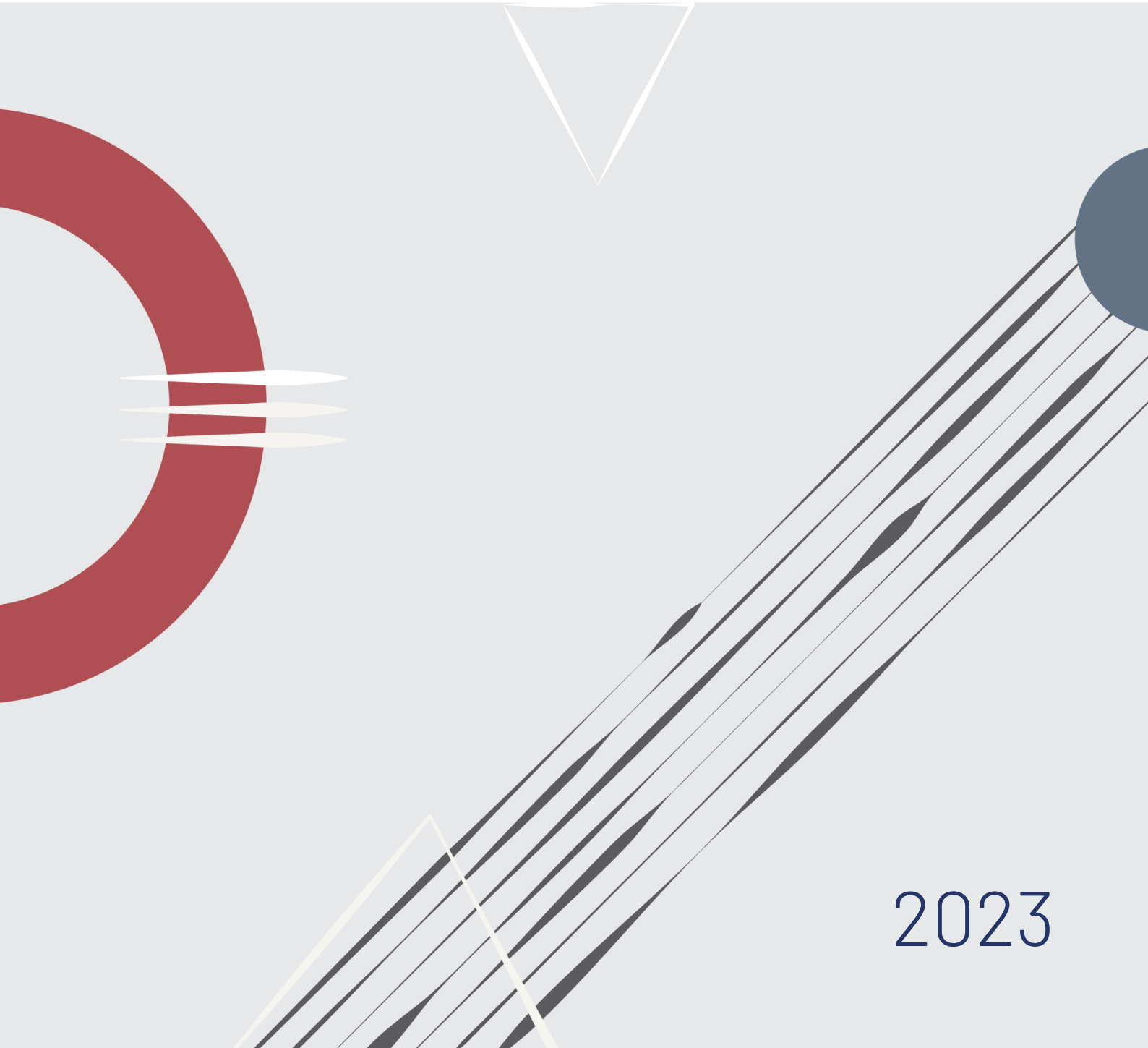
FORO NACIONAL DE CIBERSEGURIDAD

IMPULSO A LA INDUSTRIA Y A LA I+D+i. RESUMEN DE PROPUESTAS Y TRABAJOS DE LA FASE 2

OBJETIVOS Y ALCANCE



2023

Catálogo de publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES Y MEMORIA DEMOCRÁTICA

NIPO (edición online): 089-23-017-0
Fecha de edición: junio 2023

Autores

Coordinador sociedad civil:

Luis Álvarez Satorre (Cámara de Comercio de España)

Coordinadora institucional:

Lola Rebollo Revesado (INCIBE)

Autores y colaboradores:

Cristina Alcaraz Tello

Luis Fernando Álvarez-Gascón Pérez

Félix Arteaga Martín

Ana Ayerbe Fernández-Cuesta

Maite Boyero Egido

Juan Miguel Cuéllar del Río

Juan Díez González

Albert Estrada i Capilla

Juan González Martínez

Javier Jarauta Sánchez

Javier López Muñoz

Gregorio Martínez Pérez

César Maurín Castro

José Miguel Rosell Tejada

Francisco Sampalo Lainz

Salvador Trujillo González

Urko Zurutuza Ortega

ÍNDICE

1. INTRODUCCIÓN

El Foro Nacional de Ciberseguridad, como órgano de asistencia al Consejo Nacional de Ciberseguridad Nacional tiene la misión de articular y cohesionar un entorno de colaboración público-privada que, a través de diferentes líneas de acción, genere el máximo conocimiento sobre los desafíos a la Seguridad Nacional en el ciberespacio, ya sean oportunidades o amenazas, y siempre en colaboración con el Consejo Nacional de Ciberseguridad. El establecimiento de sinergias público-privadas permiten establecer un dialogo activo y ejecutable de acciones que permitan avanzar en la protección de la sociedad, y es clave en este marco poder articular acciones concretas para el fortalecimiento de la industria española y el crecimiento del ecosistema nacional de investigación.

El grupo de trabajo 2 (GT2), encargado de impulsar la industria e I+D+i nacionales, presentó sus primeros trabajos y conclusiones el pasado mes de marzo 2021 y decidió la continuidad de estos trabajos en las siguientes áreas:

- Definir una taxonomía nacional alineada con ECSO, JRC y posteriormente la del CCN, INCIBE y otras (SGT2).

- Continuar con los trabajos del barómetro incorporando a este grupo de trabajo a ObservaCiber, englobado dentro del Observatorio Nacional de Tecnología y Sociedad (ONTSI) (SGT2).

- Evaluar las acciones puestas en marcha por Gobierno de España para aumentar la digitalización y la protección frente a ciberataques de las PYMES españolas (SGT3).

- Comenzar la definición de una Agenda de Investigación e Innovación (A2I) de Ciberseguridad como elemento de aumento de competitividad para el ecosistema nacional.

- Trasladar los trabajos y conclusiones obtenidos de la primera fase en cuanto a la necesidad de talento identificado por la industria de ciberseguridad (SGT6) al Grupo de Trabajo 3 (GT3 – Formación, Capacitación y Talento) liderado por el CCN y la CRUE-Universidades.

- Trabajar en acciones de promoción exterior de la industria española de ciberseguridad (SGT1 y SGT8).

Los trabajos presentados en este informe se han realizado durante el 2022 en reuniones bimensuales entre todos los subgrupos de trabajo y reflejan la imperante necesidad de continuar con las actividades del GT2, más allá de las conclusiones y resultados presentados en este documento, lo que permitirá alcanzar el objetivo de impulsar y mejorar las capacidades de la industria y de la investigación nacional que convertirán a España en un país líder en el ámbito de la ciberseguridad.

2. CONTEXTO

La **ciberseguridad** es hoy uno de los **retos más importantes** a los que se enfrentan gobiernos, empresas y ciudadanos. En un contexto global, interconectado y dependiente de la tecnología como es el actual, **la ciberseguridad resulta imprescindible para alcanzar la necesaria confianza en el ámbito digital ligada a la imparable transformación digital de la sociedad y su tejido productivo**.

La importancia que adquiere en la actualidad el **diseño de políticas públicas para impulsar la ciberseguridad** es creciente. Un fenómeno que está alineado con la prioridad estratégica de la Unión Europea en digitalizar la economía, pues ello comportará una mayor autonomía estratégica de su industria y sectores críticos. Ya en la Comunicación oficial de la Comisión Europea "Configurar el futuro digital de Europa" (2020) [1] se prefiguraban iniciativas para promover las soluciones tecnológicas que permitirán a la UE liderar la transformación digital.

Por su parte, la **Estrategia Europea de Datos** [2], de febrero de 2020, establece cuatro pilares como requisitos previos esenciales para una sociedad empoderada por el uso de los datos, la **protección de datos**, los **derechos fundamentales**, la **seguridad** y la **ciberseguridad**.

En este marco de actuación, se lanzaba el nuevo **Programa Europa Digital** (2021-2027) [3] con una inversión total de 8.200 M€, de los cuales, 1.900 M€ se destinan al despliegue de capacidades para la ciberseguridad para administraciones públicas, empresas e individuos. Y, de forma complementaria, el **Plan de Recuperación Europeo** (*EU Recovery Plan*) [5] apuesta por una presencia tecnológica más fuerte en ámbitos como la IA, la infraestructura de datos, las redes 5G y 6G, el *blockchain* y la ciberseguridad y ciber-resiliencia.

En este contexto, la reciente Estrategia Europea de Ciberseguridad [5], presentada el 16 de diciembre de 2020 por la Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, busca **impulsar la resiliencia colectiva en Europa contra las amenazas cibernéticas y ayudar a garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios fiables** (4.500 millones de euros de inversión combinada entre la UE, los Estados miembros y la industria). Así, el objetivo 3 de la Estrategia pretende reforzar las capacidades industriales y tecnológicas de la UE en materia de ciberseguridad, incluso mediante proyectos financiados conjuntamente por los presupuestos nacionales y de la UE. Esta estrategia es un componente clave de otros planes y estrategias como el *Shaping Europe's Digital Future*, la *New Industrial Strategy*, el *EU Recovery Plan* y la *EU Security Union Strategy* 2020-2025.

A nivel nacional existe un **alineamiento con la política industrial y digital europea** y, en concreto, con la Estrategia Europea de Ciberseguridad, a través de:

- La **Estrategia Nacional de Ciberseguridad** [6], dentro de su *Objetivo IV: Cultura y compromiso con la Ciberseguridad y potenciación de las capacidades humanas y tecnológicas*, desarrolla a través de una serie de medidas que incluyen "impulsar programas de apoyo de I+D+I en seguridad digital y ciberseguridad en empresas, universidades y centros de investigación".

- La **Agenda España Digital 2026** [7], que tiene como cuarta medida de acción: *"Reforzar la capacidad española en ciberseguridad, consolidando su posición como uno de los polos europeos de capacidad empresarial".* Además, como ejes de la Agenda, se presentaron en diciembre de 2020, el Plan para la Conectividad y las Infraestructuras Digitales y la Estrategia de Impulso a la Tecnología 5G, dotados con 4.320 millones de euros hasta 2025.

- El **Plan de Recuperación, Transformación y Resiliencia de España** [8] en el contexto global del plan europeo "*Next Generation EU*", constituye el *marco global estratégico del país al incorporar una importante agenda de inversiones y reformas estructurales*, que se interrelacionan y retroalimentan para lograr objetivos transversales tales como la transformación digital de la sociedad y su tejido productivo.

- Las Directrices Generales de la **Nueva Política Industrial 2030** [9], en concreto, en el eje 1. Digitalización, "*se hace hincapié en la promoción de la ciberseguridad como una de las acciones clave a llevar a cabo dentro de la actuación 1. Impulso a la transformación digital desde el Estado*".

- La **Estrategia Española de Ciencia, Tecnología e Innovación (2021-2027)** [10] incide en la *necesidad de impulsar instrumentos de apoyo público en I+D+I para promover la ciberseguridad en la industria y en tecnologías clave*, a través del Sector estratégico 4. Seguridad para la Sociedad (línea estratégica de ciberseguridad).

- Otras estrategias vinculadas: Estrategia de Seguridad Nacional (2021) [11] y **Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave (2019-2023)** [12].

Como **instrumento para impulsar la colaboración público-privado** en esta materia se creó, en julio de 2020 en España, el **Foro Nacional de Ciberseguridad** [13], para dar respuesta al objetivo 3 de la Estrategia Nacional de Ciberseguridad *"Protección del ecosistema empresarial y social y de los ciudadanos",* a través de la línea de acción 4 *"Impulsar la ciberseguridad de ciudadanos y empresas".* Liderado por el Consejo de Seguridad Nacional y en asistencia al Consejo Nacional de Ciberseguridad, integra a representantes de la sociedad civil, expertos independientes, centros de investigación, empresas, asociaciones, etc., para debatir y generar conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

La ambición de alcanzar una **posición de liderazgo internacional en materia de ciberseguridad** será más viable si se orientan los esfuerzos de entidades públicas y

privadas con una perspectiva de especialización, seleccionando nichos con alto potencial de desarrollo y comercialización no cubiertos en la actualidad, que además de contar con las capacidades actuales del sector, respondan a retos de la industria nacional y dispongan de alta capacidad de escalado e internacionalización.

3. BARÓMETRO Y TAXONOMÍA

Durante la primera fase de los trabajos del FNCS, en el Subgrupo de Trabajo 2, se identificaron como críticas tres acciones para el sector español de la ciberseguridad:

- **Identificar la cadena de valor** completa que incluya oferta y demanda, e identifique y cualifique los actores de dicha cadena.
- **Definir, diseñar e implantar un barómetro** que mida los principales indicadores del ecosistema de ciberseguridad español.
- **Acordar una taxonomía común entre la industria y la investigación** que establezca los productos y servicios de ciberseguridad a desarrollar e implantar.

Estas tres acciones, disminuirán el gap identificado en el ecosistema de ciberseguridad español y europeo entre la industria y la investigación.

Adicionalmente, consideramos que 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.

En esta segunda fase de los trabajos se propone mantener y profundizar en el desarrollo e implantación de las tres acciones críticas identificadas, pero cambiando el orden de estas: taxonomía, cadena de valor y barómetro.

Así pues, se propone priorizar la taxonomía de las competencias de ciberseguridad, es decir, definiendo inicialmente el "qué" debemos hacer, para continuar con la cadena de valor que identifique el "quién" con los actores principales en el ecosistema, y terminar con el "cómo y cúanto" que se concretarán en el barómetro integral de la ciberseguridad.

Igualmente, esta nueva priorización ayudará a la interacción necesaria con otros grupos de trabajo que necesitan para su labor, disponer lo antes posible de una taxonomía común.

Por último, la aparición en los últimos meses del Observatorio de la Ciberseguridad (Observaciber) nos hace concluir que han de estar alineados los trabajos de este grupo de

trabajo sobre el barómetro, con los que se están realizando en Observaciber y, por tanto, agendar los trabajos de dicho barómetro, para la segunda parte del año 2023.

3.1. Situación actual de los modelos de taxonomía

En los trabajos de Foro en su fase inicial, se identificaron dos propuestas de taxonomías de referencia europeas publicadas por ECSO orientadas, hacia la industria, y por JRC orientada a la investigación y se elaboró una propuesta inicial de taxonomía híbrida, que permite relacionar ambas y cuya estructura será objeto de revisión y detalle en esta segunda fase.

Por otra parte, existen varios trabajos en diferentes organizaciones y proyectos europeos orientados a la revisión y actualización de las taxonomías existentes, que es necesario seguir y alinear con los trabajos en nuestro país.

De hecho, la importante representación española actualmente en organismos como ECSO, ENISA y otros, así como el gran impulso a la industria e investigación nacional promovido durante los últimos meses por el DSN, CCN e INCIBE, hace que consideremos que nuestro país se encuentra en condiciones idóneas para promover y liderar un modelo de taxonomía integrada de ciberseguridad.

3.2 Otras taxonomías para incluir en el modelo integrado

Durante el año 2022, se han venido desarrollando importantes iniciativas y proyectos por parte de las administraciones públicas, entre los que se pueden destacar los siguientes:

- En febrero, el Gobierno aprueba la creación del SOC-AGE [14].
- En marzo, el CCN actualiza Taxonomía de productos STIC-140 [15].
- En mayo, se publica el RD 311/2022 sobre el nuevo ENS [16].
- En octubre INCIBE publica la primera Compra Publica Precontractual (CPP1) [17].
- En octubre INCIBE publica la segunda Compra Publica Precontractual (CPP2) [18].
- En noviembre CCN anuncia un “Ciberescudo Único” y actualiza CPSTIC-105 [19].

Todas ellas, de un modo u otro, implican una actualización de los productos y servicios que se ofrecen y se demandan en nuestro sector, tanto por parte de organismos públicos como por parte de la industria y la investigación.

Estas iniciativas hacen que, durante el presente año, el sector de la ciberseguridad haya sido uno de los más dinámicos y con mayor impulso entre todos los sectores tecnológicos de la sociedad.

Al mismo tiempo, hacen que sea conveniente generar un modelo integrado de todas las taxonomías del sector, por lo que proponemos la creación y actualización constante de un **Modelo Integrado de una Taxonomía Española en Ciberseguridad** (en adelante **MITEC**) incluyendo los productos y servicios de ciberseguridad.

3.2.1. Taxonomía CCN-STIC-140. Productos de seguridad TIC

El CCN dispone de un modelo de taxonomía de referencia para productos de seguridad TIC, plasmado en el catálogo CCN-SITC-140 y cuya última actualización es de marzo del presente año.

El modelo está estructurado en tres grupos:

1. Productos cualificados para información sensible, según el ENS:
   - Formado por 9 categorías y 49 familias de productos
2. Productos aprobados para información clasificada:
   - Formado por 1 categoría y 3 familias de productos.
3. Productos y servicios de conformidad y gobernanza:
   - Formado por 6 familias de productos y servicios.

Dicha taxonomía de referencia se plasma en el catálogo de productos CCN-STIC-105 que según el nuevo ENS 2022 es necesario utilizar para la implantación del nivel ENS requerido.

Todo ello, hace necesario incorporar e integrar esta taxonomía en el Modelo Integrado de Taxonomía que se defina en los trabajos de este subgrupo.

3.2.2. Retos de la Compra Pública Innovadora de INCIBE

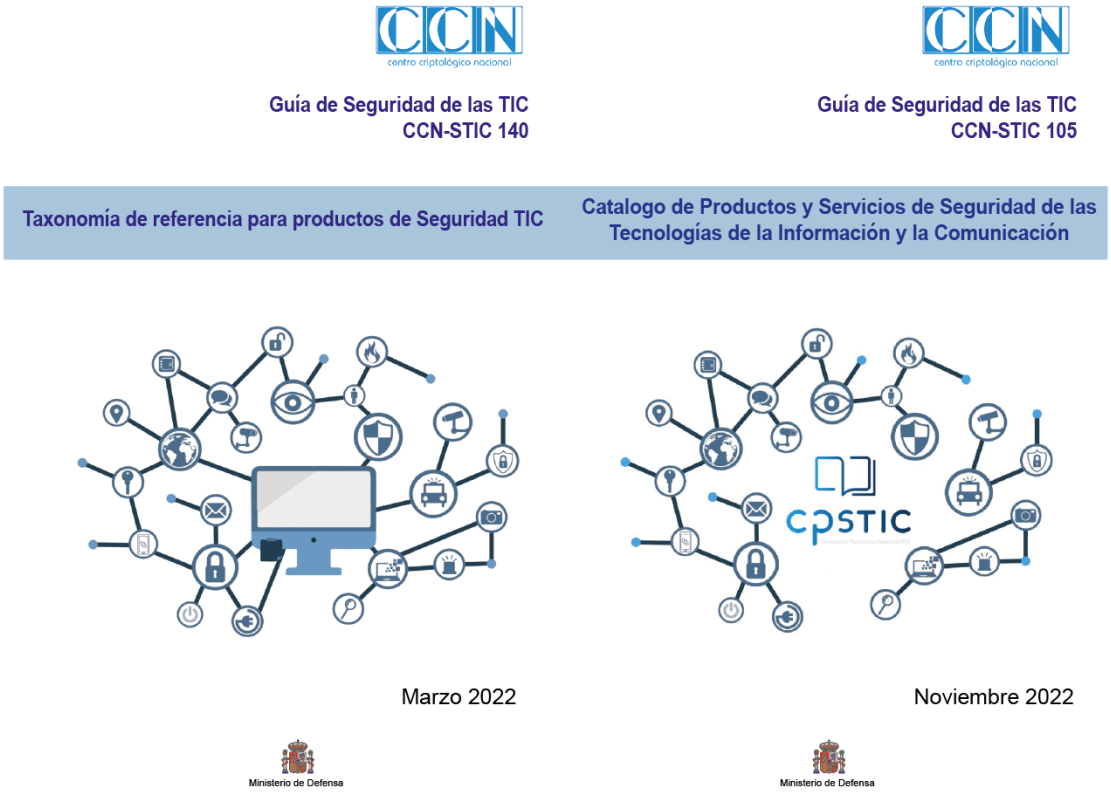
En julio de 2021, INCIBE puso en marcha una iniciativa estructurada en varias fases, que comenzó por un proceso de Consulta Preliminar al Mercado, que permitió definir un Mapa de Demanda Temprana, y seguidamente las dos iniciativas de Compra Pública Precomercial (CPP1 y CPP2) del presente año, que han supuesto un importante impulso al ecosistema de la ciberseguridad.

Desde la primera fase de dicha iniciativa, todo el sector de la ciberseguridad español, incluyendo industria e investigación, proporcionó la información necesaria para que INCIBE pudiera identificar, de forma realista y actualizada, los principales productos y servicios que se ofrecen y se requieren hoy en día en el ecosistema de ciberseguridad español.

La consecuencia práctica de dicha iniciativa, son las dos convocatorias para programas de I+D lanzados al mercado como Compra Pública Precomercial que se detallan seguidamente.

- Compra Pública Precomercial 1, donde se establecen 7 retos y necesidades públicas.
- Compra Pública Precomercial 2, donde se establecen 30 retos, incluyendo productos y centros de operaciones de ciberseguridad sectoriales.

Por tanto, el objetivo del Modelo Integrado de Taxonomía será incluir tanto los 7 retos de la primera convocatoria, como los 30 retos de la segunda, estableciendo una congruencia entre la taxonomía que se defina, con los retos que empezarán a funcionar durante 2023.

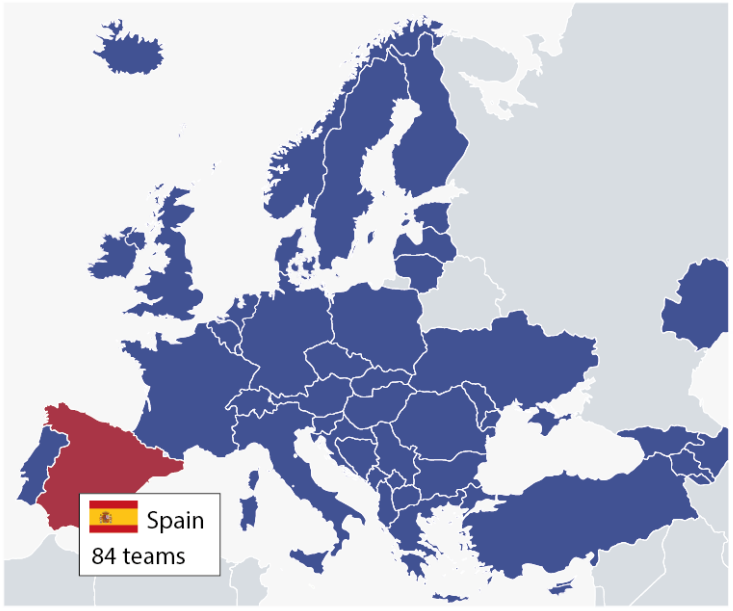


3.2.3. Servicios SOC para las Administraciones Públicas

España es el país que dispone del mayor número de CSIRT actualmente en el catálogo establecido por ENISA, contando con 84 CSIRTs públicos y privados. Esto nos posiciona igualmente como uno de los países europeos con mayor cantidad y calidad de servicios SOC.

El Gobierno español, con su iniciativa a comienzos de 2022 de crear un servicio SOC integrado para las organizaciones de la Administración General del Estado (SOC-AGE), se posiciona como pionero a nivel europeo en este tipo de iniciativas. De hecho, la Comisión Europea, dentro de su iniciativa DEP – *Digital Europe Program*, acaba de solicitar propuestas para un proyecto similar de SOCs europeos para 2023.

Como parte de esta iniciativa, en el SOC-AGE se ha definido un catálogo de más de **20 servicios** que actualmente es confidencial, pero que respetando dicha confidencialidad, en los trabajos del FNCS se verificará que los mismos estén incluidos en el modelo de taxonomía que se defina.



GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

OBSAE Observatorio de Administración Electrónica

Relaciones entidades
Coordinación incidentes

CCN centro criptológico nacional

SGAD

Implantación
Operación
Detección de incidentes

Coordinación
Seguimiento servicio

Entidades AGE

SOC (Servicio de Operaciones de Ciberseguridad

Infraestructura ciberseguridad

Inteligencia ciberseguridad

3.3. Planificación de las acciones

Hasta el momento, los trabajos de este subgrupo han estado orientados a la identificación y actualización de las diferentes fuentes de productos y servicios de ciberseguridad en los que se está trabajando en España y Europa, para posteriormente comenzar los trabajos de la definición del Modelo Integrado de Taxonomía, que se realizará durante el primer trimestre de 2023, con el objetivo de lanzar un piloto en el primer semestre del próximo año.

Posteriormente, se continuará con los trabajos de cadena de valor y de barómetro para completar los mismos en la segunda parte del año próximo, según la siguiente planificación:

DESCRIPCIÓN	Q1-23	Q2-23	Q3-23	Q4-23
1.0 Taxonomía Común de Ciberseguridad para la Industria & I+D+i				
1.1 Identificar estado actual en España y EU				
1.2 Propuesta de Taxonomía Común				
1.3 Prueba de concepto en algún Caso de Uso				
2.0 Cadena de valor de la Ciberseguridad				
3.1 Clasificación e identificación de actores				
3.2 Metodología para la identificación de actores y BBDD				
3.3 Presentación en Plataforma				
3.0 Barómetro Integral de la Ciberseguridad				
1.1 Identificar estado actual en EU				
1.2 Definición de los KPI principales y metodología de obtención				
1.3 Presentación en ObservaCiber				
1.4 Metodología de seguimiento y comunicación				

4. RETOS DE CIBERSEGURIDAD EN LAS PYMES

Ante los desafíos planteados por la pandemia de la COVID-19 y la necesidad de construir la Europa de la nueva generación, se ha puesto en marcha el programa ***Kit Digital***, financiado por los fondos Next Generation de la Unión Europea, que se materializa a través del Mecanismo de Recuperación y Resiliencia (MRR) y React-UE. El programa *Kit Digital*, se encuadra bajo el Componente 13 Inversión 3, dedicado al impulso a las PYME, asimismo, contribuye a actuaciones del Componente 15 y Componente 19.

En un país dónde su tejido empresarial está formado por pymes en un 99,83%, y la mayoría son micropymes, bien sin asalariados, bien de hasta 9 empleados, **la digitalización acelerada está suponiendo un gran reto puesto que este tipo de empresas no tiene realmente concienciación ni preparación en ciberseguridad** y, además, su nivel de madurez digital en esta materia es bajo, por lo que se considera imprescindible y prioritario trabajar a corto plazo en las siguientes actividades: sensibilización, competencias en ciberseguridad y dotación de herramientas específicas.

Para la definición y ejecución de las actividades propuestas a continuación se considera necesaria la estrecha colaboración del INCIBE con la Cámara de España.

Por otro lado, con el fin de maximizar la llegada a las empresas de las medidas propuestas, se considera la **participación activa** de la Red de cámaras de comercio, dada su capilaridad y cercanía a las pymes. Asimismo, la coordinación de la Cámara de España asegura un tratamiento uniforme en el conjunto del territorio nacional y garantiza la prestación de servicios homogéneos a las empresas.

Asimismo, para la ejecución de las medidas se pone a disposición la **red de Oficinas Acelera Pyme de las Cámaras de comercio**, creadas en colaboración con la entidad pública empresarial Red.es, para el impulso de la transformación digital de las pequeñas y medianas empresas, autónomos y emprendedores, conforme a lo establecido en el Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19, en el que se identifica como prioridad inmediata preparar y dotar de los recursos necesarios a las pymes para su desarrollo digital, así como **mejorar los servicios de asesoramiento personalizado a las PYMES y acompañamiento en su esfuerzo de digitalización**, señalando además la necesaria colaboración de las cámaras de comercio en el apoyo a la transformación digital de las pymes, a través del Plan Acelera PYME de Red.es.

Para todas las actividades que se indican a continuación se tendrá en cuenta:

- La información generada en el **Programa de Ciberseguridad de la Cámara de España** durante sus ejecuciones de 2020, 2021 y 2022.

- Asimismo, se realizará una categorización más detallada, a partir de 2023, de los asesoramientos que se realizan en las **Oficinas Acelera Pyme**, y que estén relacionados con la ciberseguridad.

- El nivel de contratación de soluciones de ciberseguridad en el ámbito del **Programa Kit Digital**, en el que la Cámara de España actúa como entidad colaboradora de Red.es.

Se adjunta en el Anexo 1 la actualización a diciembre de 2022, de los principales indicadores de los tres programas mencionados.

Por tanto, se explotará esta información para determinar los potenciales sectores prioritarios, las temáticas más urgentes, y las mayores necesidades de las pymes en materia de ciberseguridad (ya sea de concienciación o de herramientas o soluciones a implantar).

4.1. Sensibilización en ciberseguridad

Se propone la definición y realización de un ciclo de jornadas de sensibilización en las sedes de las cámaras de comercio y de las Oficinas Acelera Pyme. Para ello, se realizarán las siguientes tareas:

- Definición de temáticas.

- Identificación de cámaras y oficinas Acelera Pyme y establecimiento del calendario.

- Ejecución del ciclo de jornadas.

Asimismo, se propone la realización de una campaña de comunicación a nivel nacional. Para ello se definirá previamente un plan de comunicación adecuado.

4.2. Definición de una matriz de categorización de pymes

Con el fin de poder adaptar y personalizar las actuaciones, contenidos y herramientas de ciberseguridad a las características y circunstancias concretas de las pymes, se considera necesaria la definición de una matriz que permita su categorización. Para ello, con el apoyo del Servicio de Estudios de las Cámara de España:

- Se realizará una encuesta de ciberseguridad a pymes, a través del Observatorio de Competitividad.

- Se definirán los criterios de categorización de las pymes.

- Se identificarán y seleccionarán las fuentes de información adecuadas.

4.3. Competencias en ciberseguridad

4.3.1. Formación y capacitación a asesores

Se considera necesario disponer de personal cualificado que pueda asesorar y sensibilizar adecuadamente a las pymes, en una red que tenga la capilaridad suficiente para llegar a ellas. Por tanto, se propone realizar un programa de formación por parte del INCIBE a técnicos de cámaras de comercio localizada en la red de Oficinas Acelera Pyme, de manera que puedan prestar correctamente los servicios en materia de atención personalizada y de sensibilización a empresas.

4.3.2. Diagnóstico y asesoramiento personalizado

La Cámara de España, ejecuta, a través de la Red de cámaras de comercio, un programa de ayudas, que capacita a las pymes a prevenir los principales riesgos en ciberseguridad, asumibles por ellas mismas, para garantizar que los sistemas de información y telecomunicaciones que utilizan poseen un adecuado nivel de ciberseguridad.

La primera fase del programa para la pyme consiste en un análisis exhaustivo de sus sistemas de información y telecomunicaciones para identificar los principales riesgos referidos a la ciberseguridad.

Este diagnóstico continuará con su ejecución en 2023, a través de las cámaras de comercio, si bien se actualizará en función de la explotación de los datos de ejecución del propio programa y de la definición de la matriz de categorización de pymes.

Asimismo, se puede prestar asesoramiento personalizado y acompañamiento a pymes en materia de ciberseguridad, a través de la Red de Oficinas Acelera Pyme de las cámaras de comercio, establecidas en colaboración con Red.es.

4.3.3. Ayudas para la implantación de soluciones

En la segunda fase del programa mencionado en el apartado anterior, la empresa recibe una subvención para la implantación de herramientas de ciberseguridad. Se realiza un seguimiento del ritmo de ejecución y de la adecuación de los proyectos de implantación.

Las soluciones por implantar se corresponden con las recomendadas en la fase I, de asesoramiento. Por tanto, parte de los trabajos a corto-medio plazo sería revisar y actualizar, en su caso, el catálogo de soluciones subvencionables del programa. En cualquier caso, este no detendrá su ejecución.

4.3.4. Creación e implantación del sello de procesos de ciberseguridad INCIBE – CCE en empresas y entidades

INCIBE y la Cámara de España, a través de la Red de Cámaras, podrían convertirse en referencia y emisoras del "Sello de Confianza de Ciberseguridad" INCIBE - CCE, actuando como prescriptora y emisora de una homologación (sello o certificado) referido a temas de ciberseguridad. Esto es, actuar como institución que delimitara los términos y condiciones que una empresa española debería disponer para cumplir con unos determinados estándares en materia de ciberseguridad.

Las cámaras se encargarían de informar a las empresas sobre los requisitos precisos, así como de comprobar el cumplimiento de éstos.

Las tareas relativas a esta actividad serían:

- Definición de requisitos.
- Elaboración de un estándar.
- Formación y capacitación a cámaras.
- Despliegue del "Sello de Confianza de Ciberseguridad" INCIBE – CCE.

4.4. Cronograma de próximos pasos

DESCRIPCIÓN	Q1-23	Q2-23	Q3-23	Q4-23
1 Sensibilización en Ciberseguridad				
1.1 Jornadas de sensibilización y talleres de capacitación				
1.2 Campaña de Comunicación Nacional				
2 Definición matriz de categorización de pyme				
2.1 Observatorio Competitividad CCE-Encuesta Ciberseguridad a Pymes				
2.2 Selección y definición de criterios de categorización				
2.3 Identificación y selección de fuentes de información				
3 Competencias en Ciberseguridad				
3.1 Formación y capacitación a asesores				
3.2 Diagnóstico y asesoramiento pesonalizado				
3.3 Ayudas para implantación de soluciones				
3.4 Sello Ciberseguridad INCIBE - CCE				

5. AGENDA DE INVESTIGACIÓN E INNOVACIÓN EN CIBERSEGURIDAD (A2I)

En la documentación generada y publicada en 2021 [20] por el Grupo de Trabajo 2, "Impulso a la industria y a la I+D+i" se recomienda la definición de una **agenda de investigación e innovación** a nivel nacional, de forma que se prioricen los ámbitos de I+D+i en los que se debe apostar a nivel regional y nacional y en donde deben centrarse los esfuerzos investigadores de innovación y de financiación.

Para la elaboración de dicha agenda, 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 agenda de investigación e innovación (en adelante A2I). Es destacable el esfuerzo llevado a cabo por la *European Cyber Security Organisation* (ECSO) [21] en su grupo de trabajo WG6 y también los trabajos de cuatro pilotos europeos: SPARTA, ECHO, CONCORDIA y CyberSec4Europe [22] a través de sus respectivas hojas de ruta.

Es en este contexto donde se plantea la definición de una A2I nacional, y cuyos objetivos, alcance y metodología se describen en el resto de este documento.

5.1. Objetivos de la A2I

El objetivo principal de la A2I es analizar las necesidades en materia de I+D+i en ciberseguridad, conocer las capacidades actuales del ecosistema español, y con todo ello identificar las oportunidades que se pueden presentar como país en esta materia a medio y largo plazo. De esta manera, se pretende contribuir de forma activa a la coordinación de las actividades españolas de investigación e innovación en el marco de la Estrategia de Ciberseguridad Nacional.

La elaboración de la A2I persigue los siguientes objetivos concretos:

- **Detección de las capacidades y fortalezas** del ecosistema nacional de I+D+i en ciberseguridad, identificando ámbitos o temáticas y su desarrollo (productos, servicios, patentes, publicaciones).

- **Detección de las prioridades y necesidades** de ciberseguridad por parte de los usuarios finales (Administraciones Públicas, Ministerio de Defensa, Fuerzas y Cuerpos de Seguridad del Estado, Ministerio del Interior, empresas, ciudadanos, etc.) y en especial por parte de la demanda sofisticada (sectores estratégicos, SOCs, etc.).

- **Identificación de la capacidad de adquisición de soluciones o volumen de mercado** por parte de las administraciones y otros usuarios finales.

- **Análisis de los condicionantes sociales, tecnológicos, económicos o políticos**.

- **Análisis de los instrumentos** dedicados de manera específica a la ciberseguridad, como convocatorias de apoyo a la I+D+i de, entre otros, los países identificados en la sección 4.3.3, así como un análisis comparativo entre países de los resultados derivados de dichos instrumentos.

- **Contrastes y correlaciones** entre necesidades, capacidades e instrumentos existentes a nivel nacional y su comparación con el resto de los países identificados.

- **Detección de los nichos y oportunidades** existentes en el panorama nacional e internacional de soluciones y productos de ciberseguridad y, por consiguiente, oportunidad para la Industria de ciberseguridad nacional en combinación con los demás actores del ecosistema de I+D+i.

- **Propuesta de las líneas estratégicas** de I+D+i en ciberseguridad con alto potencial en España.

- **Armonización de los programas de financiación** en España (nacionales, regionales y locales) de la I+D+i en ciberseguridad acorde a objetivos estratégicos.

- **Identificar e involucrar al ecosistema inversor** nacional público y privado.

5.2. Modelo de gobernanza

Para la elaboración de los resultados previstos, se propone la creación de un modelo de gobernanza basado en la colaboración público-privada abierto a la colaboración y participación de los agentes y actores relevantes, con espíritu de transparencia, neutralidad, consenso en sus decisiones y coordinado con otras iniciativas relacionadas.

El objetivo es que todos los posibles participantes, puedan primeramente aportar su visión, participar en revisiones y, finalmente, aportar su refrendo o conformidad con el texto generado.

Los trabajos para la elaboración de la A2I estarán liderados por INCIBE, como responsable último de su gestión y seguimiento, y contarán con la participación activa de un **grupo decisor** (conformado preliminarmente con los integrantes del subgrupo 5, del grupo de trabajo 2 "Impulso a la industria y a la I+D+i" del Foro Nacional de Ciberseguridad con la posibilidad de unirse miembros de otros subgrupos de dicho grupo), en el que participará un grupo de agentes reducido, pero representativo del sector para la toma

ágil de decisiones y revisión de la documentación y entregables, así como del trabajo final, actuando igualmente como tractores dentro de lo colectivos a los que representan.

5.3. Alcance

La A2I será un documento que identifique las principales líneas de investigación e innovación en ciberseguridad y que tendrá como público objetivo principal el sector de la ciberseguridad nacional, integrado fundamentalmente tanto por la industria de ciberseguridad, los organismos de investigación, así como agentes normalizadores y reguladores y las autoridades competentes en esta materia. También es de interés para aquellas entidades con alta demanda de soluciones en ciberseguridad, en especial los SOCs y CSIRTS públicos y privados, Fuerzas y Cuerpos de Seguridad del Estado, así como operadores estratégicos de sectores críticos. Por último, es también de alto interés, tanto para inversores privados especializados en ciberseguridad como para las Administraciones públicas (locales, regionales, o nacionales) con programas de financiación a la I+D+i.

5.3.1. Partes interesadas

Las partes interesadas serán las entidades que, a través de sus representantes designados, participen en la elaboración y validación de la A2I para lo cual podrán proporcionar su aportación y opinión, y participar en la discusión y debates con el objetivo de que la versión final de la A2I sea debidamente consensuada y contrastada.

Los participantes de esta iniciativa serán seleccionados por ser expertos en alguna de las áreas de interés identificados en esta A2I de conformidad con los objetivos establecidos. El grupo de participantes debe ser suficiente en número y suficientemente representativo de todos los colectivos del sector para garantizar una perspectiva global desde todos los puntos de vista.

Se busca contar con representantes de los siguientes colectivos:

5.3.2. Autoridades competentes nacionales.

La creación de un documento de estas características requiere la colaboración y la aprobación por parte de todos los actores principales implicados en el marco de la Ciberseguridad nacional definido por la **Estrategia de Ciberseguridad Nacional** para contar con el consenso y respaldo de todos los intervinientes, entre los que se encuentran todos los actores implicados con competencias en ciberseguridad.

5.3.3. Usuarios finales

Los **usuarios finales** que demandan soluciones de ciberseguridad, entre los que se encuentran las Administraciones Públicas, el Ministerio de Defensa, el Ministerio de Interior, incluyendo las Fuerzas y Cuerpos de Seguridad del Estado, los representantes de pymes, de ciudadanos, así como la demanda sofisticada (sectores y operadores estratégicos) son también actores relevantes en la elaboración de esta A2I.

5.3.4. Organismos de investigación

De igual modo, el documento debe plasmar las capacidades de los **organismos de investigación** de carácter nacional**,** por lo que se requiere contar con su visión y activa participación. Según la Ley 14/2011 (reformada por la Ley 17/2022), un organismo de investigación es una entidad pública o privada que tiene como objetivo principal la realización de actividades de investigación científica y técnica. Estos organismos pueden ser universidades, centros de investigación, institutos y/o centros tecnológicos, unidades de I+D empresarial, fundaciones, etc.

5.3.5. Industria de ciberseguridad

La visión de la **industria de la ciberseguridad** como agente capaz de generar soluciones y productos de ciberseguridad a los usuarios finales, guiando y canalizando la actividad del ecosistema investigador, también es fundamental a la hora de redactar un documento de estas características. En esta categoría se engloban entidades de todos los tamaños desde startups de nicho, micropymes, pymes y grandes empresas, y tanto centradas en producto como en servicios.

5.3.6. Asociaciones y agrupaciones sectoriales

Representativas tanto de la industria, como de la investigación, así como de usuarios finales sectoriales.

Por ejemplo, la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC) [23], compuesta por universidades y centros de investigación y tecnológicos, ha identificado la creación de esta A2I como una de las medidas prioritarias a realizar para la formulación, definición y aterrizaje de las estrategias tanto nacionales como europeas en materia de I+D+i en ciberseguridad.

5.3.7. Ecosistema inversor

Potenciar nuestra industria de ciberseguridad nacional actual y futura requerirá también identificar, involucrar y hacer partícipe a los agentes públicos y privados de inversión sensibles a la A2I y los propósitos que persigue.

5.3.8. Otros agentes

Se invita a otros agentes involucrados en la actividad investigadora, innovadora, financiadora, normativa o reguladora a que aporten su visión y colaboren de forma activa y participativa.

INCIBE y el resto de los miembros del grupo decisor podrán proporcionar contactos en las entidades enumeradas anteriormente, si fuera necesario, para la elaboración de la A2I.

5.4. Taxonomía

Para la elaboración de los resultados previstos, es preciso disponer de una taxonomía o taxonomías de referencia que permitan clasificar las fortalezas, las oportunidades, las soluciones, así como las líneas de investigación u otras características necesarias. Esto permitirá seguir esquemas de referencia aceptados por el sector de ciberseguridad español y que permitan la clasificación de elementos y facilitar su comparación.

La taxonomía por emplear será la elaborada por el SGT2 denominada MITEC y será utilizada a lo largo de los trabajos descritos en este documento. La taxonomía en sí misma no forma parte del alcance de la A2I, pero deberá ser utilizada a lo largo de los trabajos descritos en este documento.

Los anexos de este documento amplían más información en relación con la taxonomía a emplear.

5.5. Resultados previstos

El resultado principal a generar en este proyecto es la elaboración de la propia **A2I** como documento de referencia, que aglutina los objetivos planteados.

Adicionalmente, para poder completar esta información se prevé también como resultado previo la generación de determinados **informes preparatorios**. Estos informes deberán contener un diagnóstico riguroso sobre el estado actual de determinadas temáticas y tener entidad de documento independiente con posibilidad de poder publicarse por separado siendo autocontenidos y aportando información completa por sí mismos.

Se detallan a continuación los citados informes preparatorios:

5.5.1. Análisis comparativo de agendas estratégicas y otras iniciativas internacionales

En el contexto europeo, disponemos de distintos estudios en ámbito de la ciberseguridad y la seguridad. Más concretamente, la asociación europea ECSO (*European Cybersecurity Organisation*) elaboró a finales de 2016 una Agenda Estratégica de Investigación e Innovación (SRIA) [24] en el ámbito de la ciberseguridad, que fue posteriormente analizado por ENISA [25].

Del mismo modo se incluye el *roadmap* tecnológico elaborado por SPARTA [26] que es uno de los 4 pilotos de centros de competencia en ciberseguridad lanzados por la Comisión Europea.

La Comisión Europea ha elaborado también un “Cybersecurity Atlas” [27] donde se realiza un mapeado de todos los grupos de investigación europeos en el ámbito de la ciberseguridad.

Asimismo, en el contexto europeo, la Comisión Europea acaba de hacer públicos los resultados del estudio de caracterización del sector de la seguridad civil europeo [28].

Estos documentos deberán ser analizados y comparados previamente para la elaboración de la A2I en España, así como otros posibles documentos de referencia de consorcios de proyecto, asociaciones u organizaciones internacionales, u hojas de ruta para facilitar objetivos comunes, así como perfilar oportunidades diferenciales identificadas.

5.5.2. Mapa de capacidades de I+D en ciberseguridad

El objetivo es identificar las líneas de investigación del ecosistema nacional de I+D+i en ciberseguridad, identificando su grado de madurez y liderazgo en el contexto internacional, así como las más noveles, o inexistentes.

Incluyendo los siguientes grupos:

- Organismos de investigación.
- Unidades de I+D empresarial.

Para el informe de las capacidades de I+D nacionales de universidades y organismos de investigación se realizará de forma coordinada con la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC).

5.5.3. Informe de capacidades de la Industria de ciberseguridad – Oferta

El objetivo de este informe será formalizar la industria de ciberseguridad nacional (productos/soluciones y servicios) y conocer sus capacidades, en particular, en comparación con un conjunto de países de referencia, entre los que podrían encontrarse los siguientes:

- Alemania
- Francia
- Reino Unido
- Estonia
- Israel
- Estados Unidos

El informe deberá segmentar los mercados en base a la taxonomía definida, poniendo especial atención en ámbitos de valor y crecimiento.

5.5.4. Informe del mercado de la ciberseguridad – demanda

El objetivo de este informe es detectar las necesidades del mercado, actuales y futuras, tanto de sectores usuarios de ciberseguridad (Administración Pública, finanzas, transporte, fabricación, servicios de suministro, etc.) como de la propia industria de ciberseguridad (empresas de productos y servicios de ciberseguridad), en particular a necesidades que no estén suficientemente cubiertas por productos nacionales o de estados miembros de la Unión Europea.

Se deberán identificar igualmente los principales retos de ciberseguridad a los que se enfrentan las organizaciones y para los que no existe una solución adecuada.

5.5.5. Mercado de la ciberseguridad

Se incluirá en el informe el nivel de madurez y capacidad de adquisición de tecnología de los usuarios finales nacionales de tecnologías de ciberseguridad. Esta parte del informe se deberá realizar por sectores cuya resiliencia haya que preservar como son sectores relevantes del ámbito económico, de infraestructuras y de servicios, o sectores estratégicos y/o críticos. Un listado posible, sin ser exhaustivo de sectores a cubrir es:

- Financiero
- Transporte y movilidad
- Fabricación
- Servicios de suministro (agua, energía, etc.)
- Comercio
- Salud
- Alimentación
- Logística
- Telecomunicaciones
- Gobierno electrónico
- Servicios profesionales (abogados, notarios, oficinas en general).

5.5.6. Retos

Realizar una prospección tecnológica, tomando como referencia las industrias que en España se consideren prioritarias, y analizar sus retos o necesidades en ciberseguridad no cubiertas actualmente por el mercado.

Se propone segmentar los retos tecnológicos en función del ámbito de aplicación, siguiendo los ámbitos tecnológicos de la taxonomía seleccionada.

5.5.7. Informe de la financiación de la I+D en ciberseguridad

Identificación de programas de financiación de la I+D+i en España (nacionales, regionales y locales) tanto específicos como aquellos con cabida para la ciberseguridad. Adicionalmente establecer una comparativa con dichos programas de iniciativas a nivel EU y otros países siguiendo las recomendaciones descritas en el “Apartado 5.5.3”.

Visualmente podría ilustrarse esta información a modo de mapa geográfico mostrando las zonas con mayor o menor cobertura de financiación de la I+D+i en ciberseguridad.

Adicionalmente se deberían analizar los procesos de inversión (públicos, privados y mixtos) y sus actores en los últimos años y conocer sus motivaciones.

5.6. Fases previstas

Se identifican inicialmente las siguientes fases:

5.6.1. Fase previa

Esta primera fase contempla la elaboración de la A2I incluyendo la generación de sus informes preparatorios. Para ello será preciso la preparación de la licitación, con sus pliegos de descripciones técnicas y cláusulas administrativas, el proceso de validación y aprobación jurídico-económico, así como la publicación en la Plataforma de Contratación del Sector Público. A continuación, el proceso de recepción de ofertas, su valoración, comprobación de solvencias, y por último la **firma del contrato** con la entidad que resulte adjudicataria de este proceso.

5.6.2. Fase preparatoria y documental

Incluye la **investigación de escritorio** en la que se identificará y analiza documentación existente relevante a nivel nacional e internacional relacionada con los objetivos de la A2I y los distintos apartados en los que se espera una contribución.

En esta fase se realiza un **diseño preliminar** de la A2I y se identifican los **informes preparatorios** necesarios para su elaboración, con hipótesis a contrastar con la contribución de las partes interesadas. También se identifican los posibles candidatos a participar en la redacción de este documento y sus estudios preparatorios. Con esta información se puede preparar la recogida de datos por parte de los participantes con la generación de cuestionarios y guiones de entrevista. En paralelo esta fase actualiza la planificación prevista con una visión más realista de entregables, hitos y plazos.

A continuación, se procede a la **presentación oficial** de la iniciativa, en la que se invita formalmente a la participación abierta y colaboración de los participantes.

5.6.3. Fase de recopilación de datos

Se procede a la **toma de datos** en la que se entrevista de una forma guiada a los participantes de forma individual o grupal para recoger de forma completa y sistemática su visión y aportación con respecto a las temáticas a contrastar. La toma de información puede basarse en entrevistas, cuestionarios o reuniones de trabajo siguiendo técnicas como *focus group* o *think tank* u otras relevantes.

5.6.4. Fase de análisis, redacción y consolidación

Su objetivo es realizar un **análisis metodológico completo** de la documentación preparatoria junto con la opinión recabada de los participantes para la redacción

progresiva del texto de los informes preparatorios y de la A2I incluyendo sus conclusiones y recomendaciones.

Esta fase contará con hitos intermedios de validación y revisión por parte del grupo decisor y debe permitir la colaboración y refinamiento por parte de los participantes.

En esta fase se deben contrastar las hipótesis de partida, a la vez que se pueden generar nuevas que requieran de posibles contrastes específicos y puntuales por parte de los participantes. El resultado final de esta fase es un texto objetivo consensuado por todos los participantes. El texto definitivo debe contar con el refrendo específico de los participantes el cual se recomienda se encuentre explicitado en el propio documento final.

5.6.5. Fase de divulgación y difusión

Consensuado y refrendado el texto final de los informes preparatorios y la A2I, se dará comienzo a las principales actividades de esta fase, para dar a conocer el texto final de estos entregables al público objetivo indicado en el "Apartado **5.3.1.**.1" de este documento y al público en general. Los informes preparatorios podrían difundirse a medida que se vayan finalizando por diversos canales, y en el caso de la A2I, se efectuará una **presentación oficial.** Para todos los entregables, se incluirán presentaciones en otros eventos relacionados, adaptando la difusión, en cada caso, al público objetivo. En esta fase, se generarán materiales de difusión que acompañarán a las presentaciones y harán más sencillo asimilar su contenido.

5.7. Metodología

Aunque la metodología concreta a utilizar se definirá en la fase previa, se contempla utilizar al menos las siguientes técnicas:

- **Análisis documental.** Se deberá realizar un análisis profundo de la documentación que le pueda proporcionar INCIBE como input, así como una recopilación y estudio de fuentes secundarias nacionales e internacionales a identificar que puedan contribuir a enriquecer el diagnóstico de los resultados a generar.

- **Entrevistas en profundidad a actores relevantes en el sector.** Se deberá contar con la visión y aportación de actores relevantes en el sector de la ciberseguridad a través de la realización de entrevistas individuales o grupales en profundidad. La relación de participantes a entrevistar, el plan de entrevistas, y en su caso, el guion para las entrevistas semiestructuradas, serán aprobados por INCIBE.

- **Técnicas cuantitativas: realización de encuestas basadas en cuestionario a participantes identificados.**

- **Análisis y consolidación de la información** de partida junto con la contribución de los participantes.

- **Contribución de los participantes en la elaboración de los resultados** para participar en el refinamiento de los resultados y en el refrendo de los textos definitivos.
- **Difusión de los resultados** generados a través de diversos canales.
- **Uso de las herramientas colaborativas y de comunicación** para la orquestación de todas las actividades.

5.8. Cronograma e hitos principales

Las fases e hitos principales se detallan a continuación:

1. **Fase previa**, para la preparación de licitación, publicación, gestión y firma de contrato.
2. **Fase preparatoria**, durante la cual se desarrollará:

   a. Metodología propuesta y recursos disponibles.

   b. Identificación y análisis de documentación existente de referencia.

   c. Definir el diseño y marco analítico para desarrollar la iniciativa.

   d. Mapeado de las entidades de interés (potenciales participantes en el estudio) y creación de un catálogo interactivo de participantes, basado en la lista presentada en el "Apartado 5.3.1".

   e. Estrategia de recogida de datos.

   f. Principio de segmentación del resultado objetivo de cada informe preparatorio y A2I.

   g. Desarrollar documentos, cuestionarios y guiones de entrevista para recabar los datos por parte de los participantes.

   h. Integrar el documento de taxonomía elaborado por el Foro nacional de ciberseguridad.

   i. Al final de esta fase, se presentará un informe de la fase preparatoria.

3. **Fase de recopilación de datos,** durante la cual:

   a. Se elaborará de forma detallada la segmentación del resultado objetivo de cada informe preparatorio y A2I.

   b. Se recogerá y recopilará datos e información relevante utilizando metodologías estándares (informes, estadísticas, opiniones, etc.).

c. Al final de esta fase, se presentarán 2 informes intermedios, como resultado de los trabajos realizados.

4. **Fase de análisis, redacción y consolidación** durante la cual:

   a. Se elaborará un análisis de los datos e información recopilada en la fase anterior, utilizando las herramientas adecuadas.

   b. Se tratará de abordar y responder a todos los objetivos descritos en el "Apartado 5.1".

   c. Se extraerá conclusiones y lecciones aprendidas, así como un análisis pormenorizado de los datos.

   d. Se contrastará con los participantes la redacción y conclusiones que se vayan consolidando.

   e. Una presentación de la A2I, incluyendo un apartado de conclusiones globales basadas en el análisis y las características del sector de la ciberseguridad en España.

   f. Se propondrán recomendaciones (de financiación, regulación, estandarización, comunicación, etc.) que permitan a INCIBE y el grupo decisor proponer futuras tareas y acciones que favorezcan al sector de la ciberseguridad en España.

   g. Durante esta fase, el contratista presentará dos informes finales, como resultado de los trabajos realizados.

5. **Fase de divulgación y difusión,** durante la cual se desarrollarán:

   a. Un plan de difusión contemplando públicos objetivos y las acciones de difusión relacionadas.

   b. Materiales de difusión y presentaciones particularizadas para los diferentes públicos objetivos.

Se muestra a continuación, de forma resumida, una propuesta de cronograma para la realización de los trabajos incluyendo las fases y los hitos principales previstos.

DESCRIPCIÓN	Q1-23	Q2-23	Q3-23	Q4-23
1 FASE PREVIA				
Preparación de licitación				
Contratación				
2 FASE PREPARATORIA Y DOCUMENTAL				
Identificación y análisis de documentación de referencia				
Mapa de entidades de interés y participantes				
Metodología, diseño y marco analítico				
Diseño de segmentación de resultados				
Preparación cuestionarios y entrevistas				
Consolidación de taxonomía de referencia				
Informe fase preparatoria				
3 FASE DE RECOPILACIÓN DE DATOS				
Segmentación de resultados				
Recopilación y consolidación de información				
Informe intermedio 1				
Informe intermedio 2				
4 FASE DE ANÁLISIS, REDACCIÓN Y CONSOLIDACIÓN				
Análisis de datos				
Extracción de conclusiones				
Contraste con los participantes				
Presentación y recomendaciones				
Informe final para revisión				
Informe final para validación				
5 FASE DE DIVULGACIÓN Y DIFUSIÓN				
Plan de difusión				
Materiales y presentaciones				

6. PROMOCIÓN EXTERIOR DE LA INDUSTRIA DE CIBERSEGURIDAD ESPAÑOLA

Tras los primeros trabajos realizados por el grupo de trabajo de impulso a industria de ciberseguridad y a la I+D+i española en esta materia, se propone realizar un **plan estratégico a nivel país** que recopile todas aquellas acciones que se deberían abordar **para una exitosa promoción exterior**, teniendo como ejemplos a países como EE. UU., Israel, Estonia y Corea del Sur. En esta primera iteración, se ha contado con la contribución de ICEX y AMETIC.

Se propone desarrollar los siguientes puntos dentro del Plan Estratégico de Comunicación para la promoción de la industria de ciberseguridad española:

- Creación de una **marca país específica** para la promoción de la ciberseguridad española.
- Realización de una **estrategia de promoción exterior**: objetivos, destinatarios, presupuestos, esquemas de coinversión con el sector privado, KPIs, etc.
- Establecer un **organismo público líder de la iniciativa**, que dirija y decida la ciberseguridad nacional a todos los niveles.
- Desarrollo de un **catálogo de empresas españolas**: clasificado al menos, por tamaño, por especialización tecnológica o de servicios, por localización y por sectores de actividad de sus clientes principales.
- **Colaboración** estrecha dentro de este plan **con organismos internacionales** colaboradores como puedan ser: embajadas, oficinas comerciales de España en el exterior, cámaras de comercio oficiales españolas en el Exterior, comunidades, lobbies, etc...
- **Designación para los tres mercados prioritarios de un interlocutor** específico en la Oficina Comercial de España (Ofecomes), un punto de contacto, que centralice y focalice todas las actividades de promoción y generación de oportunidades comerciales.
- **Coordinación de acciones con foco en ciberseguridad dentro del Plan Cameral de Internacionalización**, que se elabora y ejecuta de acuerdo con el Ministerio de Industria, Comercio y Turismo y consensuado con ICEX. Este Plan contiene actuaciones de interés general en materia de formación, información y promoción dirigidas a promover la internacionalización de las empresas, tales como misiones comerciales, visitas y participaciones en ferias, realizadas por las cámaras de comercio. Además, el Plan incluye misiones comerciales específicas

realizadas por la Cámara de Comercio de España. Asimismo, incluye programas específicos de asesoramiento individualizado a pymes para su salida a mercados exteriores, con especial atención a la innovación, digitalización y posicionamiento exterior como factores claves de la competitividad de las pymes.

- **Creación de un programa de becarios** específicos en ciberseguridad, en una selección de Ofecomes según intereses de mercado, con una II Fase en España, tanto en empresas como en Instituciones/Asociaciones.

- **Formación y cultura de la ciberseguridad en el personal de los organismos internacionales colaboradores** en el plan estratégico, conocedor del ecosistema de ciberseguridad de España.

- Definición de un **plan de atracción de inversiones** específico a través de ***Invest In Spain*.**

De cara a cumplir con los objetivos anteriormente descritos se pueden identificar como acciones concretas dentro del Plan estratégico de comunicación para el impulso de la industria de ciberseguridad fuera de España las siguientes:

- **Encuentros bilaterales**. Por ejemplo, en programas de innovación estatales, en rondas de financiación de Startups, en eventos organizados por organismos públicos.

- Campañas específicas en **grandes eventos internacionales.**

- **Campañas específicas países clave**: EE. UU., Israel, Estonia.

- **Campañas específicas zonas clave**: Europa, América latina y Asia

- Creación de un **programa específico de internacionalización** para empresas del sector de ciberseguridad con apoyo mínimo de 5 años, al estilo de ***ICEX NEXT***: apoyos individualizados en esfuerzos de promoción de marca individual; o bien ***XPande***: Plan de Expansión Internacional de las Pymes de la Cámara de Comercio de España.

- Lanzamiento de **concursos internacionales de ideas** de aplicación a la administración pública española.

Se propone un cronograma de alto nivel para el año 2023

DESCRIPCIÓN	Q1-23	Q2-23	Q3-23	Q4-23
1. Plan detallado de trabajo y acuerdos institucionales				
2. Implementación de acciones				

7. CONCLUSIONES

Los objetivos planteados al comienzo de los trabajos de esta segunda fase del GT2 han sido alcanzados en gran medida. Sin embargo, es obvio que persisten necesidades comunes dentro del ecosistema nacional para alcanzar la misión global del FNCS, especialmente relacionadas con:

- la generación de un marco común en cuanto a una **única taxonomía** que alinee a todos los actores del ecosistema de ciberseguridad nacional y europeos (**MITEC**)
- la protección del tejido productivo nacional, impulsando la adopción de medidas de mejora de la **ciberseguridad por parte de pymes, micropymes y autónomos**
- la generación de actuaciones de I+D+i mediante la **definición de la Agenda de Investigación e Innovación (A2I)** en ciberseguridad
- el **incremento de la oferta y demanda de productos y servicios de ciberseguridad** de la industria española, así como su internacionalización
- **y el incremento el peso de la industria española de ciberseguridad** en el mercado europeo y global.

Es clave **continuar midiendo las capacidades nacionales** de manera constante y continuada, lo que permitirá comprobar que las medidas adoptadas por el Gobierno central y autoridades con competencias en ciberseguridad son efectivas y, si no lo fueran, poder adaptarlas de manera ágil. Del mismo modo la **definición de la cadena de valor** en ciberseguridad y de un **modelo relacional entre la oferta y la demanda** es fundamental para la **generación de nuevas oportunidades** para la industria en base a las prioridades de país para la protección del ciberespacio y de toda la sociedad en global.

En relación con la **taxonomía (MITEC)** y con el principal objetivo de tener un **registro común entre todos los actores de la cadena de valor**, es prioritario finalizar estos trabajos durante el primer trimestre del 2023 para que puedan ser validados por todo el sector y ser utilizados para la definición de la Agenda de investigación e innovación en ciberseguridad (A2I).

Si queremos avanzar como país tenemos que seguir protegiendo al tejido productivo, que son principalmente pymes que, durante estos últimos dos años, han comenzado una digitalización acelerada y que, si bien les permitirá ser mucho más competitivas, también les expone mucho más a los ciberataques. Por eso **es clave la continuidad y la vigilancia de la efectividad de las acciones globales** que se han puesto en marcha durante este 2022 en el ámbito de la **protección, concienciación y formación de este colectivo de PYMES, micropymes y autónomos**.

INCIBE lanzará durante el 2023 un **programa de impulso y fomento a la acreditación de proveedores de las administraciones en el ENS y en la ISO 22.300**. Este programa no solo aumentará el número de proveedores de la administración con este tipo de acreditaciones, sino que también **fomentará y dinamizará la industria que se dedica a la implantación y certificación de estas normativas**. Este programa estará alineado con las acciones descritas en el Plan de Choque de Ciberseguridad aprobado en el Acuerdo de Ministros de mayo de 2021 [29].

El objetivo de crear una Agenda de Investigación e Innovación a nivel nacional es ambicioso, a la par que necesario, y se determina que para que tenga éxito debe contar con una **participación público-privada** suficiente en número de participantes, y representativa de todas las partes interesadas. Adicionalmente, debe prestar especial atención a los cambios en las políticas industriales afines a la ciberseguridad para asegurar la participación e influencia en las mismas. Debe contar con una **gobernanza** igual de participativa, con el liderazgo del INCIBE y la presencia de miembros del Foro con compromiso firme para guiar y dirigir la preparación de la Agenda. También cabe destacar que previo a la redacción de esta A2I, se ve necesario la generación de una colección de **informes preparatorios** que proporcionen información previa específica de diferentes ámbitos tales como capacidades de I+D+i, necesidades de los usuarios finales, capacidad de la industria, oportunidades de mercado y mecanismos de financiación. Con esta información, y con la colaboración de los todos, se podrá concluir con una Agenda debidamente contrastada y refrendada, que en un escenario 2023-2030 fije los objetivos y prioridades en esta materia a nivel nacional.

El **crecimiento** de la industria y su **promoción internacional** no puede ser exitoso sin un **plan global e institucional** en el que participen todos los organismos públicos y asociaciones sectoriales que apoyen la promoción de la industria en el exterior, así como la atracción de inversión extranjera. Acciones concretas a nivel de país deben ser una prioridad para los siguientes 12 meses.

En conclusión, este grupo de trabajo plantea continuar con las acciones descritas en este documento durante el 2023 y podrá incluir nuevas si alguno de los agentes lo considera o si bien recibe una petición expresa del Consejo Nacional de Ciberseguridad.

8. REFERENCIAS

[1] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_es

[2] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es

[3]https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_es

[4] https://commission.europa.eu/strategy-and-policy/recovery-plan-europe_es

[5] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

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

[7] https://espanadigital.gob.es/

[8] https://planderecuperacion.gob.es/

[9]https://industria.gob.es/es-es/Documents/Directrices%20Generales%20de%20la%20Pol%C3%ADtica%20industrial%20espa%C3%B1ola%2025.02.19%20FINAL.pdf

[10] https://www.ciencia.gob.es/Estrategias-y-Planes/Estrategias/Estrategia-Espanola-de-Ciencia-Tecnologia-e-Innovacion-2021-2027.html;jsessionid=9462AFB00463E8B7EAE488B3FAA97A9F.2

[11] https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017

[12] https://www.dsn.gob.es/es/documento/estrategia-nacional-contra-crimen-organizado-delincuencia-grave

[13] https://foronacionalciberseguridad.es/

[14] https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Febrero/Noticia-2019-02-18-El-Gobierno-aprueba-creacion-Centro-de-Operaciones-de-Ciberseguridad-para-AGE.html

[15] https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2518-ccn-stic-140-taxonomia-de-referencia-para-productos-de-seguridad-tic/file.html

[16] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

[17] https://www.incibe.es/industria-cpi/cpi-primera-convocatoria

[18] https://www.incibe.es/industria-cpi/cpi-segunda-convocatoria

[19] https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html

[20] https://foronacionalciberseguridad.es/index.php/publicaciones

[21] https://ecs-org.eu/

[22] https://cybercompetencenetwork.eu/

[23] https://www.renic.es/es

[24] https://web.archive.org/web/20220319210957/https:/www.ecs-org.eu/documents/publications/59e615c9dd8f1.pdf

[25] https://www.enisa.europa.eu/publications/priorities-for-eu-research/at_download/fullReport

[26] https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf

[27] https://cybersecurity-atlas.ec.europa.eu/

[28] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study_en

[29] Plan de choque de Ciberseguridad https://portal.mineco.gob.es/es-es/comunicacion/Paginas/210525_np_ciberseguridad.aspx).".

[30] ECSO Market Radar Taxonomy. Recuperado de https://ecs-org.eu/documents/uploads/ecso-cybersecurity-market-radar-taxonomy-table.pdf

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

ANEXO I – ACTUALIZACIÓN DE KPIs. PROGRAMAS DE DIGITALIZACIÓN DE LAS PYMES

Cámara de Comercio de España

Ciberseguridad en las Pymes
Situación diciembre 2022

Juan Miguel Cuéllar del Río
Subdirector de Competitividad
Cámara de Comercio de España

Cámara de Comercio de España

1. **Programa Ciberseguridad de la Cámara de Comercio de España**
2. **Oficinas Acelera Pyme - Cámaras de Comercio**
3. **Programa Kit Digital**

Cámara de Comercio de España

1. **Programa Ciberseguridad de la Cámara de Comercio de España**

1. Programa Ciberseguridad

UNIÓN EUROPEA · Ciberseguridad · Cámara de Comercio de España

El uso SEGURO Y FIABLE del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

Objetivos **Estratégicos**

1. Que haya más **EMPLEADOS SENSIBILIZADOS** a través de sus empleadores mediante **planes de sensibilización**. Cuantas más empresas pongan en marcha planes de sensibilización, habrá más potenciales empleados sensibilizados en ciberseguridad que apliquen medidas de seguridad.

2. **MEJORAR LA SEGURIDAD DE LOS SERVICIOS DE LAS EMPRESAS EN EL CIBERESPACIO**
   - Fomentar que las empresas dispongan de un **plan de seguridad** como una fuente para generar confianza: más empresas/clientes harán negocios con ellas (B2B y B2C), confiarán más en ellas.
   - Fomentar que las empresas cuiden de la seguridad de su web, en particular si disponen de tienda online y utilizan formas de pago online.

3. Promover la implantación de **HERRAMIENTAS DE CIBERSEGURIDAD** en el día a día de las empresas y sus operaciones y gestiones más habituales.

4. Fomentar que las empresas tengan un plan de **CONTINGENCIA Y CONTINUIDAD.**

1. Programa Ciberseguridad

UNIÓN EUROPEA · Ciberseguridad · Cámara de Comercio de España

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Objetivo III

Protección del ecosistema empresarial y social y de los ciudadanos.

Líneas de acción

- 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.
- Impulsar en el sector empresarial la **implantación de estándares** reconocidos de ciberseguridad.

Objetivo IV

Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.

Líneas de acción

- 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.
- Promover la **difusión de la cultura de la ciberseguridad** como una buena práctica empresarial.
- **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.

1. Programa Ciberseguridad

UNIÓN EUROPEA · Ciberseguridad · Cámara de Comercio de España

Ciberseguridad

Programa de ayudas *que capacite a las pymes a prevenir los principales* **riesgos en Ciberseguridad**, *asumibles por ellas mismas, para garantizar que los Sistemas de Información y Telecomunicaciones que utilizan, poseen un adecuado nivel de Ciberseguridad.*

Fase I Plan Director

- Situación de partida y recomendaciones genéricas
- Estrategia de la organización
- Proyectos recomendados

Fase II Implantación

- Implantación de herramientas de seguridad
- Seguimiento de la implantación
- Ayuda a la Inversión

Acciones de sensibilización Ciberseguridad

Fase I

Análisis exhaustivo de los Sistemas de Información y Telecomunicaciones de la empresa para identificar los principales **riesgos referidos a la ciberseguridad**.

- Sin coste para la empresa.
- Realizado por los técnicos de las Cámaras.
- Cofinanciado por FEDER y **otro cofinanciador público.**

Fase II

La empresa recibe una **subvención** para la implantación de herramientas de ciberseguridad. Se realizará un seguimiento del ritmo de ejecución y de la adecuación de los proyectos de implantación.

- Gasto máximo cofinanciable: 4.000 €.
- Ayuda de entre un 40% y un 85%, según la CCAA.
- Cofinanciado por FEDER y la empresa.

1. Programa Ciberseguridad

Fase I: Asesoramiento

Diagnóstico individualizado para establecer recomendaciones y priorizar acciones y proyectos a implantar, en materia de ciberseguridad.

1. Programa Ciberseguridad

Fase de Ayudas

Catálogo de herramientas y soluciones tipo específicas de ciberseguridad

Herramientas de Seguridad - Ejemplos gastos elegibles:

- Gestión de la identidad y contraseñas
- Protección en el puesto de trabajo
- Detección y eliminación de malware
- Seguridad en aplicaciones y datos
- Gestión de parches y vulnerabilidades
- Seguridad en las redes
- Redes Privadas Virtuales
- Antivirus, cortafuegos, ransomware
- Adaptación a la RGPD

1. Programa Ciberseguridad

Empresas Participantes

	2020	2021	2022	Total
Beneficiarias Directas	212	279	483 (compromiso)	974
Soluciones Implantadas	349	516	662 (diciembre 2022)	1.527
Jornadas Sensibilización	39	15	10 (diciembre 2022)	64
Empresas Sensibilizadas	1.402	717	560 (estimado 2022)	2.679

1. Programa Ciberseguridad

Tamaño de las Empresas

	2020	2021	2022	Total
0 – 2 Empleados	26,42 %	31,18 %	34,62 %	31,64 %
3 – 9 Empleados	35,38 %	27,60 %	34,62 %	32,64 %
>= 10 Empleados	38,21 %	41,22 %	30,77 %	35,72 %

1. Programa Ciberseguridad

Nivel de Madurez en Ciberseguridad

		0 a 2	3 a 9	10 o más	Total
Nivel 1 (Incipiente)	La ciberseguridad de la empresa depende de los conocimientos de los empleados, no existiendo protocolos internos que establezcan la forma de actuar	88,15 %	84,07 %	69,75 %	80,15 %
Nivel 2 (Emergente)	La empresa ha establecido una serie de medidas informales con el objetivo de salvaguardar la estructura informática, no existe un plan para la formación de los trabajadores en materia de ciberseguridad	10,45 %	14,92 %	27,78 %	18,08 %
Nivel 3 (Avanzado)	La empresa ha documentado un procedimiento de actuación en materia de ciberseguridad, además de ofrecer formación a los trabajadores en esta materia	1,39 %	1,02 %	2,47 %	1,76 %

1. Programa Ciberseguridad

Nivel de Madurez en Ciberseguridad

	Incipiente	Emergente	Avanzado
Seguridad de los Equipos y Recursos Humanos	81,26 %	16,76 %	1,98 %
Medidas de Protección	73,32 %	24,48 %	2,21 %
Seguridad de las Operaciones y Comunicaciones	80,04 %	17,86 %	2,09 %
Adopción de Aspectos Normativos y Regulatorios	43,33 %	37,38 %	19,29 %

1. Programa Ciberseguridad

Proyectos Implantados

1.527 Proyectos de Ciberseguridad implantados.

Proyectos	Total	%
Copias de Seguridad	190	12,44 %
Adaptación a la RGPD	172	11,26 %
Auditoría Técnica de Seguridad.	167	10,94 %
Antimalware	155	10,15 %
Firewall (hardware)	149	9,76 %
Auditoría Página Web y Cumplimiento LSSI-CE	137	8,97 %
Sistema de Alimentación Ininterrumpida (SAI)	109	7,14 %
Red VPN (Accesos remotos seguros)	97	6,35 %
Análisis de Vulnerabilidades	95	6,22 %
Seguridad de Correo Electrónico	63	4,13 %

1. Programa Ciberseguridad

Proyectos Implantados

1.527 Proyectos de Ciberseguridad implantados.

Proyectos	Total	%
Obtención Certificación ISO 27001.	47	3,08 %
Autenticación Multifactor	30	1,96 %
Gestión centralizada de dispositivos	23	1,51 %
Plan de Contingencia y Continuidad	23	1,51 %
Encriptación de datos	19	1,24 %
Sistema de Control de Acceso	14	0,92 %
Sistema de Centralización de Certificados	11	0,72 %
Plataforma de Monitorización de Redes	10	0,65 %
Sistema SIEM (Información de seguridad y gestión de eventos)	8	0,52 %
Control de Aplicaciones (Whitelisting)	8	0,52 %

1. Programa Ciberseguridad

Próximos Pasos

- Actualización del diagnóstico personalizado, en función de la explotación de los datos de ejecución del propio programa y de la definición de la matriz de categorización de pymes.
- Actualización y ampliación de los proyectos subvencionables.
- Continuar y potenciar la sensibilización a las empresas en materia de ciberseguridad.

2. Oficinas Acelera Pyme - Cámaras de Comercio

2. Oficinas Acelera Pyme – Cámaras de Comercio

Ayudar a las **EMPRESAS** a ser más **COMPETITIVAS** en sus procesos de negocio/producción, productos o servicios utilizando **TECNOLOGÍAS DIGITALES**

Objetivos **Estratégicos**

1. **DAR CUMPLIMIENTO** a las prioridades nacionales y regionales en materia de transformación digital.
2. **APOYAR A LAS PYMES EN SU PROCESO DE DIGITALIZACIÓN.**
3. **FOMENTAR LA INNOVACIÓN, LA CREACIÓN DE EMPLEO y el EMPRENDIMIENTO DIGITAL** fortaleciendo así la competitividad.
4. **DIFUNDIR Y SENSIBILIZAR** en el uso de las tecnologías.
5. **BRINDAR INFORMACIÓN SOBRE APOYO FINANCIERO** a las pymes en la demanda para dominar la transformación digital.
6. **FOMENTAR LAS RELACIONES ENTRE LOS DISTINTOS AGENTES DEL ECOSISTEMA,** facilitando un punto de encuentro y compartiendo mejores prácticas.

2. Oficinas Acelera Pyme – Cámaras de Comercio

Actividades

Asesoramiento y Atención personalizada

- Resolución de dudas respecto a procesos de transformación digital de la pyme.
- Ilustración de las oportunidades que la digitalización puede crear para las pymes y cómo éstas pueden implementarse con éxito en la práctica.
- Apoyo específico en el diseño y la implementación de una estrategia de digitalización.
- Acceso a instalaciones y servicios para experimentación en el desarrollo de productos o soluciones.
- Información sobre ayudas de las distintas Administraciones Públicas o privadas para promover o hacer uso de tecnologías digitales innovadoras.
- Fomento de las relaciones entre los distintos agentes del ecosistema, facilitando un punto de encuentro, así como la conexión entre oferta y demanda y compartiendo mejores prácticas.

2. Oficinas Acelera Pyme – Cámaras de Comercio

Actividades

Acciones de Sensibilización

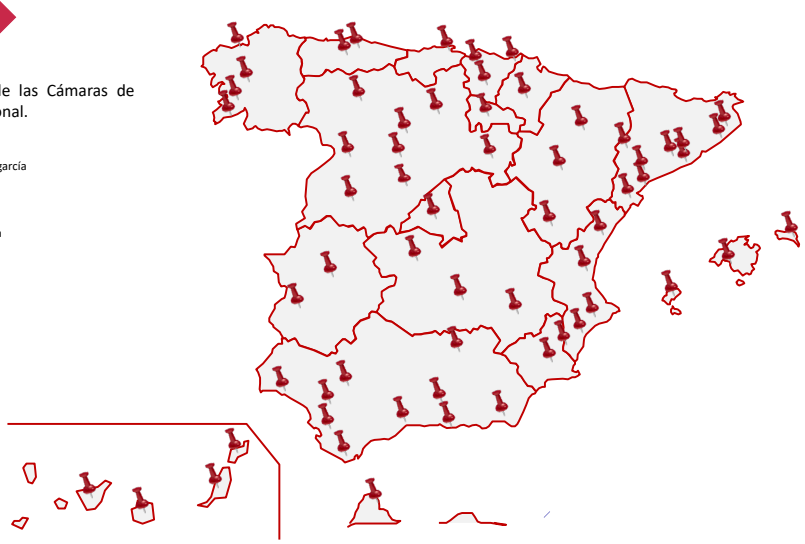
- Labores de difusión y sensibilización, incluyendo la generación, difusión y puesta en valor de contenidos, sobre las ventajas de la incorporación de las Tecnologías de la Información y las Comunicaciones (TIC) en los procesos de negocio, para optimizar su funcionamiento, de modo que se favorezca la demanda de tecnologías innovadoras que contribuyan a la mejora de su productividad.
- Establecimiento de Centros Demostradores de Tecnología para la incorporación de las nuevas tecnologías en las empresas.
- Capacitación sobre tecnologías digitales.
- Otras actividades de promoción del uso de las TIC para la mejora competitiva de las empresas.

2. Oficinas Acelera Pyme – Cámaras de Comercio

Distribución de las Oficinas Acelera Pyme

Hay un total de 62 Oficinas Acelera Pyme de las Cámaras de Comercio, repartidas por todo el territorio nacional.

A Coruña	Gran Canaria	Pontevedra, Vigo y Vilagarcía
Álava	Granada	Sabadell
Albacete	Huelva	Salamanca
Alcoy	Huesca	Sant Feliu de Gíxols
Alicante	Ibiza y Formentera	Santiago de Compostela
Almería	Jerez de la Frontera	Segovia
Badajoz	La Rioja	Sevilla
Barcelona	Lanzarote	Soria
Bilbao	León	Tarragona
Burgos	Linares	Tenerife
Cáceres	Lleida	Terrasa
Cádiz	Madrid	Teruel
Campo de Gibraltar	Málaga	Toledo
Cantabria	Mallorca	Tortosa
Castellón	Menorca	Tui
Ceuta	Motril	Valencia
Ciudad Real	Murcia	Valladolid
Fuerteventura	Navarra	Valls
Gijón	Orihuela	Zamora
Gipuzkoa	Oviedo	Zaragoza
Girona	Palencia	



2. Oficinas Acelera Pyme – Cámaras de Comercio

Actividad en Ciberseguridad

	2021	2022	Total
N.º Oficinas Cámaras	39	(39) + 23	62
Asesoramientos Personalizados	3.523	12.482	16.025
Asesoramientos en Ciberseguridad	71 (2%)	87 (0,70%)	158 (0,59%)
Jornadas Realizadas	444	1.217	1.661
Jornadas sobre Ciberseguridad	31 (6,98%)	76 (6,24%)	107 (6,44%)
Empresas sensibilizadas	12.155	22.614	34.769
Empresas sensibilizadas en Ciberseguridad	551 (4,53%)	1.947 (8,61%)	2.498 (7,18%)

2. Oficinas Acelera Pyme – Cámaras de Comercio

Próximos Pasos

- Formación específica en ciberseguridad para los técnicos de las Oficinas Acelera Pyme de las Cámaras de Comercio.
- Aprovechar el potencial de las Oficinas Acelera Pyme de las Cámaras de Comercio para:
  - Continuar y potenciar la sensibilización a las empresas en materia de ciberseguridad.
  - Plan de Comunicación para realizar sensibilización en ciberseguridad y fomentar el asesoramiento en ciberseguridad por parte de las Oficinas Acelera Pyme.

3. Programa Kit Digital

3. Programa Kit Digital

Marco del Programa

El programa Kit Digital **está financiado por los fondos Next Generation de la Unión Europea,** creados para hacer frente a los desafíos planteados por la pandemia de la COVID-19 y construir la Europa de la nueva generación. En concreto, se materializa a través del **Mecanismo de Recuperación y Resiliencia (MRR) y React-UE.**

El **Plan de Recuperación, Transformación y Resiliencia** se construye sobre la base de 4 ejes transversales, 10 políticas palanca y 30 Componentes divididos en una gran variedad de Reformas e Inversiones.

El **programa Kit Digital**, en concreto, se encuadra bajo el **Componente 13 Inversión 3,** dedicado al impulso a las PYME. Así mismo, contribuye a actuaciones del **Componente 15 y Componente 19.**

3. Programa Kit Digital

Objetivo

El **programa Kit Digital**, **nace para apoyar la transformación digital de pequeñas empresas, microempresas y personas en situación de autoempleo**, con el **objetivo de subvencionar la adopción de soluciones de digitalización disponibles en el mercado,** lo que facilitará un progreso significativo en sus niveles de madurez digital**.**

Estas soluciones permitirán a las empresas **avanzar en la digitalización de áreas clave** como *presencia en internet, venta electrónica, gestión de clientes y proveedores, oficina digital, gestión y automatización de procesos* y *ciberseguridad.*

OBJETIVO

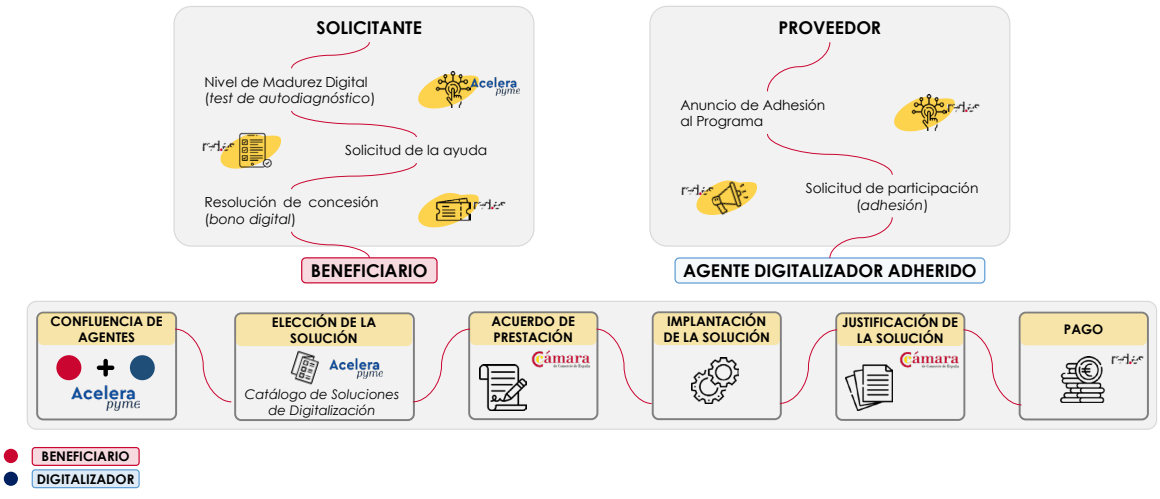
Dar cobertura a **1.000.000 de PYME y/o personas en situación de autoempleo.**

AYUDAS

Por valor de **3.067 millones de euros**, en el periodo 2021-2024.

3. Programa Kit Digital

Esquema general del Programa



3. Programa Kit Digital

Financiado por la Unión Europea NextGenerationEU · Plan de Recuperación, Transformación y Resiliencia · KIT DIGITAL · red.es · Cámara de Comercio de España

Beneficiarios

Pequeñas empresas, microempresas y personas en situación de autoempleo.

Cuyo domicilio fiscal esté ubicado en territorio español.

Independientemente de su sector o tipología de negocio.

		IMPORTE POR BONO
SEGMENTO I	Pequeñas empresas de entre 10 y menos de 50 empleados	12.000 €
SEGMENTO II	Pequeñas empresas o Microempresas de entre 3 y menos de 10 empleados	6.000 €
SEGMENTO III	Pequeñas empresas o Microempresas de entre 0 y menos de 3 empleados	2.000 €

3. Programa Kit Digital

Financiado por la Unión Europea NextGenerationEU · Plan de Recuperación, Transformación y Resiliencia · KIT DIGITAL · red.es · Cámara de Comercio de España

Categorías de Soluciones de Digitalización

El **bono digital** se podrá consumir en la **adquisición e implantación de soluciones de digitalización de las diferentes Categorías** disponibles en la plataforma Acelera Pyme y ofertadas por los Agentes Digitalizadores Adheridos. Estas Categorías de Soluciones de Digitalización, que **son extensibles a todos los sectores de actividades**, son las siguientes:

1. **SITIO WEB Y PRESENCIA EN INTERNET**
   Expansión de la presencia en internet por la creación de una web
2. **COMERCIO ELECTRÓNICO**
   Creación de una tienda online de compraventa con medios digitales
3. **GESTIÓN DE REDES SOCIALES**
   Promoción del beneficiario en redes sociales
4. **GESTIÓN DE CLIENTES**
   Digitalización y optimización de la gestión de relaciones comerciales
5. **BI Y ANALÍTICA**
   Explotación de datos para mejorar la toma de decisiones
6. **GESTIÓN DE PROCESOS**
   Automatización de procesos de negocio del beneficiario
7. **FACTURA ELECTRÓNICA**
   Digitalización de la emisión de facturas entre beneficiario y clientes
8. **SERVICIOS DE OFICINA VIRTUAL**
   Implantación de soluciones que permitan una colaboración eficiente
9. **COMUNICACIONES SEGURAS**
   Provisión de conexiones seguras entre los dispositivos del beneficiario
10. **CIBERSEGURIDAD**
    Seguridad básica y avanzada para los dispositivos del beneficiario

3. Programa Kit Digital

Funcionalidades y Servicios

Comunicaciones Seguras

- **SSL:** la solución deberá utilizar un protocolo de capa de sockets seguros, para crear una conexión segura y cifrada**.**
- **Cifrado extremo a extremo:** la solución deberá mantener las comunicaciones cifradas en todo su recorrido, con el objetivo de prevenir ataques.
- **Logs de conexión:** la solución deberá mantener un registro de los dispositivos que se han conectado a la red privada de la pyme.
- **Control de acceso:** la solución deberá permitir la conexión a la red privada de la pyme única y exclusivamente a los dispositivos autorizados por la empresa.
- **Dispositivos móviles:** la solución deberá estar disponible para su uso desde dispositivos móviles.
- **Configuración inicial y actualizaciones de seguridad:** se debe realizar una configuración inicial para su correcto uso, con las respectivas actualizaciones de firmas de *malware* y otros datos para detección de amenazas además de las actualizaciones de software de seguridad periódicas requeridas.

3. Programa Kit Digital

Funcionalidades y Servicios

Ciberseguridad

- ***Antimalware*:** la solución deberá proporcionar una herramienta que analice el dispositivo, su memoria interna y los dispositivos de almacenamiento externos**.**
- ***Antispyware*:** la solución deberá proporcionar una herramienta que detecte y evite el malware espía.
- **Correo seguro:** la solución deberá proporcionar herramientas de análisis del correo electrónico con las siguientes características: *Antispam*, con detección y filtro de correo no deseado; *Antiphishing*, con detección de correos con enlaces o malware que se sospecha sirvan para robar credenciales.
- **Navegación segura:** control de contenidos; *Antiadware* para evitar anuncios maliciosos.
- **Análisis y detección de amenazas:** la solución deberá permitir conocer el comportamiento de las amenazas conocidas y nuevas.
- **Monitorización de la red:** la solución deberá proporcionar herramientas que analicen el tráfico de red y alerten de amenazas.
- **Configuración inicial y actualizaciones de seguridad:** se debe realizar una configuración inicial para su correcto uso, con las respectivas actualizaciones de firmas de *malware* y otros datos para detección de amenazas además de las actualizaciones de software de seguridad periódicas requeridas.
- **Requisitos especiales de formación:** la formación impartida al beneficiario deberá incluir una tutorización para la configuración del software de seguridad, así como incluir un kit de concienciación en ciberseguridad para complementar la solución con habilidades de *firewall* humano.

3. Programa Kit Digital

Financiado por la Unión Europea NextGenerationEU · Plan de Recuperación, Transformación y Resiliencia · KIT DIGITAL · red.es · cámara de Comercio de España

Implantación de Soluciones de Ciberseguridad

Penetración de las categorías de soluciones de ciberseguridad en el programa. Porcentaje y número de Acuerdos de Prestación de Soluciones de Digitalización, correspondientes a las categorías de ciberseguridad, frente al total de Acuerdos (datos a 11.12.2022):

Número de empleados	Segmento I (10 – 49)	Segmento II (3 – 9)	Segmento III (0 – 2)	Total
Comunicaciones Seguras	4,13 % (2.114)	1,65 % (117)	0,50 % (1)	3,82 % (2.232)
Ciberseguridad	8,84 % (4.518)	4,98 % (353)	0,50 % (1)	8,34 % (4.872)

3. Programa Kit Digital

Financiado por la Unión Europea NextGenerationEU · Plan de Recuperación, Transformación y Resiliencia · KIT DIGITAL · red.es · cámara de Comercio de España

Próximos Pasos

- ✓ Plan de Comunicación para realizar sensibilización en ciberseguridad y fomentar la implantación de las categorías de solución de ciberseguridad y comunicaciones seguras.

ANEXO II- TAXONOMÍA DE COMPETENCIAS EN LA INDUSTRIA (ECSO)

En este Anexo I se detalla la taxonomía de capacidades definida por ECSO [30] 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 de la seguridad definidas en el marco de ciberseguridad NIST [30]: *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	Security Certification
5	IDENTIFY	Governance & Risk Management	Governance, Risk & Compliance (GRC)
6	IDENTIFY	Risk Assessment	Risk Management solutions & services
7	IDENTIFY	Rissk 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	Fraud Management
39	DETECT	Anomalies and Events	Intrusion Detection
40	DETECT	Security Continuous Monitoring	SIEM / Event Correlation Solutions
41	DETECT	Security Continuous Monitoring	Cyber Threat Intelligence
42	DETECT	Security Continuous Monitoring	Security Operations Center (SOC)
43	DETECT	Detection Processes	Underground/Darkweb investigation
44	DETECT	Detection Processes	Honeypots / Cybertraps
45	DETECT	Detection Processes	Social Media & Brand Monitoring

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

ANEXO III - TAXONOMÍA DE COMPETENCIAS EN LA INVESTIGACIÓN (JRC)

En este Anexo II se detalla la taxonomía de capacidades definida por la Comisión Europea, *Joint Research Comitee* (JRC) [31], que 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.

Esta taxonomía está actualmente en revisión.

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	**CATEGORIA**	**SUBCATEGORIA**
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;

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	CATEGORIA	SUBCATEGORIA
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		Vocational training.
34	Human Aspects	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		History of cybersecurity.

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	CATEGORIA	SUBCATEGORIA
53	Identity Management	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).

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	CATEGORIA	SUBCATEGORIA
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		ssment 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		Measurement and assessment of security levels

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	CATEGORIA	SUBCATEGORIA
109	Software and Hardware Security Engineering	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

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	**CATEGORIA**	**SUBCATEGORIA**
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).

Como se ha comentado, 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)

ANEXO IV – EJEMPLO DE TAXONOMÍA INTEGRADA GENERADA EN EL SGT2

Actualmente, se cuenta con una propuesta de taxonomía generada en el grupo de trabajo SGT2 del FNCS, que integra las taxonomías de ECSO [30] y del JRC [31], generando una taxonomía hibrida que partiendo de la taxonomía de ECSO permite mapear cada categoría de ECSO (60) con varias de las del JRC (149).

Se proporciona a modo de ejemplo una parte de la taxonomía integrada.

Esta taxonomía está siendo actualmente revisada en el marco del SGT2.

TAXONOMIA ECSO				TAXONOMIA 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

FORO
NACIONAL DE
CIBERSEGURIDAD

2023