España | digital 2026

PLAN ESTRATÉGICO INCIBE 2023-2025

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Ministerio de Asuntos Económicos y Transformación Digital

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. OBJETO Y ALCANCE DEL PRESENTE DOCUMENTO

El objeto del presente documento es recoger el Plan Estratégico Plurianual (PEP) para el periodo 2023-2025, conforme a lo comprometido por la entidad con la Subdirección General de Inspección de Servicios en relación con el control de eficacia de los artículos 85 y 86 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante LRJSP) correspondiente al Plan de Inspección de Servicios del Ministerio para el ejercicio 2020 en relación con la revisión trienal de las líneas estratégicas que se establece en los artículos 85.1 y 117.1 de la LRJSP.

Asimismo pretende adecuar la planificación prevista en el anterior PEP 2021-2025 al actual marco estratégico de la nueva agenda España Digital 2026 y a la ejecución y realización de los compromisos de INCIBE conforme a lo establecido en el Plan de Recuperación, Transformación y Resiliencia (PRTR).

De esta forma se pretende revisar y actualizar los cometidos previstos en el anterior PEP con los estipulados en el actual marco estratégico, permitiendo dar continuidad a los mismos en el presente marco temporal.

Con esta actualización se pretende por consiguiente armonizar el trabajo y las actuaciones realizadas en el pasado por INCIBE con los compromisos establecidos por el gobierno de España a través del Mecanismo de Recuperación y Resiliencia (MRR).

El PEP 2023-2025 ofrece una visión a alto nivel de las metas que INCIBE deberá alcanzar durante este periodo dando continuidad a los objetivos estratégicos previstos en el PEP 2021-2025 que permitan a la entidad desarrollar su misión eficaz y eficientemente, y avanzar hacia la realización de su visión; las líneas de actuación identificas con anterioridad que siguen vigentes en la actualidad y, finalmente el modelo de gobernanza actualizado al mismo.

Por consiguiente el PEP 2023-2025 y su alcance cubren los siguientes apartados:

- Misión, visión y valores.
- Fundamentos estratégicos y legales.
- Objetivos estratégicos y líneas de actuación.
- Modelo de gobernanza.

Con la actualización de este PEP se da cabida tanto las directrices estratégicas a través de las líneas de actuación como las actuaciones específicas a acometer en los siguientes tres años toda vez que las mismas están vinculadas con la ejecución del PRTR y del conjunto de programas identificados en la Agenda España Digital 2026.
Este plan se desglosará en planes anuales de actuación, que recogerán las acciones específicas, metas intermedias o valores aceptables y metas finales que, encuadradas dentro de las líneas de actuación del PEP, permitan avanzar hacia la consecución de los objetivos identificados.
A la finalización del plan, en 2025, INCIBE habrá contribuido a la hoja de ruta para la transformación digital de España, aprovechando las nuevas tecnologías para incrementar las capacidades de ciberseguridad en nuestro país, fomentar el desarrollo del ecosistema empresarial en ciberseguridad y potenciar el liderazgo internacional de España.

2. LA MISIÓN, VISIÓN Y VALORES DE INCIBE

2.1. Misión

La misión de INCIBE es, en consonancia con lo establecido por su Consejo de Administración de acuerdo a la estrategia y el mandato del Gobierno de España y la legislación vigente, ser un motor para la transformación digital de la sociedad, protegiendo a la ciudadanía, menores y empresas privadas en España y fomentando la industria de la ciberseguridad, impulsando la I+D+i e identificando, generando, atrayendo y desarrollando el talento.

2.2. Visión

La visión de INCIBE es:

- Que el nivel de ciberseguridad de ciudadanos y empresas se sitúe entre los cinco mejores del mundo.
- Que la innovación y oferta de productos, servicios y profesionales relacionados con la ciberseguridad en España esté considerado entre los cinco mejores del mundo.
- Posicionar a INCIBE como referente europeo en el ámbito de ciberseguridad.

2.3. Valores

Los valores de INCIBE constituyen el marco de comportamiento, más allá de la ética y responsabilidad social exigible a cualquier organización, que el Consejo de Administración fija para INCIBE y todo su personal.

Estos valores han de servir a la entidad como principios rectores del diseño, desarrollo, ejecución del PEP y son:

- Vocación de servicio público, eficaz y eficiencia, al servicio del conjunto de la ciudadanía, del tejido empresarial e industrial español y del Gobierno de España.
- Espíritu neutral y colaborativo, con todos los agentes públicos y privados, nacionales e internacionales, que promueven, conforman o demandan la ciberseguridad en España.
- Proactividad y flexibilidad, para dar una respuesta ágil, eficaz, eficiente y adaptada a los restos y cambios que demanda la ciberseguridad.
- Excelencia, como pilar fundamental en el diseño y desarrollo de nuestra actividad.
- Innovación para estar a la vanguardia de la seguridad digital, potenciando la industria de la ciberseguridad.
- Desempeño responsable y transparente, haciendo uso sostenible e inteligente de los recursos.
- Colaboración nacional e internacional, que responda a las necesidades de una realidad transversal y transnacional como es la ciberseguridad.

3. FUNDAMENTOS ESTRATÉGICOS

La ejecución del PRTR y de la agenda España Digital 2026 y la publicación de la Directiva 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, hacen recomendable actualizar la presente estrategia para recoger la actividad prevista en ambos documentos estratégicos.

El hecho de que la transformación digital sea una prioridad estratégica clave en la Unión Europea, hace que la sociedad en su conjunta tenga inevitablemente una mayor exposición a las ciberamenzas. Es por ello, que la ciberseguridad debe estar integrada en la digitalización y por ende la misma debe imperar en las actuaciones que entidades como INCIBE desarrolle para cada uno de sus públicos objetivos.

Es precisamente esta transformación la que impulsó en primera instancia la agenda España Digital y posteriormente el PRTR, como vectores de modernización y prosperidad a medio plazo, actuando en la triple dimensión de (i) infraestructuras y tecnología; (ii) economía y (iii) personas.

Fruto del desarrollo del conjunto de objetivos, medidas y actuaciones desarrolladas, en el anterior plan estratégico de INCIBE se comenzaron a diseñar y a lanzar los siguientes programas vinculados con los objetivos del PRTR (fortalecer las capacidades de ciberseguridad de ciudadanos y empresas, impulsar la industria, I+D+i y talento en ciberseguridad y poner en marcha el nodo nacional de la red europea de centros de competencia industrial tecnológica y de investigación en ciberseguridad) como son los programa CONFIA, Ciberinnova, INCIBE emprende y Talento Hacker.

En este PEP existe por consiguiente la voluntad de planificar, ejecutar y evaluar el desarrollo de estos programas conforme a las directrices establecidas y, tomando en consideración los compromisos de INCIBE conforme a los mandatos del gobierno de España.

Este PEP se actualizará si fuese necesario en base a los cambios normativos que pudieran devenir de la negociación y transposición de las diferentes normativas vinculadas con la actividad de INCIBE y/o con el componente de ciberseguridad.

4. OBJETIVOS ESTRATÉGICOS Y LÍNEAS DE ACTUACIÓN

Las metas previstas para que INCIBE pueda desarrollar su misión y pueda acercarse a su visión son los objetivos estratégicos. En el presente PEP dichos objetivos se han procedido a establecer conforme a las medidas y los ejes establecidos para INCIBE en agenda España Digital 2026 y en el PRTR. En base a dichos criterios, los objetivos establecidos son:

- **Objetivo 1**. Fortalecimiento de la ciberseguridad de la ciudadanía, pymes y profesionales.
- **Objetivo 2**. Estímulo del ecosistema empresarial del sector de la ciberseguridad.
- **Objetivo 3**. Impulso de España como nodo internacional en el ámbito de la ciberseguridad.

Para la consecución de estos objetivos y de los retos que INCIBE se ha planteado se han procedido a identificar nueve líneas de actuación, tres por objetivo, que se desgranan en dieciocho medidas operativas, dos para cada una de las líneas de actuación.

4.1. Objetivo 1. Fortalecimiento de la ciberseguridad de la ciudadanía, pymes y profesionales

Para fortalecer las capacidades en ciberseguridad y la confianza digital de la ciudadanía, menores, empresas y profesionales, se hace necesario implementar una cultura de ciberseguridad. Para ello, es recomendable invertir en la concienciación de los riesgos asociados a la digitalización y la modernización del tejido empresarial, así como en la formación en competencias digitales de ciberseguridad.

INCIBE siendo consciente del impacto que estas actuaciones tienen entre la ciudadanía y el mundo empresarial lleva años ejecutando actividades y mecanismos focalizados a impulsar sus capacidades y la confianza digital.

En la ejecución de este objetivo se dará continuidad a estas acciones de información, concienciación y formación en este campo, ampliando y reforzando sus capacidades que puedan necesitar en función de los conocimientos de los que dispongan para dotarles de ayuda, soporte y respuesta a los riesgos, amenazas e incidentes.

Todas estas actuaciones se seguirán desarrollando a través de los canales que la entidad tiene para los distintos públicos en el marco del programa CONFIA en torno a cuatro ejes:

- Acciones de concienciación y comunicación, tales como contenidos específicos adaptados a las necesidades de la ciudadanía, menores y empresas; eventos y acciones de proximidad en Comunidades Autónomas que aumenten la capilaridad de las actividades, que incorporen dinámicas y recursos interactivos y gamificados.
- Capacitación en ciberseguridad mediante el desarrollo de programas formativos y recursos específicos para la adquisición de las competencias digitales en la ciberseguridad.
- Cooperación y coordinación con acuerdos bilaterales y multilaterales para la consolidación de una cultura de ciberseguridad o la gestión de incidentes y el desarrollo de una red de actores relevantes con los que se puedan realizar actividades o con los que INCIBE desarrolle la responsabilidad social empresarial.

- Herramientas y soluciones de ciberseguridad, con el desarrollo y fomento de soluciones tecnológicas específicas y con mecanismos que permitan acercar la digitalización a las necesidades actuales de la sociedad.

Como complemento de estas iniciativas y en consonancia con el PRTR, en concreto con los CID 246 y 247, en este objetivo se plantea la realización de recursos para sus públicos objetivos y la capacidad de gestionar 20.000 llamadas en la Línea de Ayuda de Ciberseguridad 017.

Con esa perspectiva el presente objetivo persigue llevar a cabo actuaciones focalizadas en las siguientes líneas de actuación.

4.1.1. Línea de Actuación 1.1: Promoción de la concienciación y la información

Las actividades pertenecientes a esta línea de actuación buscarán concienciar a ciudadanos, menores, empresas y profesionales no sólo de los riesgos a los que pueden estar expuestos, sino de la necesidad de tomar conciencia de las acciones que pueden realizar por si mismo o a través de los recursos que pone a disposición INCIBE para conocer sus riesgos y protegerse.

INCIBE puede y debe colaborar con ellos mediante la puesta a su disposición de información, alertas tempranas, consejos y herramientas para ayudarles, así como en el establecimiento y/o fomento de los ecosistemas y canales apropiados para la cooperación y defensa conjunta ante amenazas comunes, con el objetivo, entre otros, de mejorar las capacidades digitales. Esta Línea se desarrollará a través de dos medidas estratégicas.

MEDIDA 1. Fortalecimiento de las capacidades de ciberseguridad de la ciudadanía y menores

Orientada al desarrollo de acciones focalizadas para favorecer y capacitar a estos colectivos permitiéndoles incrementar el uso seguro de las tecnologías y redes de comunicación.

MEDIDA 2. Fortalecimiento de las capacidades de ciberseguridad de los profesionales

Encaminada a la realización de actuaciones que permitan al tejido industrial y a los profesionales adoptar nuevos procesos vinculados con la ciberseguridad a fin de estar mejor capacitados para aumentar la productividad, la competitividad y su rentabilidad futura.

4.1.2. Línea de Actuación 1.2: Capacidades para la ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes

El marco de actuación de esta línea está enfocado en la prestación del servicio público que nuestra entidad presta a la sociedad mediante el refuerzo de capacidades de soporte y respuesta a incidentes, la Línea de Ayuda en Ciberseguridad, la vigilancia, alerta temprana y prospectiva, las capacidades de resiliencia y recuperación de los operadores de servicios críticos y proveedores de sectores estratégicos y, las mejoras de las capacidades tecnológicas de la propia entidad para mejorar la prestación del servicio.

Esta Línea se desarrollará a través de dos medidas estratégicas.

MEDIDA 3. Fortalecimiento de las capacidades de soporte y respuesta a incidentes

A través de esta medida evolucionarán y aumentarán las propias capacidades de ayuda, soporte y respuesta, coordinando los servicios de la Línea de Ayuda en Ciberseguridad 017, los sistemas de vigilancia, alerta temprana y prospectiva y los servicios de respuesta a incidentes de INCIBE.

MEDIDA 4. Fortalecimiento de las capacidades de resiliencia y recuperación de los operadores de servicios críticos y proveedores de sectores estratégicos

La ejecución de esta medida está enfocada al desarrollo por un lado de nuevas iniciativas internas para mejorar la prestación de servicios y por otro, de iniciativas identificadas y/o demandadas por los operadores y proveedores de los siguientes sectores estratégicos:

- Agua, energía, industria nuclear e industria química.
- Transporte y espacio.
- Financiero y tecnologías de la información y la comunicación (TIC).
- Salud, alimentario e investigación.
- Proveedores de servicios digitales (PSD).
- Cadena de suministro.
- Pymes y despachos profesionales.
- Turismo y ocio.

4.1.3. Línea de Actuación 1.3: Impulso de la colaboración público-privada y público-públicos y de la RSE

Intensificar la colaboración bilateral y/ multilateral es el objetivo de esta línea de actuación. Las necesidades globales en materia de ciberseguridad y, la forma de enfocar la colaboración hace necesario priorizar nuevamente la experiencia de INCIBE en esta materia. Los logros que se puedan conseguir alineados con la visión de la entidad dependen precisamente del impulso que se persigue con esta línea de actuación.

Esta Línea se desarrollará a través de dos medidas estratégicas.

MEDIDA 5. Consolidación del programa de trabajo de ciberseguridad nacional

En el marco de ejecución de este Plan Estratégico Plurianual se pretende consolidar la actividad desarrollada en este componente esencial de ciberseguridad en España conforme a lo establecido en la Estrategia Nacional de Ciberseguridad de 2019.

Este órgano impulsado por el Consejo de Seguridad Nacional es el mayor espacio de colaboración público-privado al aglutinar la mayor representatividad de organismos públicos y privados y de la sociedad en el ámbito de la ciberseguridad. INCIBE, en su rol de vicepresidente primero pretende con el desarrollo de esta medida impulsar el trabajo especialmente del grupo de trabajo de impulso a la industria y a la I+D+i en colaboración con la Cámara de España y seguir colaborando activamente en el resto de los grupos de los que forma parte a fin de contribuir a la identificación de las necesidades de la industria y de los centros de investigación en lo que se refiere a ciberseguridad.

MEDIDA 6. Desarrollo de la Responsabilidad Social Empresarial de INCIBE

Con esta medida se pretende impulsar las actuaciones de RSE ejecutadas hasta el momento y focalizadas en el programa de inserción al mundo empresarial a través de la realización de becas en materia de ciberseguridad.

4.2. Objetivo 2. Impulso del ecosistema empresarial del sector de la ciberseguridad

Este objetivo responde a la necesidad de contribuir a la soberanía digital europea tomando como eje principal la generación de riqueza, empleo e impulso de las empresas del sector de la ciberseguridad en España.

El constante crecimiento de esta industria acontecido en los últimos años ha permitido llegar a una situación clave para la generación de riqueza y empleo. Este objetivo por consiguiente pretende seguir estimulando la creación y el fortalecimiento empresarial mediante el impulso y afianzamiento de la industria, el fomento de la I+D+i y la identificación y desarrollo de talento para hacer frente a la demanda no cubierta de profesionales en este sector.

Este conjunto de actuaciones se desarrollará a través de tres programas:

- INCIBE Emprende, que desarrollará iniciativas de ideación, incubación y aceleración para la creación de nuevas start-ups en el sector y la consolidación y el crecimiento de las ya existentes. Focalizado en esta actividad en el marco de ejecución de este plan estratégico plurianual se pretende dotar de capilaridad a través y en colaboración con las entidades que en esta materia trabajan en el conjunto de las comunidades y ciudades autónomas.
- CIBERINNOVA, que impulsará las capacidades de la industria nacional y la competitividad de sus soluciones a través de diferentes iniciativas vinculadas a la innovación como la ejecutada a través de la Iniciativa Estratégica de Compra Pública Innovadora (IECPI).
- Talento Hacker, buscando identificar, transformar y desarrollar el talento.

Este objetivo se llevará a cabo a través de las siguientes líneas de actuación:

4.2.1. Línea de Actuación 2.1: Impulso y fortalecimiento de la industria de ciberseguridad

La industria de ciberseguridad en España es una oportunidad de generación de riqueza, empleo y desarrollo de las capacidades en un sector de enorme crecimiento. El objetivo que se persigue con esta línea de actuación es por consiguiente tanto la promoción de las iniciativas existentes hasta la fecha como la internacionalización de la misma en las diferentes fases del proceso:

- Acompañamiento y apoyo a las empresas españolas en los primeros pasos para iniciar su proceso de internacionalización a través de acciones de exploración, prospección y análisis de mercados internacionales.
- Captación e impulso a la visibilidad de las empresas españolas en los mercados internacionales objetivo para promover su presencia y la ampliación de su cartera de negocio en el exterior.
- Fomento de la implantación e inmersión en mercados internacionales para aquellas empresas que ya operan en mercados extranjeros.

Esta Línea se desarrollará a través de dos medidas estratégicas.

MEDIDA 7. Promoción de iniciativas emprendedoras de ciberseguridad

A través de esta medida estratégica se desarrollará un programa para el desarrollo de actuaciones de captación de ideas de negocio, incubación y aceleración de proyectos de emprendimiento utilizando para ello una invitación pública que persigue establecer las bases para la selección de entidades colaboradoras que puedan desarrollar actividades especializadas en la promoción de iniciativas emprendedoras en ciberseguridad, con la finalidad de incorporar emprendedores a la economía y sociedad digitales españolas.

Asimismo, en consonancia con esta invitación se pretende desarrollar un segundo programa buscando, por un lado, fomentar y apoyar el desarrollo de soluciones innovadoras en ciberseguridad tan necesarias en un entorno digital cambiando, así como la necesidad de que los emprendedores del resto de sectores de base tecnológica, incorporen la ciberseguridad en sus proyectos desde sus inicios. Impulsando la captación previa de nuevas ideas y/o proyectos especialmente en las provincias y regiones menos desarrolladas empresarialmente en el sector de la ciberseguridad. Y por el otro, impulsar y acelerar start-ups españolas a lo largo de todo el territorio nacional a través del apoyo de entidades colaboradoras, tanto públicas como privadas, que habiendo acudido a la invitación pública antes descrita suscriban convenios con INCIBE.

MEDIDA 8. Internacionalización de la industria de ciberseguridad

En consonancia con línea de actuación estratégica esta medida persigue desarrollar un programa de ayudas para la asistencia a eventos y misiones comerciales internacionales a fin de organizar e impulsar la participación española mediante la organización, coordinación y liderazgo de la delegación española asistentes en cada uno de ellos. Para llevar a cabo esta actividad INCIBE ha identificado un total de veintidós países prioritarios para la industria española en ciberseguridad, en base al tamaño de sus mercados y perspectivas de crecimiento (Reino Unido, Italia, Alemania, Francia, Países Bajos, Bélgica, Suecia, Suiza, Portugal, EE.UU. México, Canadá, Brasil, Colombia, Chile, República Dominicana, Singapur, Australia, India, Corea del Sur, Japón y Taiwán).

Asimismo, se trabajará colaborativamente con el Instituto de Comercio Exterior (ICEX) para mejorar la competitividad de la industria española de la ciberseguridad, tanto mediante la creación de un entorno adecuado que propicie el surgimiento y desarrollo de nuevas empresas del sector, como mediante la aceleración de empresas emergentes ya existentes, y apoyando la expansión internacional del conjunto del sector.

4.2.2. Línea de Actuación 2.2: Fomento de la I+D+i en ciberseguridad

Los instrumentos establecidos por INCIBE para canalizar esta línea de actuación el fortalecimiento, impulso y transformación de la I+D+i en ciberseguridad son (i) la compra pública de innovación, como instrumento esencial de las políticas públicas para impulsar la innovación y la competitividad desde los poderes públicos empleando la demanda pública de productos, servicios y suministros como instrumentos mediante el que ejecutar los mandatos de las entidades compradoras; (ii) el programa para el impulso de certificaciones

en ciberseguridad que permita capacitar a las empresas permitiéndolas adquirir una madurez a la hora de participar en procesos de contratación pública; (iii y iv) la invitación pública para la colaboración en la promoción de cátedras y de proyectos estratégicos de ciberseguridad en España respectivamente.

Esta Línea se desarrollará a través de dos medidas estratégicas.

MEDIDA 9. Transformación de la I+D+i en activos de alto valor añadido

En la búsqueda de herramientas e instrumentos que permitan impulsar la innovación y la competitividad como motor de transformación social y oportunidad para la innovación, INCIBE lleva desde 2021 ejecutando la Iniciativa Estratégica de Compra Pública Innovadora primero con una consulta preliminar al mercado y posteriormente con el documento regulador de la contratación de servicios de investigación y desarrollo en materia de ciberseguridad focalizado en programas de I+D con empresas de la industria y posteriormente con la compra pública precomercial enfocada a soluciones tecnológicas para la ciberseguridad en las pymes, para sectores estratégicos, a retos del sector público, para la mejora de las infraestructuras y los equipamiento propios de INCIBE y para pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores. En el marco de este plan estratégico plurianual se pretende realizar una nueva consulta preliminar y, llevar a cabo la firma de los contratos identificados durante la ejecución de la IECPI.

Asimismo, está previsto la publicación de un programa para el impulso de certificaciones en ciberseguridad para los procesos de implantación y certificación de normas enfocado a pymes de base tecnológica que quieran ser o sean proveedoras de las administraciones públicas.

MEDIDA 10. Desarrollo de programas de I+D+i y fortalecimiento de las capacidades en ciberseguridad por universidades

Persiguiendo la elevación de las capacidades y recursos en ciberseguridad, en los ecosistemas académico, empresarial y tecnológico, dirigidos a impulsar las capacidades en ciberseguridad de la sociedad y la economía en general, se pretende en el marco de ejecución de este plan el desarrollo de al menos dos programas que permitan la promoción y generación del conocimiento y la transferencia del mismo al sector productivo, especialmente estableciendo sinergias entre los ámbitos sociales y económicos de la ciberseguridad. Para desarrollar este propósito se ejecutará las invitaciones públicas para la promoción de cátedras y proyectos en ciberseguridad promovidos por universidades públicas o consorcios integrados por universidades públicas y privadas en los cuales una universidad pública ejerza el rol de coordinación y administración del consorcio. En este sentido la diferencia entre ambas reside en que:

- Las cátedras son un instrumento de formación donde universidad y empresas trabajan mano a mano para transferir conocimiento y experiencia especializada a los estudiantes, las empresas y el entorno social y económico. Representando una modalidad de colaboración entre la institución académica y el ámbito productivo, considerándose instrumentos idóneos para la generación, transmisión y difusión de conocimiento y capacidades especializadas en ciberseguridad.
- Los proyectos son una forma de aportar de aportar soluciones concretar a algunos de los mayores desafíos científicos y tecnológicos de nuestra sociedad y economía.

Están destinados a impulsar la aplicación de los resultados de la investigación y la innovación, combinando nuevas formas de gobernanza y colaboración, así como involucrando a la ciudadanía y al tejido productivo y social.

4.2.3. Línea de Actuación 2.3: Promoción del talento en ciberseguridad

La carencia de profesionales es un lastre para la sociedad y la industria de ciberseguridad. De ahí que resulte necesario la identificación y el desarrollo tanto de actuaciones formativas especializadas en ciberseguridad para desarrollar las capacidades tanto de ciudadanos como empresas. Asimismo, en la ejecución de esta línea de actuación se prevé favorecer la integración del personal de colectivos vulnerables e infrarrepresentados permitiéndoles una mayor integración laboral en el sector.

Esta Línea se desarrollará a través de dos medidas estratégicas.

MEDIDA 11. Fomento, detección y aprovechamiento del talento en ciberseguridad

Dentro de sus estrategias de concienciación de ciberseguridad y de dotar al sector de más profesionales, INCIBE realiza acciones dirigidas a personas de todos los sectores, incluyendo las personas con discapacidad o aquellas en riesgo de exclusión social. La preocupación por los grupos vulnerables en estos temas es un objetivo esencial de nuestra entidad, por lo que impulsa actuaciones integrales que traten de conseguir un aumento de la prevención -en particular, de ciberacoso contra personas con algún tipo de discapacidad- y la efectiva proyección de situaciones de riesgo.

Por este motivo, y con el foco en la capacitación en esta medida está previsto tanto el desarrollo de cursos de formación especializada en ciberseguridad, como la ejecución de invitaciones públicas para el desarrollo de actuaciones formativas especializadas a nivel técnico para personas con discapacidad o para colectivos infrarrepresentados y vulnerables.

De esta forma, INCIBE durante la vigencia de este plan llevará a cabo en consonancia con las mencionadas invitaciones, la identificación, planificación y desarrollo de recursos, contenidos y actividades orientadas a la promoción, identificación y promoción laboral en esta materia.

MEDIDA 12. Identificación e impulso de acciones formativas para favorecer la integración

El foco de esta medida se prevé desarrollar a través de la contratación pública de personas desempleadas y/o la reconversión profesional de personas para el sector de la ciberseguridad favoreciendo la integración de las mismas en este sector ante la necesidad de profesionales en este ámbito.

4.3. Objetivo 3. Estímulo de España como nodo internacional en el ámbito de la ciberseguridad

El ecosistema empresarial identificado en el anterior objetivo es clave para el posicionamiento en línea con la visión de INCIBE. Con este objetivo se persigue contribuir a la soberanía digital en este campo respondiendo a la Estrategia de Ciberseguridad de la Unión Europea para la Década Digital. Este itinerario persigue garantizar que la Unión

Europea alcance sus objetivos y metas de transformación digital de nuestra sociedad y economía en consonancia con los valores de la UE, que refuerce nuestro liderazgo digital y promueva políticas centradas en el ser humano, inclusivas y sostenibles que capaciten a los ciudadanos y las empresas.

Para avanzar en este compromiso y estar alineado con la estrategia de España en el ámbito europeo e internacional es clave las actuaciones que desarrollará el Centro Nacional de Competencias en Ciberseguridad de INCIBE (NCC-ES INCIBE), centro espejo del Centro Europeo de Competencias (ECCC) en el marco trianual de ejecución de este plan.

En el ámbito de este centro se llevarán a cabo las siguientes actuaciones:

- Potenciación de las capacidades y los resultados de investigación en la materia evitando la fragmentación.
- Promoción y fomento de la ejecución de proyectos con financiación en cascada de Europa para el desarrollo de capacidades comunes a nivel europeo.
- Creación de una comunidad de competencia en ciberseguridad que defina prioridades tecnológicas y aglutine experiencias existentes.
- Impulso a acciones de soporte y estudios como centro de coordinación nacional.

Con esa perspectiva el presente objetivo persigue llevar a cabo actuaciones focalizadas en las siguientes líneas de actuación.

4.3.1. Línea de Actuación 3.1: Consolidación del programa de trabajo de ciberseguridad europeo

La experiencia de INCIBE en el sector de la ciberseguridad y los conocimientos especializados en materia tecnológica, de investigación e innovación han contribuido a que INCIBE sea una entidad de referencia para el desarrollo nacional de la industria de ciberseguridad. Con esta experiencia y tras haber sido designado como Centro de Coordinación Nacional se pretende cooperar con el resto de agentes competentes, la industria, el sector público, la comunidad académica y de investigación y la ciudadanía permitiendo capitalizar a través de la puesta en marcha de proyectos transfronterizos acciones conjuntas con la UE. De esta forma, se pretende prestar apoyo técnico y económico, es especial a las pymes, facilitando el acceso a conocimientos, conectando mercados potenciales y facilitando el acceso a fuentes de financiación al tejido productivo nacional.

Esta Línea se desarrollará a través de dos medidas estratégicas.

MEDIDA 13. Apoyo técnico y económico a las empresas españolas

Para ello, esta medida pretende proporcionar conocimiento especializado teniendo en cuenta los retos específicos en ciberseguridad a nivel nacional y regional. Asimismo, pretende impulsar la organización y realización de al menos tres cumbres europeas ayudando a la promoción y difusión de los resultados de la labor de la colaboración de los distintos agentes y proporcionar conocimiento especializados teniendo en cuenta los retos específicos en ciberseguridad, a nivel nacional y regional.

MEDIDA 14. Alineamiento con el marco regulatorio y legislativo europeo

La consolidación del programa de trabajo nacional tendrá también su foco en el programa europeo normativo y legislativo para ello, se llevara a cabo acciones para

facilitar el alineamiento y la implementación de los cambios normativos necesarios para reforzar INCIBE como centro de referencia en ciberseguridad en Europa.

4.3.2. Línea de Actuación 3.2: Desarrollo del nodo de ciberseguridad nacional y autonómico

INCIBE en el marco del actual plan estratégico es consciente que la transformación digital es una política de Estado que permea a todo el territorio, a todos los sectores económicos y a todas las dimensiones sociales. Para conseguir que esta transformación sea una realidad y por consiguiente impulsar la digitalización, se pretende ejecutar en el marco de las Redes Territoriales de Especialización Tecnológica (RETECH) una iniciativa enfocada a la ciberseguridad.

Esta iniciativa poniendo el foco en un modelo de colaboración entre la entidad y las comunidades autónomas, pretende impulsar proyectos de carácter transregional orientados a la especialización regional, y con claros efectos multiplicadores en los impactos a fin de generar o potenciar iniciativas de carácter disruptivo basadas en distintas visiones, experiencias y conocimiento adquirido por las administraciones regionales, movilizando para ello sus propias redes territoriales de conocimiento y colaboración.

Esta Línea se desarrollará a través de dos medidas estratégicas.

MEDIDA 15. Impulso y asesoramiento a la innovación en ciberseguridad

La medida se enfocará al desarrollo de actuaciones para apoyar la creación de ecosistemas para la ciberseguridad favoreciendo el impulso de efectos tractores focalizados en la ciberseguridad hacia nuevos modelos de desarrollo sostenibles e integradores. De ahí que se pretenda impulsar un modelo de centros demostradores o test centers que deslocalizarán la actividad y a su vez, impulsarán una red de laboratorios que estarán acreditados para certificar la ciberseguridad de productos, soluciones y servicios innovadores.

MEDIDA 16. Puesta en marcha de proyectos territoriales de transformación digital

La ejecución de RETECH ciberseguridad en el marco de esta medida pretende constituirse como una iniciativa que tiene por objetivo el desarrollo del ecosistema de en sectores estratégicos. Para ello, pretende establecer un modelo de colaboración entre INCIBE y las comunidades autónomas para el desarrollo de proyectos en la materia enfocados especialmente a los siguientes sectores productivos estratégicos de las siguientes comunidades autónomas.

- Andalucía: salud y Smart cities.
- Cantabria: industria; economía azul; agroalimentario; salud; cultura y turismo.
- Castilla y León: movilidad inteligente e industria aeroespacial.
- Castilla-La Mancha: empresas TIC.
- Cataluña: salud.
- Comunitat Valenciana: industria conectada.
- Extremadura: entorno rural; pymes y autónomos; ciudadanía.
- Galicia: movilidad inteligente (Smart Mobility).
- Islas Baleares: turismo.
- Islas Canarias: pymes y autónomos; turismo; construcción.
- Madrid: salud.

- Murcia: agroalimentario.
- Navarra: pymes y ciudadanía; movilidad eléctrica y conectada; alimentación y energía verde.
- País Vasco: industria inteligente y energía.
- Principado de Asturias: empresas de defensa, Industria 4.0, sector agroalimentario.

4.3.3. Línea de Actuación 3.3: Identificación e implantación de actuaciones y controles para reducir la exposición al riesgo

La ejecución del PRTR es una responsabilidad para INCIBE. Prueba de ello es que ha configurado este plan tomando en consideración los ejes y objetivos previstos en el mismo. En esta actuación se pretende identificar e implantar acciones y controles que minimicen la exposición al riesgo permitiendo una correcta ejecución de los compromisos asumidos.

Para conseguir dicho propósito se ha procedido a planificar un conjunto de actividades que ponen el foco en el modelo de gobernanza y control del PRTR, así como en los instrumentos jurídicos necesarios para poder ejecutar el resto de actuaciones, convenios y contratos necesarios para su cumplimiento al amparo de la siguiente normativa:

- Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.
- Orden HFP/1031/2021, de 29 de septiembre, por la que se establece el procedimiento y formato de la información a proporcionar por las Entidades del Sector Público Estatal, Autonómico y Local para el seguimiento del cumplimiento de hitos y objetivos y de ejecución presupuestaria y contable de las medidas de los componentes del Plan de Recuperación, Transformación y Resiliencia.
- Orden HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia.
- Disposiciones Operativas del Plan de Recuperación acordadas por el Gobierno de España y la Comisión Europea.

Esta Línea se desarrollará a través de dos medidas estratégicas.

MEDIDA 17. Identificación y desarrollo de instrumentos jurídicos

INCIBE consciente de su responsabilidad desarrollará un modelo de gobernanza cuya primera medida sea la puesta en marcha de unidades u oficinas de supervisión y, adoptará un manual de funciones y procedimientos de gestión, seguimiento y control del Mecanismo de Recuperación y Resiliencia en el que se recogen los aspectos esenciales para el cumplimiento de la normativa y del PRTR en su conjunto.

MEDIDA 18. Identificación y desarrollo de actuaciones de seguimiento de ejecución del PRTR

Con la ejecución de esta medida se persigue desarrollar acciones que faciliten el seguimiento a fin de dar visibilidad a la actividad y el compromiso de ejecución del PRTR en INCIBE.

5. RESUMEN DE MEDIDAS

OBJETIVO ESTRATÉGICO		MEDIDA
1	Fortalecimiento de la ciberseguridad de la ciudadanía, pymes y profesionales	1. Fortalecimiento de las capacidades de ciberseguridad de la ciudadanía y menores 2. Fortalecimiento de las capacidades de ciberseguridad de los profesionales 3. Fortalecimiento de las capacidades de soporte y respuesta a incidentes 4. Fortalecimiento de las capacidades de resiliencia y recuperación de los operadores de servicios críticos y proveedores de sectores estratégicos 5. Consolidación del programa de trabajo de ciberseguridad nacional 6. Desarrollo de la Responsabilidad Social Empresarial de INCIBE
2	Impulso del ecosistema empresarial del sector de la ciberseguridad	7. Promoción de iniciativas emprendedoras de ciberseguridad 8. Internacionalización de la industria de ciberseguridad 9. Transformación de la I+D+i en activos de alto valor añadido 10. Desarrollo de programas de I+D+i y fortalecimiento de las capacidades en ciberseguridad por universidades 11. Fomento, detección y aprovechamiento del talento en ciberseguridad 12. Identificación e impulso de acciones formativas para favorecer la integración
3	Estímulo de España como nodo internacional en el ámbito de la ciberseguridad	13. Apoyo técnico y económico a las empresas españolas 14. Alineamiento con el marco regulatorio y legislativo europeo 15. Impulso y asesoramiento a la innovación en ciberseguridad 16. Puesta en marcha de proyectos territoriales de transformación digital 17. Identificación y desarrollo de instrumentos jurídicos 18. Identificación y desarrollo de actuaciones de seguimiento de ejecución del PRTR

6. METAS DEL PLAN ESTRATÉGICO

LÍNEA DE ACTUACIÓN	META 2025
1.1 Promoción de la concienciación y la información	**Desarrollo de 300 acciones** desarrolladas para incrementar la concienciación
1.2 Capacidades para la ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes	**Desarrollo de 50 actuaciones** para el fortalecimiento de las capacidades de soporte y respuesta a incidentes
1.3 Impulso de la colaboración público-privada y público-públicos y de la RSE	Desarrollo de **60 acciones público privadas de colaboración** y/o para el desarrollo de la RSE
2.1 Impulso y fortalecimiento de la industria de ciberseguridad	Desarrollo de **50 actuaciones que impulsen la visibilidad** de las empresas españolas
2.2 Fomento de la I+D+i en ciberseguridad	Compromisos del **gasto del 100%**
2.3 Promoción del talento en ciberseguridad	**10.260 profesionales** formados en ciberseguridad
3.1 Consolidación del programa de trabajo de ciberseguridad europeo	Desarrollo de **25 actuaciones para la consolidación** del programa de trabajo
3.2 Desarrollo del nodo de ciberseguridad nacional y autonómico	Desarrollo de **50 actuaciones que contribuyan al desarrollo del nodo** de ciberseguridad nacional y autonómico
3.3 Identificación e implantación de actuaciones y controles para reducir la exposición al riesgo	**100% de actuaciones implantadas** para mitigar el riesgo

INSTITUTO NACIONAL DE CIBERSEGURIDAD