PLAN ESTRATÉGICO INCIBE 2021-2025

'De miles a millones'

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017

ÍNDICE

01 OBJETO Y ALCANCE DEL PRESENTE DOCUMENTO

El objeto del presente documento es recoger el Plan Estratégico de INCIBE para el periodo 2021-2025, que consolide las acciones llevadas a cabo en el plan anterior y establezca los cometidos previstos para INCIBE en los próximos años, permitiendo que los mismos puedan adaptarse a la proyección estratégica para la entidad de cara al futuro.

Bajo el lema ***'de miles a millones'*** este plan busca generar un efecto multiplicador en el resultado de las actuaciones que desarrolla INCIBE, y conseguir llegar a más ciudadanos y más empresas para que identifiquen, reconozcan y posicionen la organización como su referente de ciberseguridad en España. Igualmente, este Plan Estratégico permitirá impulsar la actividad de INCIBE para su posicionamiento como un actor destacado en el ámbito internacional y reafirmar el compromiso de España como referente europeo en el ámbito de la ciberseguridad.

El Plan Estratégico ofrece una visión de alto nivel de las metas que INCIBE deberá alcanzar en el Periodo 2021-2025: Los Objetivos Estratégicos para desarrollar su misión eficaz y eficientemente, y avanzar hacia la realización de su visión; y las Líneas de Actuación principales en las que se desarrollará la actividad de INCIBE durante el periodo cubierto. Por tanto, el alcance del presente Plan Estratégico cubre los siguientes apartados:

1. **Misión, visión y valores**
2. **Fundamentos Estratégicos y Legales**
3. **Objetivos estratégicos y líneas de actuación**

En un entorno cambiante y dinámico como el de la ciberseguridad, este plan de 5 años no define acciones específicas que podrían limitar la capacidad de reacción de INCIBE ante escenarios cambiantes, sino directrices estratégicas a través de líneas de actuación prioritarias. Además de los cambios tecnológicos, las condiciones sociales, económicas y políticas pueden influir significativamente en las actividades de INCIBE.

Este Plan prevé una revisión el tercer año para evaluarán los objetivos, líneas de actuación y medidas, así como grado de cumplimiento. Esto permitirá dar respuesta a los desafíos que se identifiquen durante los primeros 3 años y realizar los ajustes necesarios para garantizar el cumplimiento de sus metas. Del mismo modo, el plan cuenta con los medios y recursos necesarios en torno a 3 conceptos: **Personas**, con personal propio más el apoyo de asistencias técnicas; **Presupuesto**, con aportación patrimonial directa del accionista (Entidad Pública Empresarial Red.es), transferencias verticales de los Presupuestos Generales del Estado, ingresos por prestación de servicios derivados de encargos y la imputación de subvenciones derivados de proyectos europeos; y **Conocimiento**, adquirido en el ejercicio de su actividad, que se gestiona a través de sus sistemas de información y los diferentes informes, publicaciones y reportes.

Igualmente, este Plan se desglosará en **planes anuales**, que recogerán las acciones específicas y metas que, encuadradas dentro de las líneas de actuación del Plan Estratégico, permitan avanzar hacia la consecución de los objetivos.

A la finalización del plan, en 2025, INCIBE prestará servicios de alto valor para el conjunto de ecosistemas relacionados con la ciberseguridad. Dichos servicios contribuirán a afianzar la Sociedad de la Información y la Transformación Digital en España; y serán instrumentos eficaces del Gobierno de España para la consecución de sus objetivos.

02 MISIÓN, VISIÓN Y VALORES

MISIÓN

La Misión de INCIBE responde a la pregunta básica de "¿para qué existe?", y es la que le fija su Consejo de Administración de acuerdo a la estrategia general del Gobierno de España y la legislación vigente en materia de ciberseguridad.

La Misión de INCIBE es:

1. Mejorar la ciberseguridad y la confianza digital de ciudadanos, menores y empresas privadas de España.
2. Proteger y defender a los ciudadanos, menores y empresas privadas de España.
3. Potenciar la industria española de ciberseguridad.
4. Impulsar la I+D+i española en ciberseguridad.
5. Identificar, generar, atraer y desarrollar profesionales del sector de ciberseguridad.

Nuestra misión es ser un motor para la transformación digital de la sociedad, protegiendo a ciudadanos, menores y empresas privadas en España y fomentando la industria de la ciberseguridad, la I+D+i y el talento.

VISIÓN

La VISIÓN de INCIBE es:

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

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 todos sus empleados:

1. Vocación de servicio público
2. Espíritu neutral y colaborativo
3. Proactividad y flexibilidad
4. Excelencia
5. Innovación
6. Desempeño responsable y transparente
7. Colaboración nacional e internacional

03 FUNDAMENTOS ESTRATÉGICOS Y LEGALES

El crecimiento exponencial de la tecnología y la hiperconectividad ofrecen enormes oportunidades de desarrollo económico y social, y nos acercan a un mundo global e interdependiente. Al mismo tiempo, este profundo proceso de digitalización trae consigo nuevas amenazas para la seguridad. Cada desarrollo, cada avance tecnológico, ofrece esta dualidad de riesgo-oportunidad que debe ser abordado. Las amenazas cibernéticas a las que se enfrentan ciudadanos y empresas comparten al menos 3 características clave:

- Carácter evolutivo y cambiante, lo que hace imprescindible un proceso ágil, eficaz y **sostenible** de investigación y formación de las personas e instituciones encargadas de velar por la seguridad digital, y una transferencia de ese conocimiento a ciudadanos, empresas y gobiernos para mantener el ecosistema digital protegido.
- Mayor complejidad de las amenazas e incidentes cibernéticos, así como una mayor sofisticación del ciberdelito y el ciberdelincuente.
- Carácter global y transnacional de las amenazas e incidentes cibernéticos, lo que nos lleva a abordar la cuestión desde una perspectiva de colaboración y cooperación en el ámbito internacional.

Hoy estamos iniciando nuevos caminos de desarrollo tecnológico que van a requerir de nosotros un mayor esfuerzo. El desarrollo de la inteligencia artificial o el 5G parecen los más inmediatos, y también otras tecnologías habilitadoras (blockchain, computación cuántica, etc.) que tendrán un enorme impacto en los próximos años. Por todo esto, en los próximos 5 años el número de dispositivos conectados a internet se multiplicará exponencialmente, y ejecutarán de manera autónoma las decisiones necesarias para su ordinario funcionamiento. Las ventajas son innumerables, pero nunca antes el grado de exposición al riesgo será tan elevado para transportes, energía, comunicaciones, sector financiero y un largo etcétera de sectores críticos. Los desafíos a la seguridad digital de ciudadanos y empresas que plantea este escenario ya son enormes, y debemos anticipar las decisiones que nos permitan afrontarlos.

En este escenario global, el Gobierno de España presentó en julio de 2020 la agenda España Digital 2025, un cuaderno de bitácora para la transformación digital del país que permita optimizar los beneficios socioeconómicos de la digitalización, minimizando sus riesgos asociados. Esta agenda digital se desarrolla a través de 10 ejes estratégicos, siendo el cuarto de ellos la ciberseguridad. El Plan Estratégico de INCIBE se alinea conceptual y temporalmente con a esa agenda, y con los objetivos y metas que esta persigue. Al tiempo que se alinea con el cuerpo estratégico de la Seguridad Nacional que se define en apartado posterior.

Por último, la irrupción de la covid-19 ha generado un enorme impacto en términos sanitarios, económicos y sociales. Desde la perspectiva de la ciberseguridad, la covid-19 supone un desafío al provocar un ensanchamiento de la superficie de riesgo. El teletrabajo, el telestudio y un incremento del ocio digital asociado a las restricciones de movilidad de los ciudadanos han acelerado esa digitalización, y en consecuencia los riesgos asociados a la misma.

Otra consecuencia de esta pandemia ha sido una profunda caída de la economía de los países en términos de producto interior bruto y empleo. Para hacer frente a esta situación, la Unión Europea acordó en julio de 2020 medidas extraordinarias de recuperación en el marco del instrumento «Next Generation EU», un plan de 750.000 millones de euros. Este mecanismo se ha articulado en España a través de un Plan de Recuperación, Transformación y Resiliencia de la Economía española, presentado en octubre de 2020 y que movilizará cerca de 140.000 millones de euros, de los que 72.000 se ejecutarán entre 2021 y 2023, y en el que INCIBE tomará parte para desarrollar actividades que contribuyan a la recuperación económica y transformación del país.

Además de este contexto, se han considerado también los siguientes fundamentos estratégicos y legales: Estrategias definidas o de las que es participe el Gobierno de España, el cuerpo normativo aprobado o incorporado por el Parlamento nacional que influyen directamente en la misión y funciones de INCIBE, y los destinatarios a los que se orienta la actividad de INCIBE.

MARCO ESTRATÉGICO:

- La Estrategia Nacional de Ciberseguridad de 2019 (ENCS19), principal documento estratégico que guía el Plan.
- La Estrategia de Seguridad Nacional de 2017, que incorpora a INCIBE como uno de los organismos para alcanzar sus objetivos.
- La agenda España Digital 2025 del Ministerio de Asuntos Económicos y Transformación Digital.
- La Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023.

MARCO LEGAL:

- La Estrategia de Ciberseguridad de la UE El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- La Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 8/2011, de 28 de abril, de protección de las infraestructuras críticas.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes en materia de administración digital, contratación del sector público y telecomunicaciones.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- El Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas.
- La Ley Orgánica 3/2018, de 5 de diciembre, de protección de Datos Personales y Garantía de los Derechos Digitales.

DESTINATARIOS DE LOS OBJETIVOS ESTRATÉGICOS

Los Objetivos del Plan Estratégico de INCIBE se orientan a unos destinatarios específicos que se subdividen en cuatro grandes grupos:

CIUDADANOS:

- Cualquiera que emplee tecnologías y dispositivos, con especial atención en los menores por ser un colectivo muy vulnerable.

EMPRESAS:

- Operadores de Servicios Esenciales y sectores estratégicos.
- Grandes, medianas y pequeñas empresas.
- Microempresas y autónomos.
- La industria de ciberseguridad en general.

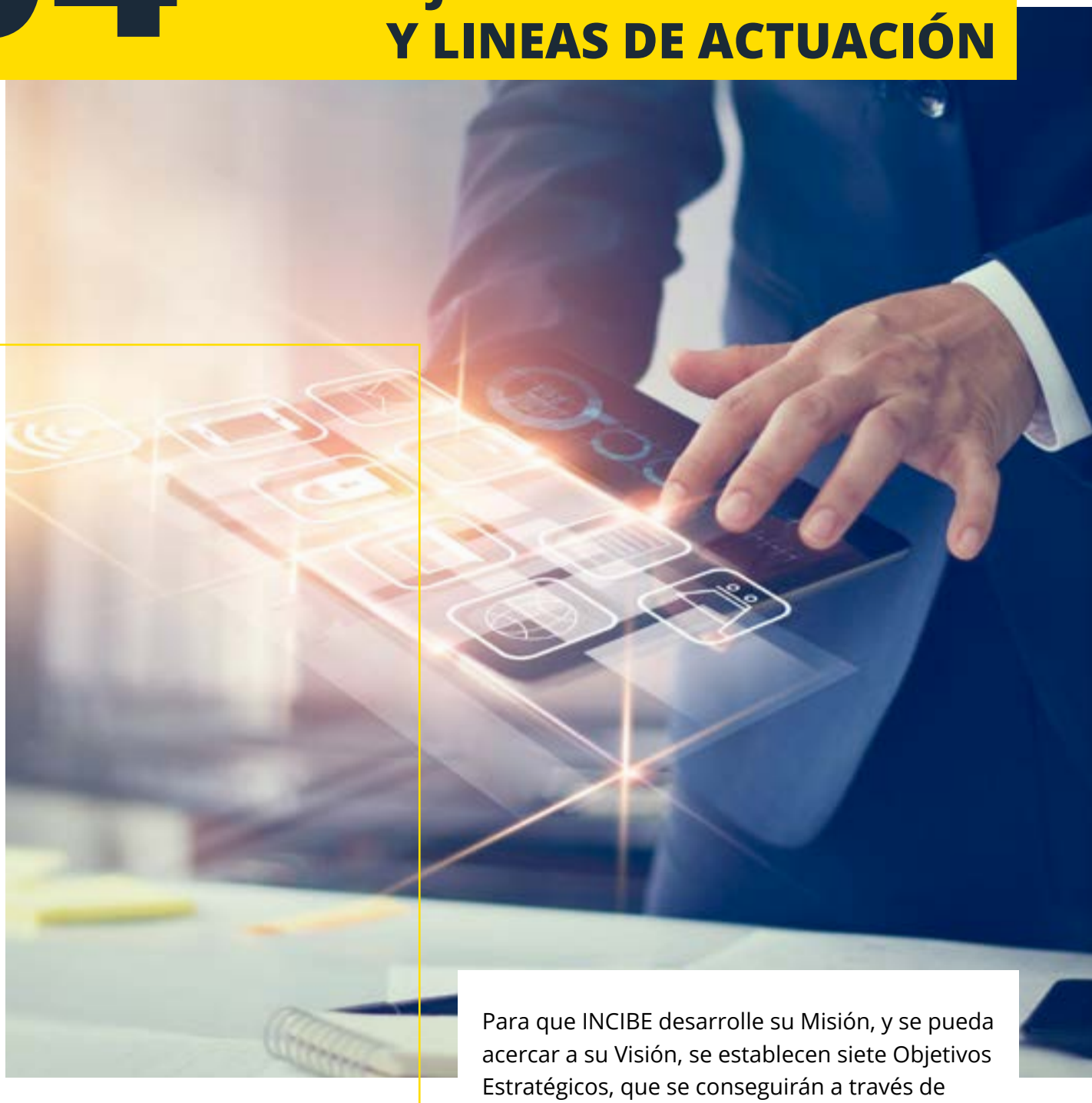
ORGANISMOS PÚBLICOS:

- Secretaría General de Administración Digital (SGAD).
- Centro Criptológico Nacional (CCN).
- Departamento de Seguridad Nacional (DSN).
- Mando Conjunto del Ciberespacio (MCCE).
- Oficina de Coordinación de Ciberseguridad.
- Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

OTROS AGENTES DE INTERÉS:

- Otros agentes públicos de ciberseguridad con los que se relaciona INCIBE.
- El entorno académico y de investigación, usuarios de la Red Académica y de Investigación RedIRIS, y tractores de la generación de nuevos productos y servicios de ciberseguridad.
- Los profesionales de la ciberseguridad, además de los expertos reconocidos.
- Los jóvenes talentos y otros colectivos, con el objetivo de promocionar el interés por la ciberseguridad y su capacitación.
- Otros agentes nacionales e internacionales de todos los sectores y ámbitos que en el desarrollo de sus actividades interactúan con el ámbito de la ciberseguridad.
- El propio INCIBE, ya que se acometerán actuaciones para la mejora de la entidad en todos los aspectos.

04 OBJETIVOS ESTRATÉGICOS Y LINEAS DE ACTUACIÓN



Para que INCIBE desarrolle su Misión, y se pueda acercar a su Visión, se establecen siete Objetivos Estratégicos, que se conseguirán a través de iniciativas estructuradas en Líneas de Actuación, que a su vez se concretan en Medidas.

01. OBJETIVO ESTRATÉGICO PROMOVER UNA CULTURA DE CIBERSEGURIDAD EN ESPAÑA

Una ciberseguridad efectiva requiere generar conciencia sobre las amenazas y riesgos existentes, desarrollando una cultura de ciberseguridad, y potenciando mecanismos de concienciación y formación. Esta cultura de ciberseguridad se refiere al conocimiento y adopción por parte de ciudadanos, empresas y administración pública, de hábitos saludables y buenas prácticas cibernéticas.

LÍNEA DE ACTUACIÓN 1.1

Promoción de la concienciación y la información

INCIBE pondrá a disposición de ciudadanos y empresas información, alertas, consejos y herramientas para ayudarles. Establecerá y fomentará los canales necesarios para la cooperación y defensa ante amenazas comunes, mejorando las capacidades digitales.

MEDIDA 1. Fortalecimiento de las capacidades de ciberseguridad de la sociedad.

MEDIDA 2. Fortalecimiento de capacidades de ciberseguridad de empresas.

MEDIDA 3. Incremento de capacidades de ciberseguridad de "actores intermedios".

MEDIDA 4. Fortalecimiento de servicios públicos, canales y herramientas para la extensión de la cultura de ciberseguridad.

LÍNEA DE ACTUACIÓN 1.2

Impulso de la colaboración público-privada y de la RSC

INCIBE realizará acciones para impulsar la colaboración público-privada, extendiendo la cultura de ciberseguridad, y los servicios de valor añadido. Destacan las actividades que se realicen en el marco del Foro Nacional de Ciberseguridad, uno de los 6 componentes de la Estrategia Nacional de Ciberseguridad de 2019.

MEDIDA 5. Desarrollo del Foro Nacional de Ciberseguridad (contribución).

MEDIDA 6. Identificación y Desarrollo de "mecanismos de multiplicación" de los esfuerzos de fortalecimiento.

MEDIDA 7. Desarrollo de la Responsabilidad Social Empresarial de INCIBE.

LÍNEA DE ACTUACIÓN 1.3

Impulso de la Generación de Conocimiento sobre CS

INCIBE generará conocimiento del sector. A través de la investigación de realidades concretas, se obtendrá una visión más amplia los mecanismos de información y alerta que desarrolla INCIBE. Esto permitirá entender tendencias a largo plazo, y establecerá mapas de conocimiento de alto valor sobre ciberseguridad a nivel nacional e internacional.

MEDIDA 8. Desarrollo del conocimiento de la ciberseguridad en España.

02. OBJETIVO ESTRATÉGICO AUMENTAR Y FORTALECER LAS CAPACIDADES PARA DETECTAR LAS CIBERAMENAZAS

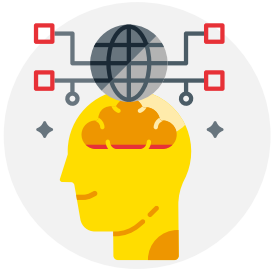
La detección de vectores de ataque de manera proactiva permitirá una alerta temprana adecuada. INCIBE debe conocer las ciberamenazas, entender cómo actúan, y detectar potenciales víctimas para protegerlas, mitigando daño que las ciberamenazas puedan causar. Este objetivo pretende que INCIBE fortalezca sus capacidades para obtener y generar lo que se conoce como *Inteligencia de Ciberamenazas,* y que explote esta inteligencia de manera eficaz.

LÍNEA DE ACTUACIÓN 2.1

Capacidades para la detección

INCIBE desarrollará capacidades para detectar aquello que pueda afectar a la seguridad frente a ciberamenazas.
Es necesario, además, que INCIBE obtenga cada vez más información mediante medios propios, reduciendo su dependencia de fuentes externas proveedoras de información.

MEDIDA 9. Optimización y desarrollo continuado de las capacidades de detección.



LÍNEA DE ACTUACIÓN 2.2

Capacidades para la inteligencia

INCIBE construirá capacidades que permitan analizar y enriquecer los datos que se obtengan, para generar conocimiento nuevo a partir de la agregación de múltiples fuentes de detección.

MEDIDA 10. Optimización y desarrollo continuado de las capacidades de inteligencia.

MEDIDA 11. Desarrollo de capacidades para la medición del riesgo.

LÍNEA DE ACTUACIÓN 2.3

Explotación de la información

INCIBE generará valor a partir del conocimiento que obtenga de la explotación y diseminación de la información, desarrollando acciones que permitan generar valor a partir de la inteligencia.

MEDIDA 12. Desarrollo y fortalecimiento de las capacidades para la accionabilidad de información de ciberinteligencia.

MEDIDA 13. Difusión de la información de ciberinteligencia para la accionabilidad de terceros.

OBJETIVO ESTRATÉGICO

03. POTENCIAR LAS CAPACIDADES DE AYUDA, SOPORTE Y RESPUESTA FRENTE A RIESGOS, AMENAZAS E INCIDENTES

El servicio público de ciberseguridad que ofrece INCIBE debe ser completo, de calidad y de fácil acceso, estimulando la demanda de servicios del sector de la ciberseguridad. Para dar respuesta a las crecientes necesidades de ciudadanos y empresas, INCIBE trabajará en canales electrónicos para recibir las peticiones de ayuda, y en medios automatizados para realizar un diagnóstico y dar una respuesta.

LÍNEA DE ACTUACIÓN 3.1

Capacidades para la ayuda, soporte y respuesta

INCIBE trabajará en prestar un servicio de ayuda, soporte y respuesta ágil, de calidad y de fácil acceso ante consultas e incidentes de ciberseguridad. Este servicio podrá además crecer y adaptarse a la demanda.

MEDIDA 14. Fortalecimiento de las capacidades de soporte y respuesta a incidentes.

MEDIDA 15. Fortalecimiento de los servicios de soporte y respuesta a incidentes.

LÍNEA DE ACTUACIÓN 3.2

Servicios especializados para empresas

INCIBE desarrollará servicios para la protección de las empresas del sector privado, especialmente operadores de servicios estratégicos. INCIBE debe establecer los mecanismos que aseguren información ante cualquier incidente que afecte a estas empresas.

MEDIDA 16. Fortalecimiento de las capacidades de respuesta de empresas y pymes ante incidentes de ciberseguridad.

MEDIDA 17. Fortalecimiento de las capacidades de resiliencia y recuperación de los Operadores de Servicios Críticos y Proveedores de Servicios Digitales.

MEDIDA 18. Protección de activos de empresas.

LÍNEA DE ACTUACIÓN 3.3

Capacidades para la gestión de crisis cibernéticas

INCIBE deberá estar preparado para asumir la parte que le corresponda en la gestión de las crisis, a través de los mecanismos necesarios.

MEDIDA 19. Desarrollo y optimización de las capacidades de gestión de crisis.

OBJETIVO ESTRATÉGICO

04. DESARROLLAR LAS CAPACIDADES NECESARIAS PARA PROTEGER Y DEFENDER ACTIVAMENTE A CIUDADANOS Y EMPRESAS

A través de este objetivo se desarrollarán iniciativas que promuevan una protección y prevención activas ante criminales profesionalizados y especializados. Desde INCIBE se desarrollará la defensa activa de ciudadanos y empresas, poniendo en marcha acciones destinadas a identificar anomalías de manera preventiva.

LÍNEA DE ACTUACIÓN 4.1

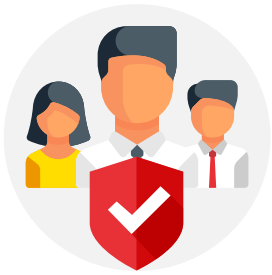
Diseño, implantación y operación de medidas de ciberdefensa activa de menores en Internet

INCIBE desarrollará acciones específicas orientadas a la prevención y protección de los menores en el ciberespacio, al ser un colectivo especialmente vulnerable a las amenazas en Internet.

MEDIDA 20. Fortalecimiento y optimización de las capacidades de prevención.

MEDIDA 21. Fortalecimiento y optimización de las capacidades de defensa activa.

MEDIDA 22. Operación de herramientas y soluciones.



LÍNEA DE ACTUACIÓN 4.2

Diseño, implantación y operación de medidas de ciberdefensa activa de ciudadanos y empresas

INCIBE incorporará medidas concretas de defensa activa para ciudadanos y empresas, con especial interés en medianas empresas, pymes y autónomos que por sus características, no siempre pueden garantizar su protección en el mundo digital.

MEDIDA 23. Implementación y desarrollo de soluciones y medidas de defensa activa de ciudadanos y empresas.

LÍNEA DE ACTUACIÓN 4.3

Avances normativos para la protección de ciudadanos y, empresas

INCIBE trabajará para impulsar la seguridad de la industria, también a través del marco regulatorio. Aunque INCIBE pueda proponer la implantación de medidas de ciberdefensa, la mayor parte de ellas requieren de la colaboración de empresas privadas, un aspecto fundamental.

MEDIDA 24. Proposición de modificaciones normativas para la protección de ciudadanos y empresas.

05. OBJETIVO ESTRATÉGICO IMPULSAR LA INDUSTRIA ESPAÑOLA Y LA I+D+I DE CIBERSEGURIDAD

España debe contar con los recursos técnicos y humanos necesarios, y la capacitación adecuada para cubrir las exigencias de la ciberseguridad nacional. También es necesario desarrollar una política clara de impulso de la I+D+i en el sector de la ciberseguridad, como una palanca clave de crecimiento.

LÍNEA DE ACTUACIÓN 5.1

Potenciación de la industria española de ciberseguridad

INCIBE impulsará la industria del sector, su competitividad y su internacionalización. Esto se hará a través de la generación de nuevos actores, y de una industria fuerte e internacional.

MEDIDA 25. Impulso al emprendimiento en ciberseguridad.

MEDIDA 26. Desarrollo y fortalecimiento de la industria de ciberseguridad.

MEDIDA 27. Internacionalización de la industria de ciberseguridad.

LÍNEA DE ACTUACIÓN 5.2

Impulso a la I+D+i española en ciberseguridad.

El panorama de ciberamenazas y de empresas capaces de prestar servicios para hacerles frente, evoluciona de forma constante. INCIBE impulsará la I+D+i en ciberseguridad, que se configura como una necesidad y como una oportunidad para el crecimiento económico con la creación de nuevas empresas innovadoras.

MEDIDA 28. Fortalecer e incrementar las capacidades de I+D+i.

MEDIDA 29. Transformación de la I+D+i en activos de alto valor añadido.

MEDIDA 30. Potenciar la posición española en I+D+i relacionado con la ciberseguridad.

LÍNEA DE ACTUACIÓN 5.3

Impulso a la inversión empresarial en ciberseguridad

INCIBE trabajará para fomentar la atracción de capital e inversión en industria e I+D+i de ciberseguridad. El crecimiento y desarrollo de la industria de ciberseguridad española estará vinculado a su capacidad de tracción de capital para la puesta en marcha de iniciativas.

MEDIDA 31. Atracción de inversión para el crecimiento y desarrollo de la industria de ciberseguridad.

06. OBJETIVO ESTRATÉGICO PROMOVER Y DETECTAR TALENTO EN CIBERSEGURIDAD

Existe una creciente demanda a nivel global de profesionales de la seguridad digital. INCIBE debe dinamizar la detección, promoción y desarrollo del talento que permita dar respuesta a las necesidades de la industria. Esto debe hacerse aumentando la cantidad y la calidad del talento disponible.

LÍNEA DE ACTUACIÓN 6.1

Fomento, detección y aprovechamiento del talento en ciberseguridad

INCIBE fomentará la identificación y promoción del talento, detectando y contribuyendo al desarrollo de los perfiles y las competencias en ciberseguridad, y su gestión para que evolucionen y mejoren.

MEDIDA 32. Mejorar las capacidades de empresas para la identificación y desarrollo del talento en ciberseguridad.

MEDIDA 33. Generación e identificación de talento en ciberseguridad.

LÍNEA DE ACTUACIÓN 6.2

Fomento de la capacitación del talento en ciberseguridad

INCIBE ofrecerá y fomentará la generación de contenidos actuales, atractivos y adaptados a las necesidades de cada público, asegurando que dichos contenidos llegan a sus destinatarios. Todo ello para aumentar la capacitación en ciberseguridad.

MEDIDA 34. Transformación de talento en ciberseguridad.

MEDIDA 35. Fortalecer la cooperación público-privada para la generación y desarrollo del talento en ciberseguridad.

07. OBJETIVO ESTRATÉGICO POSICIONAR INCIBE COMO REFERENTE EUROPEO DE CIBERSEGURIDAD

Para desarrollar su actividad en un entorno transnacional y de cooperación internacional, INCIBE debe jugar un papel destacado en el plano internacional. INCIBE debe integrarse en foros para la protección de ciudadanos y empresas, adaptándose y mejorando para hacer frente a los desafíos de la ciberseguridad.

LÍNEA DE ACTUACIÓN 7.1

El reconocimiento y posicionamiento de INCIBE como impulsor de la ciberseguridad y la confianza digital.

INCIBE asegurará la posición de España en los foros nacionales e internacionales relevantes, incrementando la cooperación y asegurando la transferencia y adquisición de buenas prácticas en ciberseguridad.

MEDIDA 36. Posicionamiento de INCIBE como actor de referencia en el ámbito nacional e internacional.

MEDIDA 37. Desarrollo del relacionamiento estratégico de INCIBE.

LÍNEA DE ACTUACIÓN 7.2

Impulso de España como nodo internacional de la ciberseguridad.

INCIBE desarrollará las iniciativas necesarias para consolidar a España como nodo internacional de la Ciberseguridad. España es actualmente el cuarto país de la Unión Europea en relación a su madurez en ciberseguridad.

MEDIDA 38. Impulso del Centro Espejo de Ciberseguridad en España.

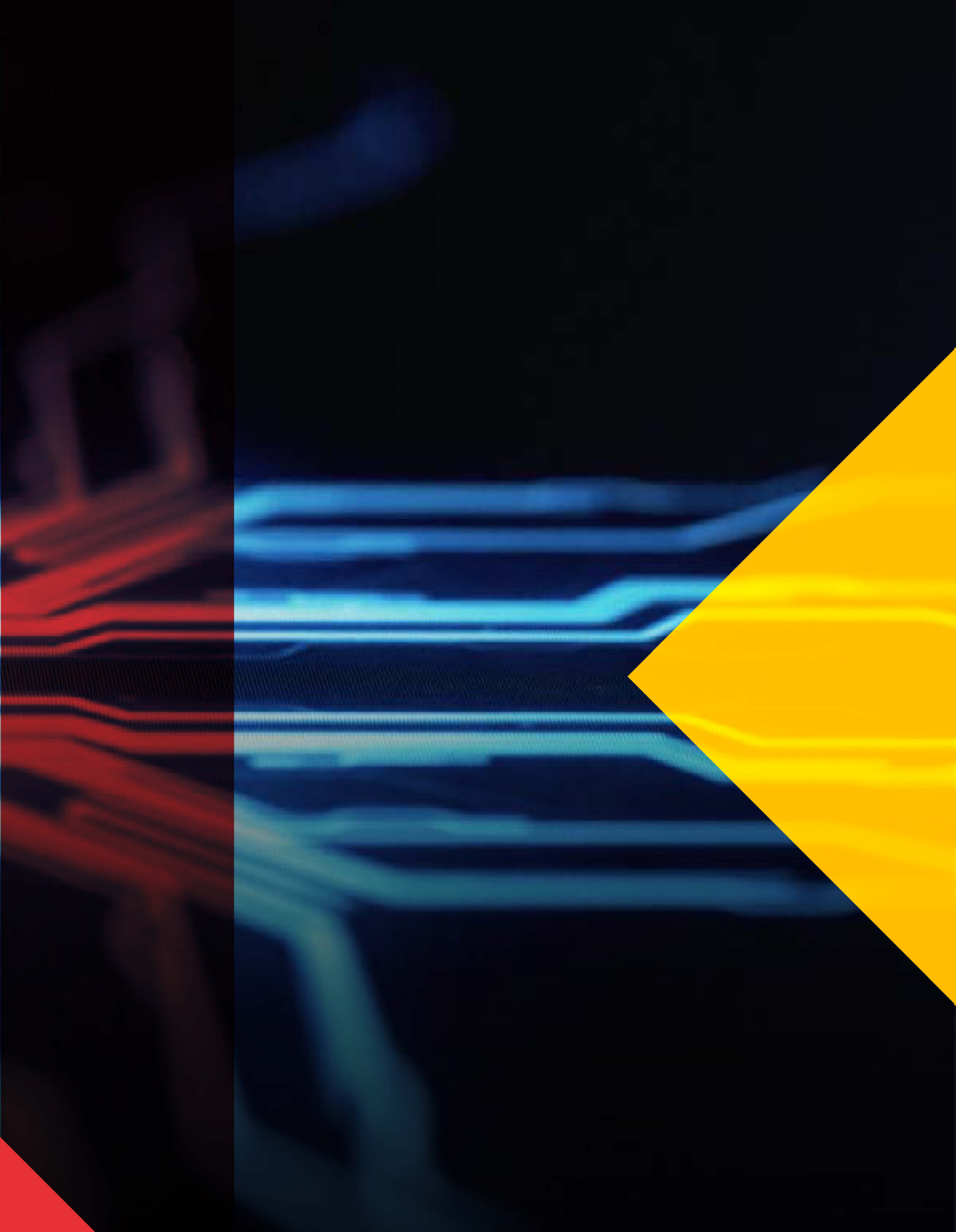
MEDIDA 39. Impulso y coordinación de la comunidad de ciberseguridad.

05

RESUMEN DE MEDIDAS

OBJETIVO ESTRATÉGICO	MEDIDA
01 PROMOVER UNA CULTURA DE CIBERSEGURIDAD EN ESPAÑA	**1.** Fortalecimiento de las capacidades de ciberseguridad de la sociedad. **2.** Fortalecimiento de las capacidades de ciberseguridad de empresas. **3.** Incremento de capacidades de ciberseguridad de "actores intermedios". **4.** Fortalecimiento de servicios públicos, canales herramientas para la extensión de la cultura de ciberseguridad. **5.** Desarrollo del Foro Nacional de Ciberseguridad (contribución). **6.** Identificación y desarrollo de mecanismos de multiplicación de los esfuerzos de fortalecimiento. **7.** Desarrollo de la Responsabilidad Social empresarial de INCIBE. **8.** Desarrollo del conocimiento de la ciberseguridad en España.
02 AUMENTAR Y FORTALECER LAS CAPACIDADES PARA DETECTAR CIBERAMENAZAS	**9.** Optimización y desarrollo continuado de las capacidades de detección. **10.** Optimización y desarrollo continuado de las capacidades de inteligencia. **11.** Desarrollo de capacidades para la medición del riesgo. **12.** Desarrollo y fortalecimiento de las capacidades para la accionabilidad de información de ciberinteligencia. **13.** Difusión de la información de ciberinteligencia para la accionabilidad de terceros.
03 POTENCIAR LAS CAPACIDADES DE AYUDA, SOPORTE Y RESPUESTA FRENTE A RIESGOS, AMENAZAS E INCIDENTES	**14.** Fortalecimiento de las capacidades de soporte y respuesta de incidentes. **15.** Fortalecimiento de los servicios de soporte y respuesta a incidentes. **16.** Fortalecimiento de las capacidades de respuesta de empresas y pymes ante incidentes de ciberseguridad. **17.** Fortalecimiento de las capacidades de resiliencia y recuperación de los Operadores de Servicios Críticos y Proveedores de Servicios Digitales. **18.** Protección de activos de empresas. **19.** Desarrollo y optimización de las capacidades de gestión de crisis.

OBJETIVO ESTRATÉGICO	MEDIDA
04 DESARROLLAR LAS CAPACIDADES NECESARIAS PARA PROTEGER Y DEFENDER ACTIVAMENTE A CIUDADANOS Y EMPRESAS	***20.*** Fortalecimiento y optimización de las capacidades de prevención. ***21.*** Fortalecimiento y optimización de las capacidades de defensa activa. ***22.*** Operación de herramientas y soluciones. ***23.*** Implementación y desarrollo de soluciones y medidas de defensa activa. ***24.*** Proposición de modificaciones normativas para la protección de ciudadanos y empresas.
05 IMPULSAR LA INDUSTRIA ESPAÑOLA Y LA I+D+I DE CIBERSEGURIDAD	***25.*** Impulso al emprendimiento en ciberseguridad ***26.*** Desarrollo y fortalecimiento de la industria de ciberseguridad. ***27.*** Internacionalización de la industria de ciberseguridad. ***28.*** Fortalecer e incrementar las capacidades de I+D+i. ***29.*** Transformación de la I+D+i en activos de alto valor añadido. ***30.*** Potenciar la posición española de la I+D+i relacionado con la ciberseguridad. ***31.*** Atracción de inversión para el crecimiento y desarrollo de la industria de ciberseguridad.
06 PROMOVER Y DETECTAR TALENTO EN CIBERSEGURIDAD	***32.*** Mejoras de las capacidades de empresas para la identificación y desarrollo del talento en ciberseguridad. ***33.*** Generación e identificación de talento en ciberseguridad. ***34.*** Transformación de talento en ciberseguridad. ***35.*** Fortalecer la cooperación público-privada para la generación y desarrollo del talento en ciberseguridad.
07 POSICIONAR INCIBE COMO REFERENTE EUROPEO DE CIBERSEGURIDAD	***36.*** Posicionamiento de INCIBE como actor de referencia en el ámbito nacional e internacional. ***37.*** Desarrollo del relacionamiento estratégico de INCIBE. ***38.*** Impulso del Centro Espejo de Ciberseguridad en España. ***39.*** Impulso y coordinación de la comunidad de ciberseguridad.



GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017

PLAN ANUAL DE ACTIVIDAD INCIBE 2021

Resultados conseguidos

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017

ÍNDICE

1. PRESENTACIÓN

Qué es INCIBE

La S.M.E. Instituto Nacional de Ciberseguridad de España (INCIBE), M.P., S.A., sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaria de Estado de Digitalización e Inteligencia Artificial (SEDIA), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital en el sector privado. En particular para los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

Dentro de la actividad del Instituto se encuentra INCIBE-CERT, el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España. En el caso de la gestión de incidentes que afecten a operadores críticos del sector privado, INCIBE-CERT está operado conjuntamente por INCIBE y CNPIC, Centro Nacional de Protección de Infraestructuras y Ciberseguridad del Ministerio del Interior.

Actividad de INCIBE

El desarrollo de la Inteligencia Artificial, el 5G y otras tecnologías habilitadoras están generando una profundización exponencial de la digitalización y su previsible impacto socioeconómico, así como una ampliación de la superficie de riesgo para la seguridad digital. Ampliar o generar capacidades (técnicas y humanas) en ciberseguridad es clave para poder incorporar las oportunidades de la digitalización minimizando sus riesgos asociados.

En este escenario global, el Gobierno de España presentó en julio de 2020 la agenda España Digital 2025, un cuaderno de bitácora para la transformación digital del país que permita optimizar los beneficios socioeconómicos de la digitalización, minimizando sus riesgos asociados. Esta agenda digital se desarrolla a través de 10 ejes estratégicos, siendo el cuarto de ellos la ciberseguridad. INCIBE se alinea su actividad con a esa agenda y con los objetivos y metas que esta persigue, junto al cuerpo estratégico de la Seguridad Nacional referido anteriormente.

Para hacerlo, el Instituto busca contribuir a que el nivel de seguridad digital de ciudadanos y empresas privadas, así como la industria española de ciberseguridad, estén entre los cinco mejores del mundo, orientando sus actividades al desarrollo de 3 ejes estratégicos:

- **Fortalecimiento de la ciberseguridad de ciudadanos, PyMEs y profesionales**. Para que España sea uno de los países más ciberseguros del mundo debe incrementar las capacidades de ciberseguridad.

- **Impulso del ecosistema empresarial del Sector Ciberseguridad.** El segundo eje de actuación se orienta hacia el impulso el ecosistema de ciberseguridad español a través de 3 palancas: (i) el desarrollo de la industria de ciberseguridad, (ii) el impulso de I+D+i, y (iii) la identificación, generación y desarrollo del talento.

- **Impulso de España como nodo internacional en el ámbito de la Ciberseguridad.** A través de este eje, INCIBE trabaja en la consolidación de España como uno de los países con mayor madurez de ciberseguridad en el ámbito europeo y global.

2. PLAN ESTRATÉGICO 2021-2025

El Plan Estratégico de INCIBE para el periodo 2021-2025, bajo el lema '***de miles a millones'***, busca generar un efecto multiplicador en el resultado de actuaciones que desarrolla, y conseguir llegar a más ciudadanos y más empresas con el objetivo de **elevar el nivel de ciberseguridad de la ciudadanía y empresas privadas.** Igualmente, este plan permitirá impulsar la actividad para su posicionamiento como un actor destacado en el ámbito internacional y reafirmar el compromiso de España como referente europeo en el ámbito de la ciberseguridad.

En un entorno cambiante y dinámico como el de la ciberseguridad, este plan de 5 años no define acciones específicas que podrían limitar la capacidad de reacción de INCIBE ante escenarios cambiantes, sino directrices estratégicas a través de líneas de actuación prioritarias. A la finalización del plan, en 2025, INCIBE prestará servicios de alto valor para el conjunto de ecosistemas relacionados con la ciberseguridad. Dichos servicios contribuirán a afianzar la Sociedad de la Información y la Transformación Digital en España; y serán instrumentos eficaces del Gobierno de España para la consecución de sus objetivos.

Misión, Visión y Valores

En el marco de dicho plan, la misión de INCIBE es ser un motor para la transformación digital de la sociedad, protegiendo a ciudadanos, menores y empresas privadas en España y fomentando la industria de la ciberseguridad, la I+D+i y el talento.

Para ello, la visión se focaliza en tres aspectos, 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 y, posicionar INCIBE como referente europeo en el ámbito de la ciberseguridad.

Para poder responder a la misión y visión planteadas, se han definido una serie de valores para INCIBE, que servirán asimismo como principios rectores del diseño del Plan Estratégico, y que serán también referentes durante su desarrollo y ejecución:

- Vocación de servicio público
- Espíritu neutral y colaborativo
- Proactividad y flexibilidad
- Excelencia
- Innovación
- Desempeño responsable y transparente
- Colaboración nacional e internacional

Fundamentos estratégicos y legales

El crecimiento exponencial de la tecnología y la hiperconectividad ofrecen enormes oportunidades de desarrollo económico y social, y nos acercan a un mundo global e interdependiente. Al mismo tiempo, este profundo proceso de digitalización trae consigo nuevas amenazas para la seguridad. Cada desarrollo, cada avance tecnológico, ofrece esta dualidad de riesgo-oportunidad que debe ser abordado. Las amenazas cibernéticas a las que se enfrentan ciudadanos y empresas comparten al menos 3 características clave:

- Carácter evolutivo y cambiante, lo que hace imprescindible un proceso ágil, eficaz y **sostenible** de investigación y formación de las personas e instituciones encargadas de velar por la seguridad digital, y una transferencia de ese conocimiento a ciudadanos, empresas y gobiernos para mantener el ecosistema digital protegido.
- Mayor complejidad de las amenazas e incidentes cibernéticos, así como una mayor sofisticación del ciberdelito y el ciberdelincuente.
- Carácter global y transnacional de las amenazas e incidentes cibernéticos, lo que nos lleva a abordar la cuestión desde una perspectiva de colaboración y cooperación en el ámbito internacional.

El Plan Estratégico se alinea conceptual y temporalmente con España Digital 2025, la agenda para la transformación digital del país en los próximos 5 años. Igualmente este Plan nace en un contexto de pandemia global del que se deriva el Plan de Recuperación, Transformación y Resiliencia de la Economía Española mediante el que se articula el instrumento «Next Generation EU», en el cual INCIBE tomará parte para desarrollar actividades que contribuyan a la recuperación económica y transformación del país.

- Marco Estratégico
  - La **Estrategia Nacional de Ciberseguridad de 2019 (**ENCS19), que es el documento estratégico principal que sirve de base para el presente Plan. Una parte sustancial de los objetivos y de las acciones definidos en la ENCS19 caen directamente dentro de la misión asignada a INCIBE, y por tanto deben inexcusablemente ser contemplados en este Plan.
  - La **Estrategia de Seguridad Nacional de 2017**, que fija unos objetivos generales transversales a todos los ámbitos: la gestión de crisis, la cultura de Seguridad Nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España; y que incorpora a INCIBE como uno de los organismos del Estado para alcanzar los objetivos de dicha estrategia.
  - La **agenda España Digital 2025** del Ministerio de Asuntos Económicos y Transformación Digital.
  - La **Estrategia Nacional contra el Crimen Organizado** y la Delincuencia Grave 2019-2023, entre cuyas prioridades se encuentra la lucha contra el cibercrimen.
- Cuerpo normativo aprobado o incorporado por el Parlamento nacional que influyen directamente en la misión y funciones de INCIBE como los siguientes:

- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148, conocida como Directiva NIS.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de Datos Personales y Garantía de los Derechos Digitales.

Del mismo modo, se tiene en cuenta para este Plan de Actividad el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, para que INCIBE pueda implementar las actuaciones derivadas de este RD. Esta normativa no figura en el Plan Estratégico original porque en el momento de presentación del Plan Estratégico 2021-2025, el RD 43/2021 no estaba vigente.

Destinatarios clave

Las actividades de INCIBE se orientan a destinatarios como ciudadanos, empresas, organismos públicos y otros agentes de interés de todos los sectores y ámbitos que en el desarrollo de sus actividades interactúan con el ámbito de la ciberseguridad y a los que INCIBE se aproxima desde su vocación de servicios público y promotor de la cultura de la ciberseguridad.

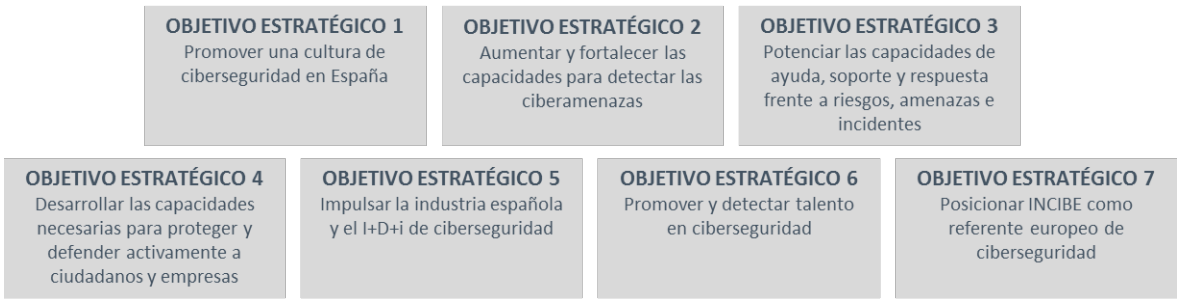
Concretamente, estos destinatarios se subdividen en cuatro grandes grupos:

- Ciudadanos: cualquiera que emplee tecnologías y dispositivos, con especial atención en los menores por ser un colectivo muy vulnerable.
- Empresas: Operadores de Servicios Esenciales, y sectores estratégicos; las grandes, medianas y pequeñas empresas; las microempresas y los autónomos; y la industria de Ciberseguridad en general.
- Organismos Públicos:
  - Secretaría General de Administración Digital (SGAD);
  - Centro Criptológico Nacional (CCN);
  - Departamento de Seguridad Nacional (DSN);
  - Mando Conjunto del Ciberespacio (MCCE);
  - Oficina de Coordinación de Ciberseguridad; y
  - Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

- Otros Agentes de Interés:
  - Otros agentes públicos de ciberseguridad con los que se relaciona INCIBE
  - El entorno académico y de investigación, usuarios de la Red Académica y de Investigación RedIRIS, y tractores de la generación de nuevos productos y servicios de ciberseguridad.
  - Los profesionales de la ciberseguridad, además de los expertos reconocidos.
  - Los jóvenes talentos y otros colectivos, con el objetivo de promocionar el interés por la ciberseguridad y su capacitación.
  - Otros agentes nacionales e internacionales de todos los sectores y ámbitos que en el desarrollo de sus actividades interactúan con el ámbito de la ciberseguridad
  - El propio INCIBE, ya que se acometerán actuaciones para la mejora de la entidad en todos los aspectos.

Objetivos estratégicos

El Plan de Actividad 2021 desarrolla su actividad en el marco de los objetivos estratégicos que figuran en el Plan Estratégico 2021-2025, y que son los siete siguientes:



A continuación se desarrollan los Objetivos y Líneas de Acción, que se asocian de manera correspondiente a las dotaciones presupuestarias previstas y en curso para el período enero-diciembre 2021, completando así el global del Plan en función de la previsión de gasto por parte de INCIBE.

Para que INCIBE desarrolle su Misión, y se pueda acercar hacia su Visión, se establecen los **7 objetivos estratégicos para el período 21-25**:

- **OBJETIVO ESTRATÉGICO 1**. Promover una cultura de ciberseguridad en España.
- **OBJETIVO ESTRATÉGICO 2.** Aumentar y fortalecer las capacidades para detectar las ciberamenazas.
- **OBJETIVO ESTRATÉGICO 3.** Potenciar las capacidades de ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes.
- **OBJETIVO ESTRATÉGICO 4**. Desarrollar las capacidades necesarias para proteger y defender activamente a ciudadanos, menores y empresas.
- **OBJETIVO ESTRATÉGICO 5**. Impulsar la industria española y la I+D+i de ciberseguridad.
- **OBJETIVO ESTRATÉGICO 6**. Promover y detectar talento en ciberseguridad.

- **OBJETIVO ESTRATÉGICO 7**. Posicionar INCIBE como referente europeo de ciberseguridad

Para la consecución de estos objetivos INCIBE llevará a cabo iniciativas y actuaciones que se estructuran en líneas de actuación. En los siguientes apartados se describen los **7 objetivos estratégicos** y las líneas de actuación previstas que permitirán alcanzarlo.

OBJETIVO ESTRATÉGICO 1. Promover una cultura de la Ciberseguridad en España

La primera responsabilidad es generar conciencia acerca de la existencia de esas amenazas y riesgos, y conseguir esa participación imprescindible para construir y desarrollar una cultura de ciberseguridad en colaboración con actores públicos y privados, tanto en el ámbito nacional como internacional, y potenciar mecanismos de concienciación, información y formación.

Esta cultura de ciberseguridad hace referencia al conocimiento, adopción y compromiso sostenible con hábitos saludables y buenas prácticas en el mundo cibernético por parte de ciudadanos, empresas y administración pública. Los espacios de encuentro entre INCIBE y los destinatarios de su misión, o entre empresas, entidades o individuos que pudieran tener características e intereses similares, contribuirán a la consecución de este objetivo. Las líneas de actuación que conducirán a la consecución del objetivo 1 son:

LÍNEA DE ACTUACIÓN 1.1: Promoción de la concienciación y la información

Las actividades pertenecientes a esta línea de actuación buscarán concienciar a ciudadanos y empresas no sólo de que están expuestos, sino de que deben tomar las acciones necesarias para conocer sus riesgos y protegerse. Esta Línea se desarrollará a través de 4 medidas estratégicas:

MEDIDA 1. Fortalecimiento de las capacidades de ciberseguridad de la sociedad

MEDIDA 2. Fortalecimiento de capacidades de ciberseguridad de empresas

MEDIDA 3. Incremento de capacidades de ciberseguridad de "actores intermedios"

MEDIDA 4. Fortalecimiento de Servicios Públicos, Canales y Herramientas para la extensión de la Cultura de Ciberseguridad

LÍNEA DE ACTUACIÓN 1.2: Impulso de la colaboración público-privada y de la RSC

La seguridad digital de ciudadanos y empresas debe ser un compromiso compartido. Bajo esta línea de actuación, INCIBE realizará acciones para impulsar la colaboración público-privada para la extensión de una cultura de ciberseguridad, los servicios de valor añadido y el cumplimiento de su misión.

MEDIDA 5. Desarrollo del Foro Nacional de Ciberseguridad (contribución)

MEDIDA 6. Identificación y Desarrollo de "mecanismos de multiplicación" de los esfuerzos de fortalecimiento

MEDIDA 7. Desarrollo de la Responsabilidad Social Empresarial de INCIBE

LÍNEA DE ACTUACIÓN 1.3: Impulso de la Generación de Conocimiento sobre CS

La generación de conocimiento sobre la realidad de las amenazas y riesgos cibernéticos en diferentes ámbitos, sectores productivos y a nivel nacional e internacional, ofrece una foto amplia de la realidad sobre la que desarrollar la actividad de INCIBE. A través de esta línea de actuación se contribuirá al posicionamiento de INCIBE como un actor destacado y fuente de conocimiento de alto valor sobre ciberseguridad a nivel nacional e internacional.

MEDIDA 8. Desarrollo del Conocimiento de la Ciberseguridad en España

OBJETIVO ESTRATÉGICO 2. Aumentar y fortalecer las capacidades para detectar las ciberamenazas.

La detección de diferentes vectores de ataque de manera proactiva permitirá una alerta temprana adecuada y en algunos casos la detección de posibles intrusiones que no se hayan desplegado o que el usuario no percibe.

Por tanto, INCIBE debe conocer las ciberamenazas, detectar al menos sus potenciales víctimas españolas y los activos españoles comprometidos, y entender cómo actúan, es decir, conocer sus TTP's (Técnicas, Tácticas y Procedimientos) y cuáles son las infraestructuras que usan. La información que se obtenga debe ser accionable, es decir, debe permitir a INCIBE tomar acciones para la prevención y protección de las víctimas potenciales, para su defensa activa o para la mitigación del daño que las ciberamenazas puedan causar.

Las líneas de actuación previstas que conducirán a la consecución del objetivo 2 son:

LÍNEA DE ACTUACIÓN 2.1: Capacidades para la detección

Dentro de esta línea de actuación se desarrollan las acciones dirigidas a crear y operar capacidades que permitan a INCIBE detectar aquello que pueda ser significativo para la seguridad de los españoles frente a las ciberamenazas.

MEDIDA 9. Optimización y desarrollo continuado de las capacidades de detección

LÍNEA DE ACTUACIÓN 2.2: Capacidades para la inteligencia

La detección por sí sola no es suficiente. Los datos que se obtengan deben ser normalizados, relacionados, analizados y enriquecidos a partir de información previa, de contexto y de datos obtenidos de otras fuentes, de forma que sea posible generar conocimiento nuevo a partir de la agregación de múltiples fuentes de detección.

MEDIDA 10. Optimización y desarrollo continuado de las capacidades de inteligencia

MEDIDA 11. Desarrollo de capacidades para la medición del riesgo.

LÍNEA DE ACTUACIÓN 2.3: Explotación de la información

INCIBE debe poder generar valor a partir del conocimiento que obtenga de las dos líneas de actuación anteriores a través de la explotación y diseminación de la información. Esta línea de actuación recogerá todas las acciones orientadas a esta generación de valor a partir de la inteligencia.

MEDIDA 12. Desarrollo y fortalecimiento de las capacidades para la accionabilidad de información de ciberinteligencia

MEDIDA 13. Difusión de la información de ciberinteligencia para la accionabilidad de terceros.

OBJETIVO ESTRATÉGICO 3. Potenciar las capacidades de ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes.

Cuando un ciudadano o una empresa contactan con INCIBE porque percibe que puede tener un problema de ciberseguridad, debe recibir un servicio público de ciberseguridad integrado, de calidad y de fácil acceso, y que sea un estímulo a la demanda de los servicios que ofrece el sector empresarial de la ciberseguridad.

Para dar respuesta a estas necesidades de ciudadanos y empresas, INCIBE trabajará no sólo en canales electrónicos para recibir las peticiones de ayuda, sino también en medios automatizados para diagnosticar y responder cuando ello sea posible.

Las líneas de actuación que conducirán a la consecución del objetivo 3 son aquellas que permitan generar:

LÍNEA DE ACTUACIÓN 3.1: Capacidades para la ayuda, soporte y respuesta

Las acciones que se encuentran dentro de esta línea de actuación son aquellas dirigidas a que INCIBE preste un servicio de ayuda, soporte y respuesta ágil, de calidad y de fácil acceso.

MEDIDA 14. Fortalecimiento de las capacidades de soporte y respuesta a incidentes

MEDIDA 15. Fortalecimiento de los servicios de soporte y respuesta a incidentes

LÍNEA DE ACTUACIÓN 3.2: Servicios especializados para empresas

A través de esta línea de actuación se desarrollarán servicios para protección en el ciberespacio para las empresas del sector privado. Deben establecerse los mecanismos que aseguren que INCIBE está puntualmente informado ante cualquier incidente que pueda afectar a estas empresas, de forma que se puedan tomar acciones lo antes posible.

MEDIDA 16. Fortalecimiento de las capacidades de respuesta de empresas y pymes ante incidentes de Ciberseguridad

MEDIDA 17. Fortalecimiento de las capacidades de resiliencia y recuperación de los Operadores de Servicios Críticos y Proveedores de Servicios Digitales

MEDIDA 18. Protección de activos de empresas

LÍNEA DE ACTUACIÓN 3.3: Capacidades para la gestión de crisis cibernéticas

Inevitablemente, un incidente o conjunto de incidentes, pueden generar una situación catalogada como crisis. INCIBE, dentro del alcance de las responsabilidades que se le asignen en el Sistema de Seguridad Nacional, debe estar preparado para asumir la parte que le corresponda en la gestión de las crisis. Las actuaciones que preparen a INCIBE en este sentido, deberán ser recogidas en esta línea de actuación.

MEDIDA 19. Desarrollo y optimización de las capacidades de gestión de crisis

OBJETIVO ESTRATÉGICO 4. Desarrollar las capacidades necesarias para proteger y defender activamente a ciudadanos y empresas.

A través de este objetivo se desarrollarán iniciativas que desde el Estado promuevan una protección y prevención activas ante criminales cada vez más profesionalizados y especializados. Por tanto, desde INCIBE, se desarrollarán las líneas de actuación que busquen proteger el ciberespacio para defender activamente a ciudadanos y empresas. Estas actuaciones necesitarán de la cooperación público-privada, y para conseguirla, en muchos casos se requerirá de modificaciones normativas. Las líneas de actuación que conducirán a la consecución del objetivo 4 son:

LÍNEA DE ACTUACIÓN 4.1: Diseño, implantación y operación de medidas de ciberdefensa activa de menores en Internet

A través de esta línea de actuación se desarrollarán acciones específicas orientadas a la prevención y protección de los menores en el ciberespacio, al ser precisamente un colectivo especialmente sensible y vulnerable a las amenazas en Internet.

MEDIDA 20. Fortalecimiento y optimización de las capacidades de prevención

MEDIDA 21 Fortalecimiento y optimización de las capacidades de defensa activa

MEDIDA 22. Operación de herramientas y soluciones

LÍNEA DE ACTUACIÓN 4.2: Diseño, implantación y operación de medidas de ciberdefensa activa de ciudadanos y empresas

Esta línea de actuación incorporará medidas específicas de defensa activa para ciudadanos y empresas. Serán públicos de especial interés las medianas empresas, pymes

y autónomos que por sus características, recursos y tamaño, en muchas ocasiones no pueden contar con las capacidades de grandes empresas para mejorar su protección en el mundo digital.

MEDIDA 23. Implementación y desarrollo de soluciones y medidas de defensa activa de ciudadanos y empresas

LÍNEA DE ACTUACIÓN 4.3: Avances normativos para la protección de ciudadanos y, empresas

Como ya prevé la propia ENCS19 en su Línea de Actividad 4 - Medida 5, aunque INCIBE pueda proponer la implantación de medidas de ciberdefensa activa, la mayor parte de ellas requieren de la colaboración de empresas privadas o de modificaciones normativas. Todas las actuaciones y propuestas en este sentido, se desarrollarán bajo esta línea de actuación.

MEDIDA 24. Proposición de modificaciones normativas para la protección de ciudadanos y empresas

OBJETIVO ESTRATÉGICO 5. Impulsar la industria española y el I+D+i de ciberseguridad

Para afrontar los desafíos que plantea la ciberseguridad, España debe contar con los recursos técnicos y humanos necesarios y la capacitación adecuada para cubrir las exigencias de la ciberseguridad nacional, lo cual además es un habilitador clave para una economía que quiera desarrollar el crecimiento de su sector de ciberseguridad. De igual modo, es necesario el desarrollo de una política clara de impulso de la I+D+i en el sector de la ciberseguridad. A través de este objetivo se impulsará esta palanca clave de crecimiento.

Las líneas de actuación que conducirán a la consecución del objetivo 5 son aquellas que permitan generar:

LÍNEA DE ACTUACIÓN 5.1: Potenciación de la industria española de ciberseguridad

La ciberseguridad en un país no es posible sin una adecuada oferta de productos y servicios de ciberseguridad. Por eso a través de esta línea de actuación se impulsará la industria del sector, su competitividad y su internacionalización.

MEDIDA 25. Impulso al emprendimiento en ciberseguridad

MEDIDA 26. Desarrollo y fortalecimiento de la industria de ciberseguridad

MEDIDA 27. Internacionalización de la industria de ciberseguridad

LÍNEA DE ACTUACIÓN 5.2: Impulso a la I+D+i española en ciberseguridad

La ciberseguridad es un mundo que cambia y evoluciona muy rápido. Con la explosión de la transformación digital, y la aparición de nuevos paradigmas tecnológicos, el panorama de ciberamenazas y de empresas capaces de prestar servicios para hacerles frente, evoluciona de forma constante.

MEDIDA 28. Fortalecer e incrementar las capacidades de I+D+i

MEDIDA 29. Transformación de la I+D+i en activos de alto valor añadido

MEDIDA 30. Potenciar la posición española en I+D+i relacionado con la ciberseguridad

LÍNEA DE ACTUACIÓN 5.3: Impulso a la Inversión Empresarial en Ciberseguridad

El crecimiento y desarrollo de la Industria de Ciberseguridad española estará vinculado a su capacidad de tracción de capital para la puesta en marcha de iniciativas.

MEDIDA 31. Atracción de inversión para el crecimiento y desarrollo de la industria de Ciberseguridad

OBJETIVO ESTRATÉGICO 6. Promover y detectar talento en ciberseguridad.

Existe una creciente demanda a nivel global de profesionales de la seguridad digital como consecuencia del desarrollo de la economía digital y, en general, una digitalización cada vez más profunda y presente en la vida cotidiana de ciudadanos, empresas y Administraciones Públicas. Esta realidad está elevando la demanda de servicios de ciberseguridad que garanticen, en el mundo digital, los estándares de seguridad y confianza del mundo físico. INCIBE debe asumir un rol de dinamizador activo para la detección, promoción y desarrollo del talento. Para impulsar este objetivo 6, INCIBE prevé desarrollar estas líneas de actuación:

LÍNEA DE ACTUACIÓN 6.1: Fomento, detección y aprovechamiento del talento en ciberseguridad

Se debe fomentar la identificación y promoción del talento que demanda el mercado laboral actual y futuro. Para ello INCIBE podrá realizar actuaciones que favorezcan esta identificación y promoción, de los perfiles y las competencias en ciberseguridad necesarias.

MEDIDA 32. Mejoras las capacidades de empresas para la identificación y desarrollo del talento en ciberseguridad

MEDIDA 33. Generación e identificación de talento en ciberseguridad

LÍNEA DE ACTUACIÓN 6.2: Fomento de la capacitación del Talento en ciberseguridad

Se debe fomentar la capacitación en ciberseguridad de los profesionales, adecuada a la demanda del mercado laboral. INCIBE podrá ofrecer, y fomentará la generación por parte de otros agentes, de contenidos actuales, atractivos y adaptados a las necesidades de cada público, asegurando que dichos contenidos llegan a sus destinatarios y son adecuadamente aprovechados.

MEDIDA 34. Transformación de talento en ciberseguridad

MEDIDA 35. Fortalecer la cooperación público-privada para la generación y desarrollo del talento en ciberseguridad

OBJETIVO ESTRATÉGICO 7. Posicionar INCIBE como referente europeo de ciberseguridad.

Con este séptimo objetivo se desarrollarán las actuaciones necesarias para que INCIBE evolucione y se anticipe a las necesidades que permitan cumplir los objetivos estratégicos anteriores, sobre las bases de la mejora continua, el desarrollo profesional y la innovación interna. Al mismo tiempo, bajo este objetivo se trabajara en el seguimiento y control de su actividad, que redunde en una extracción y reutilización del conocimiento generado internamente.

Las líneas de actuación que conducirán a la consecución de este objetivo 7 son:

LÍNEA DE ACTUACIÓN 7.1: El reconocimiento y posicionamiento de INCIBE como impulsor de la ciberseguridad y la confianza digital

Para el cumplimiento de su misión como un actor clave en la ciberseguridad de ciudadanos y empresas en España, INCIBE implementará las acciones necesarias que contribuyan a asegurar la posición de España en los foros nacionales e internacionales relevantes, incrementar la cooperación con otros actores clave y a asegurar la transparencia

MEDIDA 36. Posicionamiento de INCIBE como actor de referencia en el ámbito nacional e internacional

MEDIDA 37. Desarrollo del relacionamiento estratégico de INCIBE

LÍNEA DE ACTUACIÓN 7.2: Impulso de España como nodo internacional de la ciberseguridad

A través de esta Línea de Actuación, INCIBE desarrollará las iniciativas necesarias para consolidar a España como nodo internacional de la ciberseguridad.

MEDIDA 38. Impulso del Centro Espejo de Ciberseguridad en España

MEDIDA 39. Impulso y coordinación de la comunidad de ciberseguridad

3. RESULTADOS CONSEGUIDOS

A continuación, se incorpora el marco de resultados finalmente conseguidos del plan anual 2021. Los indicadores y subindicadores configuran el plan de trabajo vinculados a las medidas, y se identifican los resultados finalmente alcanzados para el presente ejercicio:

OBJETIVO 1: Promover una cultura de ciberseguridad en España			
Peso (LA)	**Línea de acción de Actuación y Medida**	**Peso (MED s/LA)**	**Ejecución**
LÍNEA 1.1. Promoción de la concienciación y la información			
10%	MEDIDA 1 Fortalecimiento e las capacidades de ciberseguridad de la Sociedad	30%	100%
	MEDIDA 2 Fortalecimiento de capacidades de empresas	35%	100%
	MEDIDA 3 Incremento de capacidades de ciberseguridad de "actores intermedios"	15%	100%
	MEDIDA 4 Fortalecimiento de Servicios Públicos, Canales y Herramientas para la extensión de la Cultura de Ciberseguridad	20%	100%
LÍNEA 1.2. Impulso de la colaboración público-privada y de la RSC			
8%	MEDIDA 5 Desarrollo del Foro Nacional de Ciberseguridad (contribución)	40%	100%
	MEDIDA 6 Identificación y Desarrollo de "mecanismos de multiplicación" de los esfuerzos de fortalecimiento	50%	100%
	MEDIDA 7 Desarrollo de la Responsabilidad Social Empresarial de INCIBE	10%	100%
LÍNEA 1.3. Impulso de la Generación de Conocimiento sobre Ciberseguridad			
2%	MEDIDA 8 Desarrollo del Conocimiento de la Ciberseguridad en España	100%	94,70%

OBJETIVO 2: Aumentar y fortalecer las capacidades para detectar las ciberamenazas

Peso (LA)	Línea de acción de Actuación y Medida	Peso (MED s/LA)	Ejecución
LÍNEA 2.1. Capacidades para la Detección			
6%	MEDIDA 9 Optimización y desarrollo continuado de las capacidades de detección	100%	100%
LÍNEA 2.2. Capacidades para la Inteligencia			
3%	MEDIDA 10 Optimización y desarrollo continuado de las capacidades de inteligencia	60%	100%
	MEDIDA 11 Desarrollo de capacidades para la medición del riesgo	40%	100%
LÍNEA 2.3. Explotación de la Información			
3%	MEDIDA 12 Desarrollo y fortalecimiento de las capacidades para la accionabilidad de informafición de ciber-inteligencia	70%	100%
	MEDIDA 13 Difusión de la información de ciber-inteligencia para la accionabilidad de terceros	30%	100%

OBJETIVO 3: Potenciar las capacidades de ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes

Peso (LA)	Línea de acción de Actuación y Medida	Peso (MEDs/LA)	Ejecución
LÍNEA 3.1. Capacidades para la ayuda, soporte y respuesta			
8%	MEDIDA 14 Fortalecimiento de las capacidades de soporte y respuesta a incidentes	50%	100%
	MEDIDA 15 Fortalecimiento de los servicios de soporte y respuesta a incidentes	50%	96,70%
LÍNEA 3.2. Servicios especializados para empresas			
7%	MEDIDA 16 Fortalecimiento de las capacidades de respuesta de empresas y pymes ante incidentes de ciberseguridad	25%	100%
	MEDIDA 17 Fortalecimiento de las capacidades de resiliencia y recuperación de los Operadores de Servicios Críticos y Proveedores de Servicios Digitales	50%	100%
	MEDIDA 18 Protección de activos de empresas	25%	100%
LÍNEA 3.3. Capacidades para la gestión de crisis cibernéticas			
1%	MEDIDA 19 Desarrollo y optimización de las capacidades de gestión de crisis	100%	100%

OBJETIVO 4: Desarrollar las capacidades necesarias para proteger y defender activamente a ciudadanos y empresas			
Peso (LA)	**Línea de acción de Actuación y Medida**	**Peso (MED s/LA)**	**Ejecución**
LÍNEA 4.1. Diseño, implantación y operación de medidas de ciberdefensa activa de menores en Internet			
7%	MEDIDA 20 Fortalecimiento y optimización de las capacidades de prevención	70%	100%
	MEDIDA 21 Fortalecimiento y optimización de las capacidades de defensa activa	15%	100%
	MEDIDA 22 Operación de herramientas y soluciones	15%	100%
LÍNEA 4.2. Diseño, implantación y operación de medidas de ciberdefensa activa de ciudadanos y empresas			
2%	MEDIDA 23 Implementación y desarrollo de soluciones y medidas de defensa activa	100%	100%
LÍNEA 4.3. Avances normativos para la protección de ciudadanos y empresas			
2%	MEDIDA 24 Proposición de modificaciones normativas para la protección de ciudadanos y empresas	100%	100%

OBJETIVO 5: Impulsar la industria española y el I+D+i de ciberseguridad

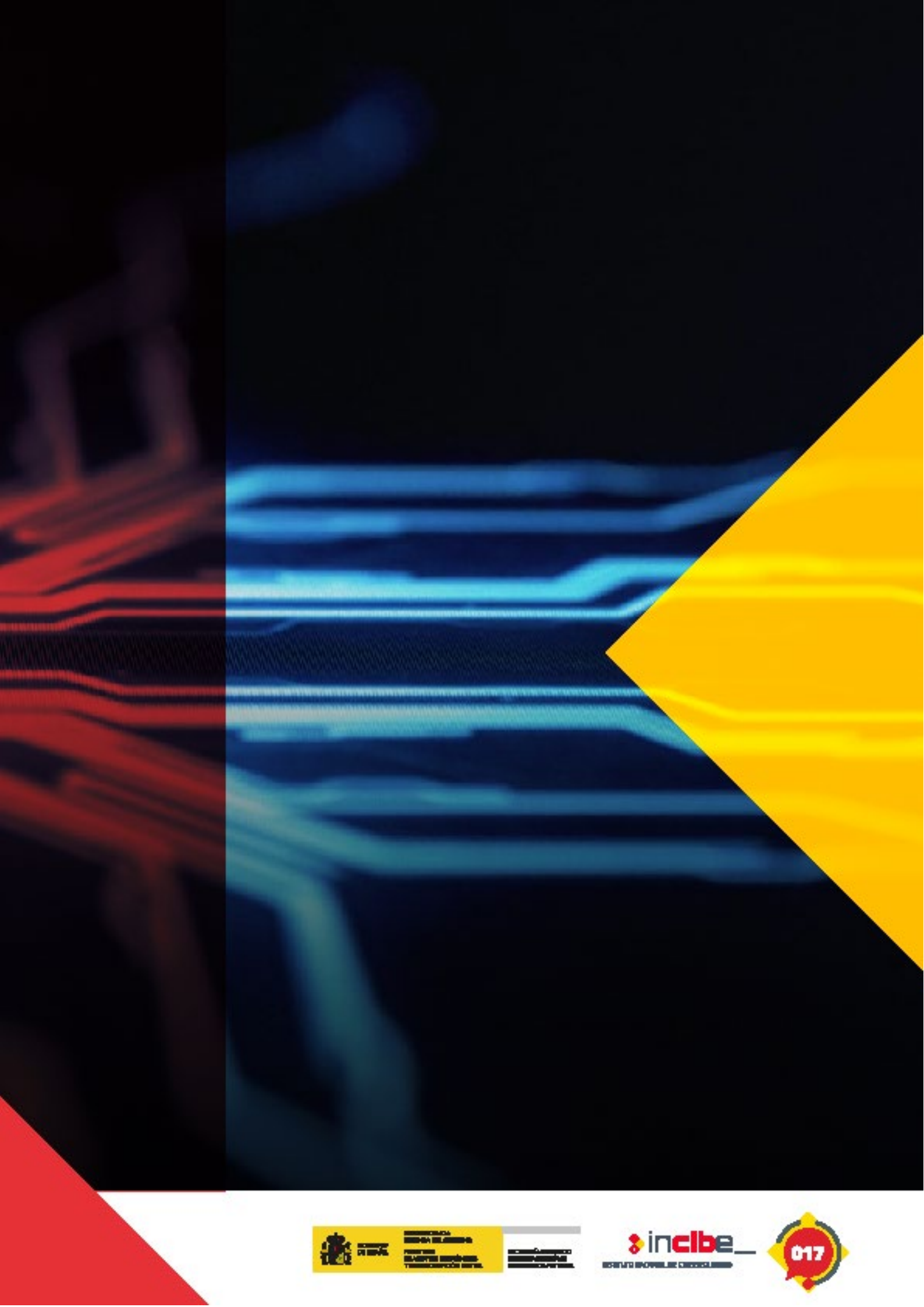
Peso (LA)	Línea de acción de Actuación y Medida	Peso (MED s/LA)	Ejecución
LÍNEA 5.1. Potenciación de la industria española de ciberseguridad			
11%	MEDIDA 25 Impulso al emprendimiento en Ciberseguridad	35%	100%
	MEDIDA 26 Desarrollo y fortalecimiento de la industria de ciberseguridad	40%	98%
	MEDIDA 27 Internacionalización de la industria de ciberseguridad	25%	100%
LÍNEA 5.2. Impulso a la I+D+i española en ciberseguridad			
12%	MEDIDA 28 Fortalecer e incrementar las capacidades de I+D+i	25%	91,60%
	MEDIDA 29 Transformación de la I+D+i en activos de alto valor añadido	50%	100%
	MEDIDA 30 Potenciar la posición española en I+D+i relacionado con la ciberseguridad	25%	98,30%
LÍNEA 5.3. Impulso a la inversión empresarial en ciberseguridad			
1%	MEDIDA 31 Atracción de inversión para el crecimiento y desarrollo de la Industria de Ciberseguridad	100%	100%

OBJETIVO 6: Promover y detectar talento en ciberseguridad

Peso (LA)	Línea de acción de Actuación y Medida	Peso (MED s/LA)	Ejecución
LÍNEA 6.1. Fomento, detección y aprovechamiento del talento en ciberseguridad			
3%	MEDIDA 32 Mejoras las capacidades de empresas para la identificación y desarrollo del talento en ciberseguridad	35%	100%
	MEDIDA 33 Generación e identificación de talento en ciberseguridad	65%	100%
LÍNEA 6.2. Fomento de la capacitación del Talento en ciberseguridad			
3%	MEDIDA 34 Transformación de talento en ciberseguridad	70%	100%
	MEDIDA 35 Fortalecer la cooperación público-privada para la generación y desarrollo del talento en ciberseguridad	30%	100%

OBJETIVO 7: Posicionar INCIBE como referente europeo de ciberseguridad

Peso (LA)	Línea de acción de Actuación y Medida	Peso (MED s/LA)	Ejecución
LÍNEA 7.1. El reconocimiento y posicionamiento de INCIBE como impulsor de la ciberseguridad y la confianza digital			
9%	MEDIDA 36 Posicionamiento de INCIBE como actor de referencia en el ámbito nacional e internacional	65%	100%
	MEDIDA 37 Desarrollo del relacionamiento estratégico de INCIBE	35%	100%
LÍNEA 7.2. Impulso de España como nodo internacional de ciberseguridad			
2%	MEDIDA 38 Impulso del Centro Espejo de Ciberseguridad en España	45%	100%
	MEDIDA 39 Impulso y coordinación de la comunidad de ciberseguridad	55%	100%



España | digital 2026

PLAN ANUAL DE ACTIVIDAD INCIBE 2022

Resultados conseguidos

Financiado por la Unión Europea
NextGenerationEU

Gobierno de España
Vicepresidencia Primera del Gobierno
Ministerio de Asuntos Económicos y Transformación Digital
Secretaría de Estado de Digitalización e Inteligencia Artificial

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. PRESENTACIÓN

Qué es INCIBE

La S.M.E. Instituto Nacional de Ciberseguridad de España (INCIBE), M.P., S.A., sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaria de Estado de Digitalización e Inteligencia Artificial (SEDIA), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital en el sector privado. En particular para los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

Dentro de la actividad del Instituto se encuentra INCIBE-CERT, el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España. En el caso de la gestión de incidentes que afecten a operadores críticos del sector privado, INCIBE-CERT está operado conjuntamente por INCIBE y CNPIC, Centro Nacional de Protección de Infraestructuras y Ciberseguridad del Ministerio del Interior.

Actividad de INCIBE

El desarrollo de la Inteligencia Artificial, el 5G y otras tecnologías habilitadoras están generando una profundización exponencial de la digitalización y su previsible impacto socioeconómico, así como una ampliación de la superficie de riesgo para la seguridad digital. Ampliar o generar capacidades (técnicas y humanas) en ciberseguridad es clave para poder incorporar las oportunidades de la digitalización minimizando sus riesgos asociados.

En este escenario global, el Gobierno de España presentó en julio de 2020 la agenda España Digital 2025, un cuaderno de bitácora para la transformación digital del país que permita optimizar los beneficios socioeconómicos de la digitalización, minimizando sus riesgos asociados. Esta agenda digital se desarrolla a través de 10 ejes estratégicos, siendo el cuarto de ellos la ciberseguridad. INCIBE se alinea su actividad con a esa agenda y con los objetivos y metas que esta persigue, junto al cuerpo estratégico de la Seguridad Nacional referido anteriormente.

Para hacerlo, el Instituto busca contribuir a que el nivel de seguridad digital de ciudadanos y empresas privadas, así como la industria española de ciberseguridad, estén entre los cinco mejores del mundo, orientando sus actividades al desarrollo de 3 ejes estratégicos:

- **Fortalecimiento de la ciberseguridad de ciudadanos, PyMEs y profesionales**. Para que España sea uno de los países más ciberseguros del mundo debe incrementar las capacidades de ciberseguridad.

- **Impulso del ecosistema empresarial del Sector Ciberseguridad.** El segundo eje de actuación se orienta hacia el impulso el ecosistema de ciberseguridad español a través de 3 palancas: (i) el desarrollo de la industria de ciberseguridad, (ii) el impulso de I+D+i, y (iii) la identificación, generación y desarrollo del talento.

- **Impulso de España como nodo internacional en el ámbito de la Ciberseguridad.** A través de este eje, INCIBE trabaja en la consolidación de España como uno de los países con mayor madurez de ciberseguridad en el ámbito europeo y global.

2. PLAN ESTRATÉGICO 2021-2025

El Plan Estratégico de INCIBE para el periodo 2021-2025, bajo el lema '***de miles a millones'***, busca generar un efecto multiplicador en el resultado de actuaciones que desarrolla, y conseguir llegar a más ciudadanos y más empresas con el objetivo de **elevar el nivel de ciberseguridad de la ciudadanía y empresas privadas.** Igualmente, este plan permitirá impulsar la actividad para su posicionamiento como un actor destacado en el ámbito internacional y reafirmar el compromiso de España como referente europeo en el ámbito de la ciberseguridad.

En un entorno cambiante y dinámico como el de la ciberseguridad, este plan de 5 años no define acciones específicas que podrían limitar la capacidad de reacción de INCIBE ante escenarios cambiantes, sino directrices estratégicas a través de líneas de actuación prioritarias. A la finalización del plan, en 2025, INCIBE prestará servicios de alto valor para el conjunto de ecosistemas relacionados con la ciberseguridad. Dichos servicios contribuirán a afianzar la Sociedad de la Información y la Transformación Digital en España; y serán instrumentos eficaces del Gobierno de España para la consecución de sus objetivos.

Misión, Visión y Valores

En el marco de dicho plan, la misión de INCIBE es ser un motor para la transformación digital de la sociedad, protegiendo a ciudadanos, menores y empresas privadas en España y fomentando la industria de la ciberseguridad, la I+D+i y el talento.

Para ello, la visión se focaliza en tres aspectos, 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 y, posicionar INCIBE como referente europeo en el ámbito de la ciberseguridad.

Para poder responder a la misión y visión planteadas, se han definido una serie de valores para INCIBE, que servirán asimismo como principios rectores del diseño del Plan Estratégico, y que serán también referentes durante su desarrollo y ejecución:

- Vocación de servicio público
- Espíritu neutral y colaborativo
- Proactividad y flexibilidad
- Excelencia
- Innovación
- Desempeño responsable y transparente
- Colaboración nacional e internacional

Fundamentos estratégicos y legales

El crecimiento exponencial de la tecnología y la hiperconectividad ofrecen enormes oportunidades de desarrollo económico y social, y nos acercan a un mundo global e interdependiente. Al mismo tiempo, este profundo proceso de digitalización trae consigo nuevas amenazas para la seguridad. Cada desarrollo, cada avance tecnológico, ofrece esta dualidad de riesgo-oportunidad que debe ser abordado. Las amenazas cibernéticas a las que se enfrentan ciudadanos y empresas comparten al menos 3 características clave:

- Carácter evolutivo y cambiante, lo que hace imprescindible un proceso ágil, eficaz y **sostenible** de investigación y formación de las personas e instituciones encargadas de velar por la seguridad digital, y una transferencia de ese conocimiento a ciudadanos, empresas y gobiernos para mantener el ecosistema digital protegido.
- Mayor complejidad de las amenazas e incidentes cibernéticos, así como una mayor sofisticación del ciberdelito y el ciberdelincuente.
- Carácter global y transnacional de las amenazas e incidentes cibernéticos, lo que nos lleva a abordar la cuestión desde una perspectiva de colaboración y cooperación en el ámbito internacional.

El Plan Estratégico se alinea conceptual y temporalmente con España Digital 2025, la agenda para la transformación digital del país en los próximos 5 años. Igualmente este Plan nace en un contexto de pandemia global del que se deriva el Plan de Recuperación, Transformación y Resiliencia de la Economía Española mediante el que se articula el instrumento «Next Generation EU», en el cual INCIBE tomará parte para desarrollar actividades que contribuyan a la recuperación económica y transformación del país.

- Marco Estratégico
  - La **Estrategia Nacional de Ciberseguridad de 2019 (**ENCS19), que es el documento estratégico principal que sirve de base para el presente Plan. Una parte sustancial de los objetivos y de las acciones definidos en la ENCS19 caen directamente dentro de la misión asignada a INCIBE, y por tanto deben inexcusablemente ser contemplados en este Plan.
  - La **Estrategia de Seguridad Nacional de 2017**, que fija unos objetivos generales transversales a todos los ámbitos: la gestión de crisis, la cultura de Seguridad Nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España; y que incorpora a INCIBE como uno de los organismos del Estado para alcanzar los objetivos de dicha estrategia.
  - La **agenda España Digital 2025** del Ministerio de Asuntos Económicos y Transformación Digital.
  - La **Estrategia Nacional contra el Crimen Organizado** y la Delincuencia Grave 2019-2023, entre cuyas prioridades se encuentra la lucha contra el cibercrimen.
- Cuerpo normativo aprobado o incorporado por el Parlamento nacional que influyen directamente en la misión y funciones de INCIBE como los siguientes:

- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148, conocida como Directiva NIS.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de Datos Personales y Garantía de los Derechos Digitales.

Del mismo modo, se tiene en cuenta para este Plan de Actividad el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, para que INCIBE pueda implementar las actuaciones derivadas de este RD. Esta normativa no figura en el Plan Estratégico original porque en el momento de presentación del Plan Estratégico 2021-2025, el RD 43/2021 no estaba vigente.

Destinatarios clave

Las actividades de INCIBE se orientan a destinatarios como ciudadanos, empresas, organismos públicos y otros agentes de interés de todos los sectores y ámbitos que en el desarrollo de sus actividades interactúan con el ámbito de la ciberseguridad y a los que INCIBE se aproxima desde su vocación de servicios público y promotor de la cultura de la ciberseguridad.

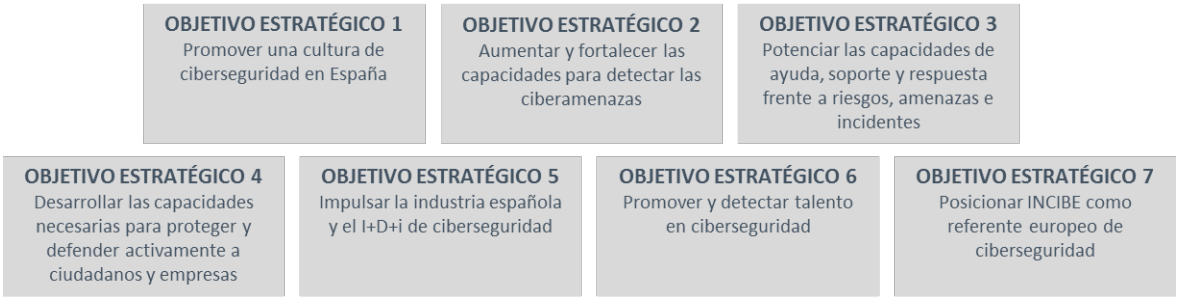
Concretamente, estos destinatarios se subdividen en cuatro grandes grupos:

- Ciudadanos: cualquiera que emplee tecnologías y dispositivos, con especial atención en los menores por ser un colectivo muy vulnerable.
- Empresas: Operadores de Servicios Esenciales, y sectores estratégicos; las grandes, medianas y pequeñas empresas; las microempresas y los autónomos; y la industria de Ciberseguridad en general.
- Organismos Públicos:
  - Secretaría General de Administración Digital (SGAD);
  - Centro Criptológico Nacional (CCN);
  - Departamento de Seguridad Nacional (DSN);
  - Mando Conjunto del Ciberespacio (MCCE);
  - Oficina de Coordinación de Ciberseguridad; y
  - Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

- Otros Agentes de Interés:
  - Otros agentes públicos de ciberseguridad con los que se relaciona INCIBE
  - El entorno académico y de investigación, usuarios de la Red Académica y de Investigación RedIRIS, y tractores de la generación de nuevos productos y servicios de ciberseguridad.
  - Los profesionales de la ciberseguridad, además de los expertos reconocidos.
  - Los jóvenes talentos y otros colectivos, con el objetivo de promocionar el interés por la ciberseguridad y su capacitación.
  - Otros agentes nacionales e internacionales de todos los sectores y ámbitos que en el desarrollo de sus actividades interactúan con el ámbito de la ciberseguridad
  - El propio INCIBE, ya que se acometerán actuaciones para la mejora de la entidad en todos los aspectos.

Objetivos estratégicos

El Plan de Actividad 2022 desarrolla su actividad en el marco de los objetivos estratégicos que figuran en el Plan Estratégico 2021-2025, y que son los siete siguientes:



A continuación se desarrollan los Objetivos y Líneas de Acción, que se asocian de manera correspondiente a las dotaciones presupuestarias previstas y en curso para el período enero-diciembre 2022, completando así el global del Plan en función de la previsión de gasto por parte de INCIBE.

Para que INCIBE desarrolle su Misión, y se pueda acercar hacia su Visión, se establecen los **7 objetivos estratégicos para el período 21-25**:

- **OBJETIVO ESTRATÉGICO 1**. Promover una cultura de ciberseguridad en España.
- **OBJETIVO ESTRATÉGICO 2.** Aumentar y fortalecer las capacidades para detectar las ciberamenazas.
- **OBJETIVO ESTRATÉGICO 3.** Potenciar las capacidades de ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes.
- **OBJETIVO ESTRATÉGICO 4**. Desarrollar las capacidades necesarias para proteger y defender activamente a ciudadanos, menores y empresas.
- **OBJETIVO ESTRATÉGICO 5**. Impulsar la industria española y la I+D+i de ciberseguridad.
- **OBJETIVO ESTRATÉGICO 6**. Promover y detectar talento en ciberseguridad.

- **OBJETIVO ESTRATÉGICO 7**. Posicionar INCIBE como referente europeo de ciberseguridad

Para la consecución de estos objetivos INCIBE llevará a cabo iniciativas y actuaciones que se estructuran en líneas de actuación. En los siguientes apartados se describen los **7 objetivos estratégicos** y las líneas de actuación previstas que permitirán alcanzarlo.

OBJETIVO ESTRATÉGICO 1. Promover una cultura de la Ciberseguridad en España

La primera responsabilidad es generar conciencia acerca de la existencia de esas amenazas y riesgos, y conseguir esa participación imprescindible para construir y desarrollar una cultura de ciberseguridad en colaboración con actores públicos y privados, tanto en el ámbito nacional como internacional, y potenciar mecanismos de concienciación, información y formación.

Esta cultura de ciberseguridad hace referencia al conocimiento, adopción y compromiso sostenible con hábitos saludables y buenas prácticas en el mundo cibernético por parte de ciudadanos, empresas y administración pública. Los espacios de encuentro entre INCIBE y los destinatarios de su misión, o entre empresas, entidades o individuos que pudieran tener características e intereses similares, contribuirán a la consecución de este objetivo. Las líneas de actuación que conducirán a la consecución del objetivo 1 son:

LÍNEA DE ACTUACIÓN 1.1: Promoción de la concienciación y la información

Las actividades pertenecientes a esta línea de actuación buscarán concienciar a ciudadanos y empresas no sólo de que están expuestos, sino de que deben tomar las acciones necesarias para conocer sus riesgos y protegerse. Esta Línea se desarrollará a través de 4 medidas estratégicas:

MEDIDA 1. Fortalecimiento de las capacidades de ciberseguridad de la sociedad

MEDIDA 2. Fortalecimiento de capacidades de ciberseguridad de empresas

MEDIDA 3. Incremento de capacidades de ciberseguridad de "actores intermedios"

MEDIDA 4. Fortalecimiento de Servicios Públicos, Canales y Herramientas para la extensión de la Cultura de Ciberseguridad

LÍNEA DE ACTUACIÓN 1.2: Impulso de la colaboración público-privada y de la RSC

La seguridad digital de ciudadanos y empresas debe ser un compromiso compartido. Bajo esta línea de actuación, INCIBE realizará acciones para impulsar la colaboración público-privada para la extensión de una cultura de ciberseguridad, los servicios de valor añadido y el cumplimiento de su misión.

MEDIDA 5. Desarrollo del Foro Nacional de Ciberseguridad (contribución)

MEDIDA 6. Identificación y Desarrollo de "mecanismos de multiplicación" de los esfuerzos de fortalecimiento

MEDIDA 7. Desarrollo de la Responsabilidad Social Empresarial de INCIBE

LÍNEA DE ACTUACIÓN 1.3: Impulso de la Generación de Conocimiento sobre CS

La generación de conocimiento sobre la realidad de las amenazas y riesgos cibernéticos en diferentes ámbitos, sectores productivos y a nivel nacional e internacional, ofrece una foto amplia de la realidad sobre la que desarrollar la actividad de INCIBE. A través de esta línea de actuación se contribuirá al posicionamiento de INCIBE como un actor destacado y fuente de conocimiento de alto valor sobre ciberseguridad a nivel nacional e internacional.

MEDIDA 8. Desarrollo del Conocimiento de la Ciberseguridad en España

OBJETIVO ESTRATÉGICO 2. Aumentar y fortalecer las capacidades para detectar las ciberamenazas.

La detección de diferentes vectores de ataque de manera proactiva permitirá una alerta temprana adecuada y en algunos casos la detección de posibles intrusiones que no se hayan desplegado o que el usuario no percibe.

Por tanto, INCIBE debe conocer las ciberamenazas, detectar al menos sus potenciales víctimas españolas y los activos españoles comprometidos, y entender cómo actúan, es decir, conocer sus TTP's (Técnicas, Tácticas y Procedimientos) y cuáles son las infraestructuras que usan. La información que se obtenga debe ser accionable, es decir, debe permitir a INCIBE tomar acciones para la prevención y protección de las víctimas potenciales, para su defensa activa o para la mitigación del daño que las ciberamenazas puedan causar.

Las líneas de actuación previstas que conducirán a la consecución del objetivo 2 son:

LÍNEA DE ACTUACIÓN 2.1: Capacidades para la detección

Dentro de esta línea de actuación se desarrollan las acciones dirigidas a crear y operar capacidades que permitan a INCIBE detectar aquello que pueda ser significativo para la seguridad de los españoles frente a las ciberamenazas.

MEDIDA 9. Optimización y desarrollo continuado de las capacidades de detección

LÍNEA DE ACTUACIÓN 2.2: Capacidades para la inteligencia

La detección por sí sola no es suficiente. Los datos que se obtengan deben ser normalizados, relacionados, analizados y enriquecidos a partir de información previa, de contexto y de datos obtenidos de otras fuentes, de forma que sea posible generar conocimiento nuevo a partir de la agregación de múltiples fuentes de detección.

MEDIDA 10. Optimización y desarrollo continuado de las capacidades de inteligencia

MEDIDA 11. Desarrollo de capacidades para la medición del riesgo.

LÍNEA DE ACTUACIÓN 2.3: Explotación de la información

INCIBE debe poder generar valor a partir del conocimiento que obtenga de las dos líneas de actuación anteriores a través de la explotación y diseminación de la información. Esta línea de actuación recogerá todas las acciones orientadas a esta generación de valor a partir de la inteligencia.

MEDIDA 12. Desarrollo y fortalecimiento de las capacidades para la accionabilidad de información de ciberinteligencia

MEDIDA 13. Difusión de la información de ciberinteligencia para la accionabilidad de terceros.

OBJETIVO ESTRATÉGICO 3. Potenciar las capacidades de ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes.

Cuando un ciudadano o una empresa contactan con INCIBE porque percibe que puede tener un problema de ciberseguridad, debe recibir un servicio público de ciberseguridad integrado, de calidad y de fácil acceso, y que sea un estímulo a la demanda de los servicios que ofrece el sector empresarial de la ciberseguridad.

Para dar respuesta a estas necesidades de ciudadanos y empresas, INCIBE trabajará no sólo en canales electrónicos para recibir las peticiones de ayuda, sino también en medios automatizados para diagnosticar y responder cuando ello sea posible.

Las líneas de actuación que conducirán a la consecución del objetivo 3 son aquellas que permitan generar:

LÍNEA DE ACTUACIÓN 3.1: Capacidades para la ayuda, soporte y respuesta

Las acciones que se encuentran dentro de esta línea de actuación son aquellas dirigidas a que INCIBE preste un servicio de ayuda, soporte y respuesta ágil, de calidad y de fácil acceso.

MEDIDA 14. Fortalecimiento de las capacidades de soporte y respuesta a incidentes

MEDIDA 15. Fortalecimiento de los servicios de soporte y respuesta a incidentes

LÍNEA DE ACTUACIÓN 3.2: Servicios especializados para empresas

A través de esta línea de actuación se desarrollarán servicios para protección en el ciberespacio para las empresas del sector privado. Deben establecerse los mecanismos que aseguren que INCIBE está puntualmente informado ante cualquier incidente que pueda afectar a estas empresas, de forma que se puedan tomar acciones lo antes posible.

MEDIDA 16. Fortalecimiento de las capacidades de respuesta de empresas y pymes ante incidentes de Ciberseguridad

MEDIDA 17. Fortalecimiento de las capacidades de resiliencia y recuperación de los Operadores de Servicios Críticos y Proveedores de Servicios Digitales

MEDIDA 18. Protección de activos de empresas

LÍNEA DE ACTUACIÓN 3.3: Capacidades para la gestión de crisis cibernéticas

Inevitablemente, un incidente o conjunto de incidentes, pueden generar una situación catalogada como crisis. INCIBE, dentro del alcance de las responsabilidades que se le asignen en el Sistema de Seguridad Nacional, debe estar preparado para asumir la parte que le corresponda en la gestión de las crisis. Las actuaciones que preparen a INCIBE en este sentido, deberán ser recogidas en esta línea de actuación.

MEDIDA 19. Desarrollo y optimización de las capacidades de gestión de crisis

OBJETIVO ESTRATÉGICO 4. Desarrollar las capacidades necesarias para proteger y defender activamente a ciudadanos y empresas.

A través de este objetivo se desarrollarán iniciativas que desde el Estado promuevan una protección y prevención activas ante criminales cada vez más profesionalizados y especializados. Por tanto, desde INCIBE, se desarrollarán las líneas de actuación que busquen proteger el ciberespacio para defender activamente a ciudadanos y empresas. Estas actuaciones necesitarán de la cooperación público-privada, y para conseguirla, en muchos casos se requerirá de modificaciones normativas. Las líneas de actuación que conducirán a la consecución del objetivo 4 son:

LÍNEA DE ACTUACIÓN 4.1: Diseño, implantación y operación de medidas de ciberdefensa activa de menores en Internet

A través de esta línea de actuación se desarrollarán acciones específicas orientadas a la prevención y protección de los menores en el ciberespacio, al ser precisamente un colectivo especialmente sensible y vulnerable a las amenazas en Internet.

MEDIDA 20. Fortalecimiento y optimización de las capacidades de prevención

MEDIDA 21 Fortalecimiento y optimización de las capacidades de defensa activa

MEDIDA 22. Operación de herramientas y soluciones

LÍNEA DE ACTUACIÓN 4.2: Diseño, implantación y operación de medidas de ciberdefensa activa de ciudadanos y empresas

Esta línea de actuación incorporará medidas específicas de defensa activa para ciudadanos y empresas. Serán públicos de especial interés las medianas empresas, pymes

y autónomos que por sus características, recursos y tamaño, en muchas ocasiones no pueden contar con las capacidades de grandes empresas para mejorar su protección en el mundo digital.

MEDIDA 23. Implementación y desarrollo de soluciones y medidas de defensa activa de ciudadanos y empresas

LÍNEA DE ACTUACIÓN 4.3: Avances normativos para la protección de ciudadanos y, empresas

Como ya prevé la propia ENCS19 en su Línea de Actividad 4 - Medida 5, aunque INCIBE pueda proponer la implantación de medidas de ciberdefensa activa, la mayor parte de ellas requieren de la colaboración de empresas privadas o de modificaciones normativas. Todas las actuaciones y propuestas en este sentido, se desarrollarán bajo esta línea de actuación.

MEDIDA 24. Proposición de modificaciones normativas para la protección de ciudadanos y empresas

OBJETIVO ESTRATÉGICO 5. Impulsar la industria española y el I+D+i de ciberseguridad

Para afrontar los desafíos que plantea la ciberseguridad, España debe contar con los recursos técnicos y humanos necesarios y la capacitación adecuada para cubrir las exigencias de la ciberseguridad nacional, lo cual además es un habilitador clave para una economía que quiera desarrollar el crecimiento de su sector de ciberseguridad. De igual modo, es necesario el desarrollo de una política clara de impulso de la I+D+i en el sector de la ciberseguridad. A través de este objetivo se impulsará esta palanca clave de crecimiento.

Las líneas de actuación que conducirán a la consecución del objetivo 5 son aquellas que permitan generar:

LÍNEA DE ACTUACIÓN 5.1: Potenciación de la industria española de ciberseguridad

La ciberseguridad en un país no es posible sin una adecuada oferta de productos y servicios de ciberseguridad. Por eso a través de esta línea de actuación se impulsará la industria del sector, su competitividad y su internacionalización.

MEDIDA 25. Impulso al emprendimiento en ciberseguridad

MEDIDA 26. Desarrollo y fortalecimiento de la industria de ciberseguridad

MEDIDA 27. Internacionalización de la industria de ciberseguridad

LÍNEA DE ACTUACIÓN 5.2: Impulso a la I+D+i española en ciberseguridad

La ciberseguridad es un mundo que cambia y evoluciona muy rápido. Con la explosión de la transformación digital, y la aparición de nuevos paradigmas tecnológicos, el panorama de ciberamenazas y de empresas capaces de prestar servicios para hacerles frente, evoluciona de forma constante.

MEDIDA 28. Fortalecer e incrementar las capacidades de I+D+i

MEDIDA 29. Transformación de la I+D+i en activos de alto valor añadido

MEDIDA 30. Potenciar la posición española en I+D+i relacionado con la ciberseguridad

LÍNEA DE ACTUACIÓN 5.3: Impulso a la Inversión Empresarial en Ciberseguridad

El crecimiento y desarrollo de la Industria de Ciberseguridad española estará vinculado a su capacidad de tracción de capital para la puesta en marcha de iniciativas.

MEDIDA 31. Atracción de inversión para el crecimiento y desarrollo de la industria de Ciberseguridad

OBJETIVO ESTRATÉGICO 6. Promover y detectar talento en ciberseguridad.

Existe una creciente demanda a nivel global de profesionales de la seguridad digital como consecuencia del desarrollo de la economía digital y, en general, una digitalización cada vez más profunda y presente en la vida cotidiana de ciudadanos, empresas y Administraciones Públicas. Esta realidad está elevando la demanda de servicios de ciberseguridad que garanticen, en el mundo digital, los estándares de seguridad y confianza del mundo físico. INCIBE debe asumir un rol de dinamizador activo para la detección, promoción y desarrollo del talento. Para impulsar este objetivo 6, INCIBE prevé desarrollar estas líneas de actuación:

LÍNEA DE ACTUACIÓN 6.1: Fomento, detección y aprovechamiento del talento en ciberseguridad

Se debe fomentar la identificación y promoción del talento que demanda el mercado laboral actual y futuro. Para ello INCIBE podrá realizar actuaciones que favorezcan esta identificación y promoción, de los perfiles y las competencias en ciberseguridad necesarias.

MEDIDA 32. Mejoras las capacidades de empresas para la identificación y desarrollo del talento en ciberseguridad

MEDIDA 33. Generación e identificación de talento en ciberseguridad

LÍNEA DE ACTUACIÓN 6.2: Fomento de la capacitación del Talento en ciberseguridad

Se debe fomentar la capacitación en ciberseguridad de los profesionales, adecuada a la demanda del mercado laboral. INCIBE podrá ofrecer, y fomentará la generación por parte de otros agentes, de contenidos actuales, atractivos y adaptados a las necesidades de cada público, asegurando que dichos contenidos llegan a sus destinatarios y son adecuadamente aprovechados.

MEDIDA 34. Transformación de talento en ciberseguridad

MEDIDA 35. Fortalecer la cooperación público-privada para la generación y desarrollo del talento en ciberseguridad

OBJETIVO ESTRATÉGICO 7. Posicionar INCIBE como referente europeo de ciberseguridad.

Con este séptimo objetivo se desarrollarán las actuaciones necesarias para que INCIBE evolucione y se anticipe a las necesidades que permitan cumplir los objetivos estratégicos anteriores, sobre las bases de la mejora continua, el desarrollo profesional y la innovación interna. Al mismo tiempo, bajo este objetivo se trabajara en el seguimiento y control de su actividad, que redunde en una extracción y reutilización del conocimiento generado internamente.

Las líneas de actuación que conducirán a la consecución de este objetivo 7 son:

LÍNEA DE ACTUACIÓN 7.1: El reconocimiento y posicionamiento de INCIBE como impulsor de la ciberseguridad y la confianza digital

Para el cumplimiento de su misión como un actor clave en la ciberseguridad de ciudadanos y empresas en España, INCIBE implementará las acciones necesarias que contribuyan a asegurar la posición de España en los foros nacionales e internacionales relevantes, incrementar la cooperación con otros actores clave y a asegurar la transparencia

MEDIDA 36. Posicionamiento de INCIBE como actor de referencia en el ámbito nacional e internacional

MEDIDA 37. Desarrollo del relacionamiento estratégico de INCIBE

LÍNEA DE ACTUACIÓN 7.2: Impulso de España como nodo internacional de la ciberseguridad

A través de esta Línea de Actuación, INCIBE desarrollará las iniciativas necesarias para consolidar a España como nodo internacional de la ciberseguridad.

MEDIDA 38. Impulso del Centro Espejo de Ciberseguridad en España

MEDIDA 39. Impulso y coordinación de la comunidad de ciberseguridad

3. RESULTADOS CONSEGUIDOS

A continuación, se incorpora el marco de resultados finalmente conseguidos del plan anual 2022. Los indicadores y subindicadores configuran el plan de trabajo vinculados a las medidas, y se identifican los resultados finalmente alcanzados para el presente ejercicio:

OBJETIVO 1: Promover una cultura de ciberseguridad en España			
Peso (LA)	**Línea de acción de Actuación y Medida**	**Peso (MED s/LA)**	**Ejecución**
LÍNEA 1.1. Promoción de la concienciación y la información			
10%	MEDIDA 1 Fortalecimiento e las capacidades de ciberseguridad de la Sociedad	30%	100%
	MEDIDA 2 Fortalecimiento de capacidades de empresas	35%	100%
	MEDIDA 3 Incremento de capacidades de ciberseguridad de "actores intermedios"	15%	100%
	MEDIDA 4 Fortalecimiento de Servicios Públicos, Canales y Herramientas para la extensión de la Cultura de Ciberseguridad	20%	100%
LÍNEA 1.2. Impulso de la colaboración público-privada y de la RSC			
8%	MEDIDA 5 Desarrollo del Foro Nacional de Ciberseguridad (contribución)	40%	100%
	MEDIDA 6 Identificación y Desarrollo de "mecanismos de multiplicación" de los esfuerzos de fortalecimiento	50%	100%
	MEDIDA 7 Desarrollo de la Responsabilidad Social Empresarial de INCIBE	10%	100%
LÍNEA 1.3. Impulso de la Generación de Conocimiento sobre Ciberseguridad			
2%	MEDIDA 8 Desarrollo del Conocimiento de la Ciberseguridad en España	100%	100%

OBJETIVO 2: Aumentar y fortalecer las capacidades para detectar las ciberamenazas

Peso (LA)	Línea de acción de Actuación y Medida	Peso (MED s/LA)	Ejecución
LÍNEA 2.1. Capacidades para la Detección			
6%	MEDIDA 9 Optimización y desarrollo continuado de las capacidades de detección	100%	100%
LÍNEA 2.2. Capacidades para la Inteligencia			
3%	MEDIDA 10 Optimización y desarrollo continuado de las capacidades de inteligencia	60%	100%
	MEDIDA 11 Desarrollo de capacidades para la medición del riesgo	40%	100%
LÍNEA 2.3. Explotación de la Información			
3%	MEDIDA 12 Desarrollo y fortalecimiento de las capacidades para la accionabilidad de información de ciber-inteligencia	70%	100%
	MEDIDA 13 Difusión de la información de ciber-inteligencia para la accionabilidad de terceros	30%	100%

OBJETIVO 3: Potenciar las capacidades de ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes

Peso (LA)	Línea de acción de Actuación y Medida	Peso (MEDs/LA)	Ejecución
LÍNEA 3.1. Capacidades para la ayuda, soporte y respuesta			
8%	MEDIDA 14 Fortalecimiento de las capacidades de soporte y respuesta a incidentes	50%	100%
	MEDIDA 15 Fortalecimiento de los servicios de soporte y respuesta a incidentes	50%	100%
LÍNEA 3.2. Servicios especializados para empresas			
7%	MEDIDA 16 Fortalecimiento de las capacidades de respuesta de empresas y pymes ante incidentes de ciberseguridad	25%	100%
	MEDIDA 17 Fortalecimiento de las capacidades de resiliencia y recuperación de los Operadores de Servicios Críticos y Proveedores de Servicios Digitales	50%	100%
	MEDIDA 18 Protección de activos de empresas	25%	100%
LÍNEA 3.3. Capacidades para la gestión de crisis cibernéticas			
1%	MEDIDA 19 Desarrollo y optimización de las capacidades de gestión de crisis	100%	100%

OBJETIVO 4: Desarrollar las capacidades necesarias para proteger y defender activamente a ciudadanos y empresas			
Peso (LA)	**Línea de acción de Actuación y Medida**	**Peso (MED s/LA)**	**Ejecución**
LÍNEA 4.1. Diseño, implantación y operación de medidas de ciberdefensa activa de menores en Internet			
7%	MEDIDA 20 Fortalecimiento y optimización de las capacidades de prevención	70%	100%
	MEDIDA 21 Fortalecimiento y optimización de las capacidades de defensa activa	15%	100%
	MEDIDA 22 Operación de herramientas y soluciones	15%	100%
LÍNEA 4.2. Diseño, implantación y operación de medidas de ciberdefensa activa de ciudadanos y empresas			
2%	MEDIDA 23 Implementación y desarrollo de soluciones y medidas de defensa activa	100%	100%
LÍNEA 4.3. Avances normativos para la protección de ciudadanos y empresas			
2%	MEDIDA 24 Proposición de modificaciones normativas para la protección de ciudadanos y empresas	100%	100%

OBJETIVO 5: Impulsar la industria española y el I+D+i de ciberseguridad

Peso (LA)	Línea de acción de Actuación y Medida	Peso (MED s/LA)	Ejecución
LÍNEA 5.1. Potenciación de la industria española de ciberseguridad			
11%	MEDIDA 25 Impulso al emprendimiento en Ciberseguridad	35%	100%
	MEDIDA 26 Desarrollo y fortalecimiento de la industria de ciberseguridad	40%	100%
	MEDIDA 27 Internacionalización de la industria de ciberseguridad	25%	100%
LÍNEA 5.2. Impulso a la I+D+i española en ciberseguridad			
12%	MEDIDA 28 Fortalecer e incrementar las capacidades de I+D+i	25%	100%
	MEDIDA 29 Transformación de la I+D+i en activos de alto valor añadido	50%	100%
	MEDIDA 30 Potenciar la posición española en I+D+i relacionado con la ciberseguridad	25%	100%
LÍNEA 5.3. Impulso a la inversión empresarial en ciberseguridad			
1%	MEDIDA 31 Atracción de inversión para el crecimiento y desarrollo de la Industria de Ciberseguridad	100%	100%

OBJETIVO 6: Promover y detectar talento en ciberseguridad			
Peso (LA)	**Línea de acción de Actuación y Medida**	**Peso (MED s/LA)**	**Ejecución**
LÍNEA 6.1. Fomento, detección y aprovechamiento del talento en ciberseguridad			
3%	MEDIDA 32 Mejoras las capacidades de empresas para la identificación y desarrollo del talento en ciberseguridad	35%	100%
	MEDIDA 33 Generación e identificación de talento en ciberseguridad	65%	60%
LÍNEA 6.2. Fomento de la capacitación del Talento en ciberseguridad			
3%	MEDIDA 34 Transformación de talento en ciberseguridad	70%	60%
	MEDIDA 35 Fortalecer la cooperación público-privada para la generación y desarrollo del talento en ciberseguridad	30%	100%

OBJETIVO 7: Posicionar INCIBE como referente europeo de ciberseguridad			
Peso (LA)	**Línea de acción de Actuación y Medida**	**Peso (MED s/LA)**	**Ejecución**
LÍNEA 7.1. El reconocimiento y posicionamiento de INCIBE como impulsor de la ciberseguridad y la confianza digital			
9%	MEDIDA 36 Posicionamiento de INCIBE como actor de referencia en el ámbito nacional e internacional	65%	100%
	MEDIDA 37 Desarrollo del relacionamiento estratégico de INCIBE	35%	100%
LÍNEA 7.2. Impulso de España como nodo internacional de ciberseguridad			
2%	MEDIDA 38 Impulso del Centro Espejo de Ciberseguridad en España	45%	100%
	MEDIDA 39 Impulso y coordinación de la comunidad de ciberseguridad	55%	100%