se propone dotar al EI2C de un sistema de gobernanza (hub) que lidere el desarrollo de la industria e investigación nacional asegurando la participación de los sectores público y privado en todas las fases del proceso de colaboración.

La adopción de las propuestas es imprescindible si se aspira a potenciar la autonomía estratégica nacional reivindicada en la ENCS, reducir la actual dependencia y aumentar la cuota nacional del mercado en línea con los objetivos de la Unión Europea en materia de tecnologías de ciberseguridad.

Estas propuestas contribuirán al desarrollo de la Línea de acción 5 de la ENCS, y en particular a las medidas 1, 2 (dinamizar el sector industrial), 3 (fortalecer la autonomía, propiedad intelectual y la seguridad nacional) y 9 (impulsar programas de I+D+i).

2.2.4 ¿Cuáles son las oportunidades para la I+D+i?

Para posicionar nuestra tecnología en el panorama internacional, se deben abordar una serie de propuestas que contribuirán de manera estructural a fomentar el desarrollo de tecnología española de ciberseguridad y a estimular su consumo.

Es necesario definir una agenda estratégica de investigación e innovación (SRIA) para España en el ámbito de la ciberseguridad, alineada con las prioridades de la UE, nuestra ENCS, y basada en taxonomías de ciberseguridad aceptadas internacionalmente.

Se han identificado inicialmente cinco líneas de investigación alineadas con la ENCS:

- **Desarrollar la protección de la identidad digital** para mejorar la protección de la ciudadanía, el tejido empresarial y la confiabilidad de los servicios electrónicos ofrecidos por las administraciones públicas.

- **Impulsar la creación de una red de laboratorios 5G** que ponga el foco en la ciberseguridad dentro de los procesos de diseño, despliegue y operación.

- **Abrir una línea estratégica de investigación en seguridad e inteligencia artificial** que sirva como marco de actuación para ubicarnos a la vanguardia científico-tecnológica en este campo y facilite la transferencia a la industria.

- **Abrir una línea estratégica de investigación en tecnologías cuánticas aplicadas a los desafíos de ciberseguridad**. Esta línea aparece reflejada en la Estrategia Europea de Ciberseguridad para la Década Digital al mencionar la creación del ciber-escudo europeo basado en comunicaciones cuánticas.

- **Abrir una línea estratégica de investigación en seguridad por diseño, gestión de ciberseguridad y cadena de suministro q**ue dé respuesta a retos actuales de la industria nacional. Su desarrollo está previsto en la Línea de acción 5 (medida 3) de la ENCS y en la Cybersecurity Act.

Es necesario diseñar nuevos modelos de financiación que hagan a estas líneas de investigación sostenibles

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.

Es necesario diseñar nuevos modelos de financiación que hagan a estas líneas de investigación sostenibles y que conviertan a nuestro ecosistema en un referente internacional.

Por ello, es clave llevar a cabo un estudio comparativo de las capacidades I+D+i y de los modelos de financiación, tomando como referencia modelos de financiación pública y privada diferentes al español y que puedan considerarse referentes de éxito. Las conclusiones del estudio se orientarán a seleccionar y priorizar los instrumentos más adecuados para financiar las líneas de investigación que formen parte de la SRIA.

La cohesión sectorial de las actividades de I+D+i en ciberseguridad adquiere un protagonismo estelar como catalizador de la eficiencia.

El primer movimiento pasa por la creación de una red de competencia en ciberseguridad a nivel español a imagen de los cuatro pilotos europeos: SPARTA, CyberSec4Europe, ECHO y CONCORDIA. Para agilizar su arranque, se recomienda apoyarse en los lugares con mayor concentración de capacidades de I+D+i en ciberseguridad.

El segundo paso será crear un mapa exhaustivo de capacidades en I+D+i de ciberseguridad completo y detallado, que contemple la I+D+i empresarial y las disciplinas de especialización que puedan darse en cada nodo.

Para poner en valor todo el trabajo y proyectar su calidad y competitividad se propone una campaña de promoción de la calidad de la tecnología nacional de ciberseguridad que inculque confianza en el tejido empresarial consumidor.

La prioridad inicial debe orientarse hacia el mercado español: organizaciones consumidoras de ciberseguridad y empresas de soluciones y servicios de ciberseguridad que se encargan de llevar la tecnología a los consumidores. En segunda instancia, la campaña se dirigirá hacia geografías internacionales que tengan a España como referente (LATAM) o a economías geopolíticamente afines (como el Espacio Económico Europeo).

2.2.5 ¿Cómo podemos generar, transformar, retener y atraer el talento?

El talento en ciberseguridad es un factor de producción escaso, de oferta inelástica, y por el que se compite a escala global. Los plazos necesarios para la formación de este capital humano varían en función del perfil, experiencia y conocimientos, aunque son, en general, largos.

Resulta imprescindible sensibilizar vocaciones tempranas cuanto antes, en colegios y centros de enseñanza secundaria. Esta acción debe estar apoyada en becas y ayudas directas a alumnos destacados, así como en financiación para la dotación de infraestructuras de laboratorio, además de dar visibilidad a las oportunidades de desarrollo profesional para los jóvenes en medios de comunicación social.

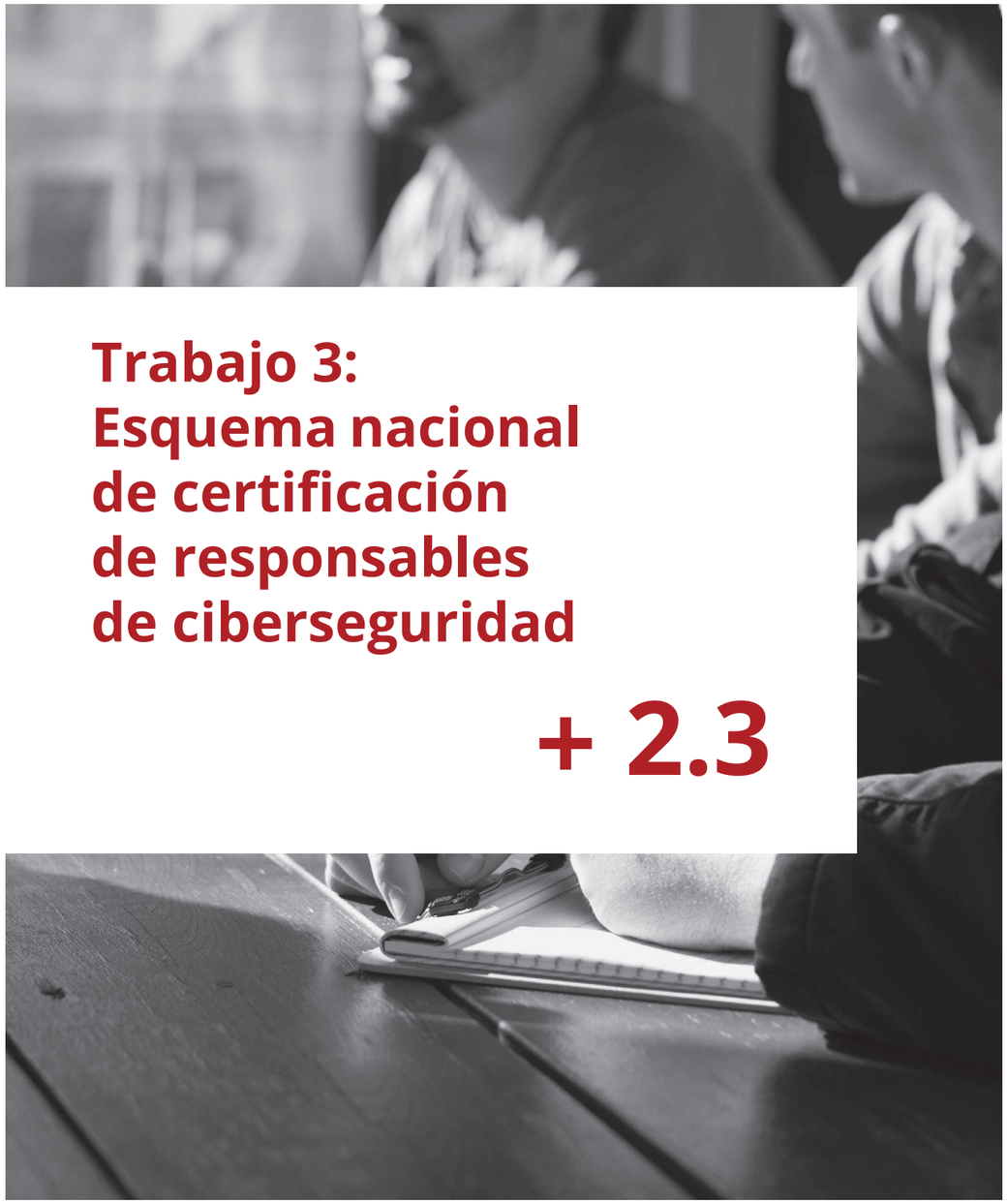
Para la fuerza laboral actual necesitamos un marco que defina y armonice roles a nivel europeo, catalogando las competencias y habilidades profesionales, que oriente a las empresas y trabajadores sobre el diseño de carreras profesionales, incentivos salariales y no salariales, etc. El proyecto SPARTA CSF es el candidato ideal que España puede empezar a aplicar sin dilación, y que debe apoyar a nivel europeo.

Desde los poderes públicos se debe respaldar otras posiciones organizativas y perfiles profesionales de la ciberseguridad, además del responsable de Seguridad de la Información, y no solo en el sector privado, sino también en la propia Administración Pública, mediante la creación de un Cuerpo Superior de Técnicos de Gestión de Riesgos de Ciberseguridad de la AGE.

Singularmente, las Fuerzas Armadas (FAS) y las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE), son organizaciones donde las peculiares técnicas de gestión del talento pueden ofrecer sus mejores resultados y, por tanto, donde más interesante puede ser su empleo para la mejor adaptación a los nuevos retos en la defensa nacional.

Con el fin de maximizar el retorno del esfuerzo inversor en I+D+i, tanto en el sector público como en el privado, que nos permita competir a escala global, España debe evitar la fragmentación y el aislamiento del talento, así como aligerar la rigidez y el coste de los procesos administrativos actuales.

Debemos promover la colaboración entre centros tecnológicos y de investigación, universidades, organismos públicos y empresas, con rotación del personal, comisiones de servicio, etc., además de revisar el marco regulatorio del emprendimiento para incentivar a aquellas ideas y personas con talento, surjan o no dentro de las organizaciones públicas o privadas que las gestionan.



Trabajo 3: Esquema nacional de certificación de responsables de ciberseguridad

+ 2.3

Trabajo 3: Esquema nacional de certificación de responsables de ciberseguridad

Elaborado por el Grupo de Trabajo 3 de formación, capacitación y talento

2.3.1. ¿Qué es el Esquema Nacional de Certificación de Responsables de Ciberseguridad?

El **Esquema Nacional de Certificación de Responsables de Ciberseguridad (RCSEG)**, fija las condiciones y requisitos para la certificación de los profesionales de la ciberseguridad. Engloba cuatro figuras recogidas en sendas normativas: responsable de la Seguridad del Esquema Nacional de Seguridad[1], responsable de Seguridad y Enlace de las infraestructuras críticas[2], responsable de la seguridad de la información[3] y responsables de Seguridad[3] de servicios o productos TIC de empresas proveedoras de infraestructuras críticas o de servicios esenciales[4].

2.3.2. ¿Quiénes son los agentes del Esquema?

El Centro Nacional de Inteligencia, a través del Centro Criptológico Nacional; la Secretaría de Estado de Digitalización e Inteligencia Artificial, a través de la Secretaría General de Administración Digital; y la Secretaría de Estado de Seguridad, a través de la Oficina de Coordinación de Ciberseguridad, son copropietarios del Esquema y responsables de su promoción y desarrollo. Podrán autorizar a otros agentes a formar parte del mismo: Entidad Nacional de Acreditación y Entidades de Certificación.

[1] RD 3/2010, de 8 de enero

[2] Ley 8/2011, de 28 de abril

[3] Real Decreto 43/2021, de 26 de enero

[4] Ley 40/2015, de 1 de octubre

2.3.3. ¿Quiénes pueden ser Entidades de Certificación, EC?

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.

Para utilizar la marca de certificación deberán contar con la aprobación del Comité de Gestión del Esquema y demostrar disponer de un mínimo de diez personas evaluadas.

Se generará un Registro de Entidades de Certificación ya acreditadas y un Registro de Personas Certificadas.

2.3.4. ¿Qué es la marca de certificación?

Al objeto de que el mercado sea capaz de identificar la condición de Entidad de Certificación y profesional certificado se crea la Marca del Esquema. Este símbolo podrá usarse por sí sola o asociada a una marca propia.

En el Reglamento del Esquema Nacional de Certificación desarrollado se especifica concretamente las normas de uso de la marca y su modelo de contrato.

2.3.5. ¿Quién puede certificarse como Responsable de Ciberseguridad, RCSEG?

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 Esquema Nacional de Seguridad, la Directiva NIS y su transposición al ordenamiento jurídico español, la Ley de Protección de Infraestructuras Críticas, incluyendo las normativas derivadas o de desarrollo de dichas regulaciones, así como aquella normativa que resulte de aplicación.

Las competencias genéricas del RCSEG se pueden concretar en las siguientes capacidades, clasificadas por áreas:

2.3.6. ¿Cómo se puede acceder a la Certificación de RCSEG?

Se establecen dos modos de acceso a la certificación:

Modo 1: certificación dirigida a profesionales con **más de 15 años** de experiencia continuada en las áreas competenciales cubiertas por el Esquema. Se requerirá para el acceso a la evaluación tener Titulación de nivel 1 o superior dentro del Marco Español de Cualificaciones para la Educación Superior (MECES).

Modo 2: certificación dirigida al **resto de profesionales**. Se requerirá Titulación universitaria equivalente o superior a grado universitario (en áreas TIC).

Adicionalmente, se requerirá un requisito que combine los años de experiencia profesional (de dos a cinco años) con formación mínima (de 150 a 600 horas).

El Reglamento del Esquema Nacional de Certificación de RCSEG desarrolla cómo se concretará la experiencia profesional a que se refieren los citados.

2.3.7. ¿Cuál es el procedimiento de evaluación?

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.

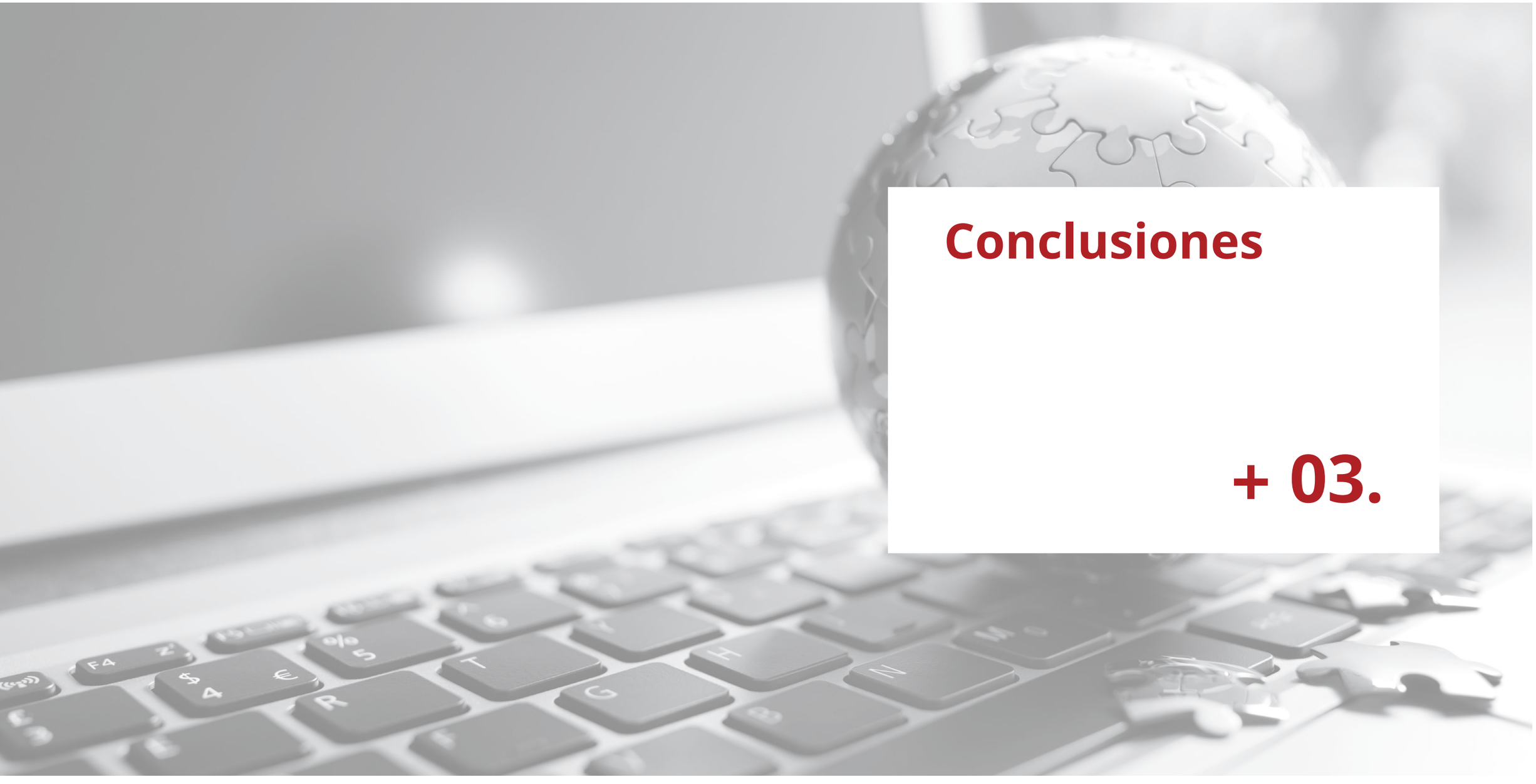
2.3.8. ¿Existe un reglamento que regule el funcionamiento de este Esquema?

Sí. Se ha desarrollado el **Reglamento de Esquema Nacional de Certificación de RCSEG** 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.

En él se recogen los requisitos que deberán acreditar los profesionales candidatos a los procesos de certificación (formación y experiencia profesional), el temario detallado para los Dominios del Esquema de Certificación de RCSEG y las reglas de uso de la Marca del Esquema.

Del mismo modo, se señala el procedimiento de selección y designación de los evaluadores de los candidatos a recibir el certificado; el modelo de informe de los resultados de las pruebas teóricas de los solicitantes y un modelo de documento justificativo de la certificación.

Por último, el Reglamento recoge tres anexos con el Código ético para las Entidades de Certificación y otro para los responsables de Ciberseguridad, así como las principales competencias y habilidades requeridas al RCSEG en vigilancia de las tendencias tecnológicas, desarrollo de la estrategia de seguridad de la información, la gestión de riesgos y gestión de la seguridad de la información y la gobernanza de los sistemas y servicios de información.



Conclusiones

+ 03.

Conclusiones

Transcurrido poco más de un año desde su constitución, el Foro Nacional de Ciberseguridad se ha convertido en un caso de éxito, reconocido tanto a nivel nacional e internacional, y considerándose una buena práctica extrapolable a otros ámbitos de la seguridad nacional y a otros países.

Tantas veces citada, pero pocas veces conseguida, la colaboración público-privada ha visto en el Foro Nacional de Ciberseguridad un claro ejemplo de materialización con la finalización de los primeros trabajos encomendados por el Consejo Nacional de Ciberseguridad, demostrando de qué manera es posible aprovechar las sinergias existentes entre lo privado y lo público en un ámbito tan transversal como la ciberseguridad. Todos sus componentes y expertos, profesionales de reconocido prestigio en sus respectivas áreas, con el conocimiento y la experiencia puestos en común, han elaborado los tres primeros trabajos del Foro.

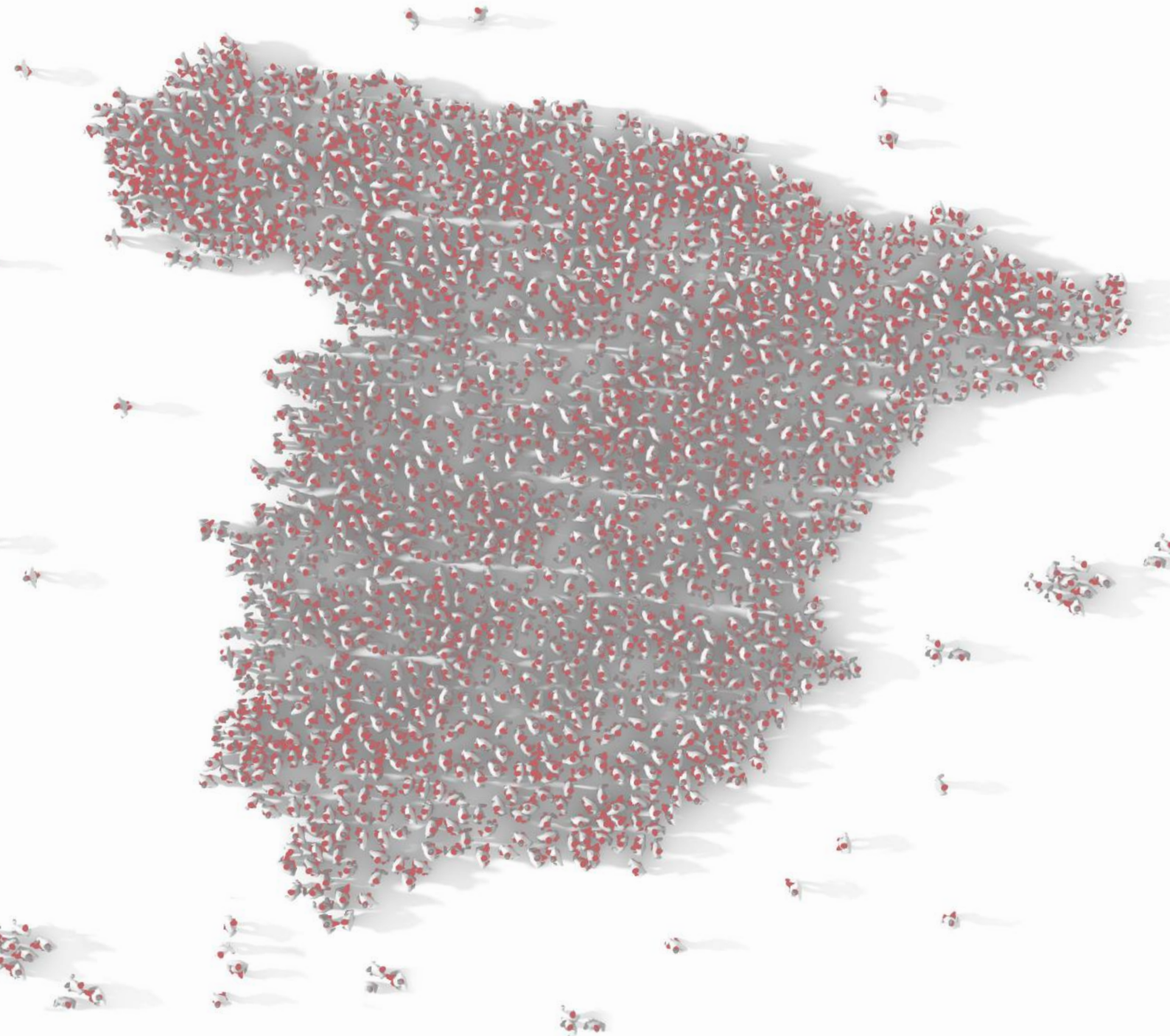
La fortaleza del Foro Nacional de Ciberseguridad recae en su composición y su grado de representatividad, de tal manera que, a través de sus miembros, se ha conseguido identificar a los mejores expertos (127) para participar en los diferentes Grupos y Subgrupos de Trabajo.

Por último, señalar que estos trabajos son un primer paso para seguir avanzando en el fortalecimiento de la colaboración público-privada; y, en ellos, se han identificado nuevos proyectos y actuaciones a abordar en un futuro. Será el propio Foro Nacional de Ciberseguridad y, en última instancia, el Consejo Nacional de Ciberseguridad, quienes aprueben los proyectos realizados y establezcan y prioricen las nuevas actividades a afrontar en un futuro próximo, siempre en línea con la ENCS.

Estos trabajos son un primer paso para seguir avanzando en el fortalecimiento de la colaboración público-privada

+++

FORO NACIONAL DE CIBERSEGURIDAD



FORO NACIONAL DE CIBERSEGURIDAD