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.

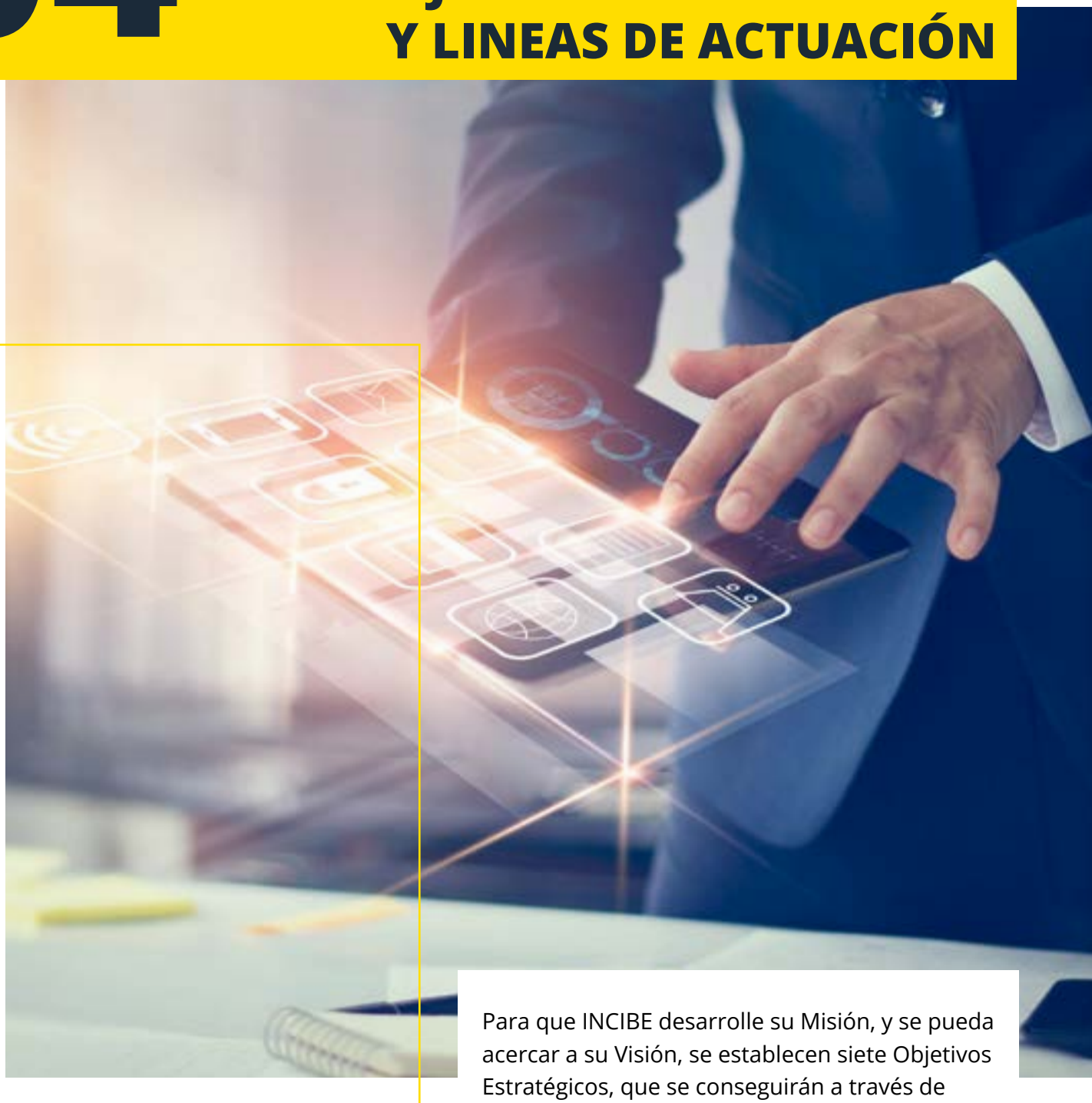
ORGANISMOS PÚBLICOS:

- 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

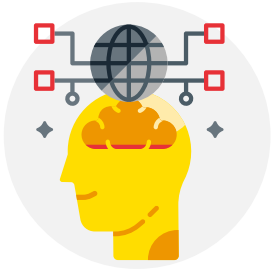
La detección de vectores de ataque de manera proactiva permitirá una alerta temprana adecuada. INCIBE debe conocer las ciberamenazas, entender cómo actúan, y detectar potenciales víctimas para protegerlas, mitigando daño que las ciberamenazas puedan causar. Este objetivo pretende que INCIBE fortalezca 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

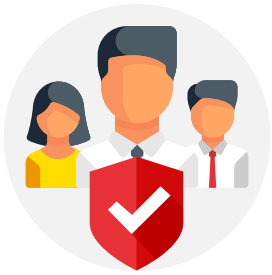
Diseño, implantación y operación de medidas de ciberdefensa activa de menores en Internet

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.

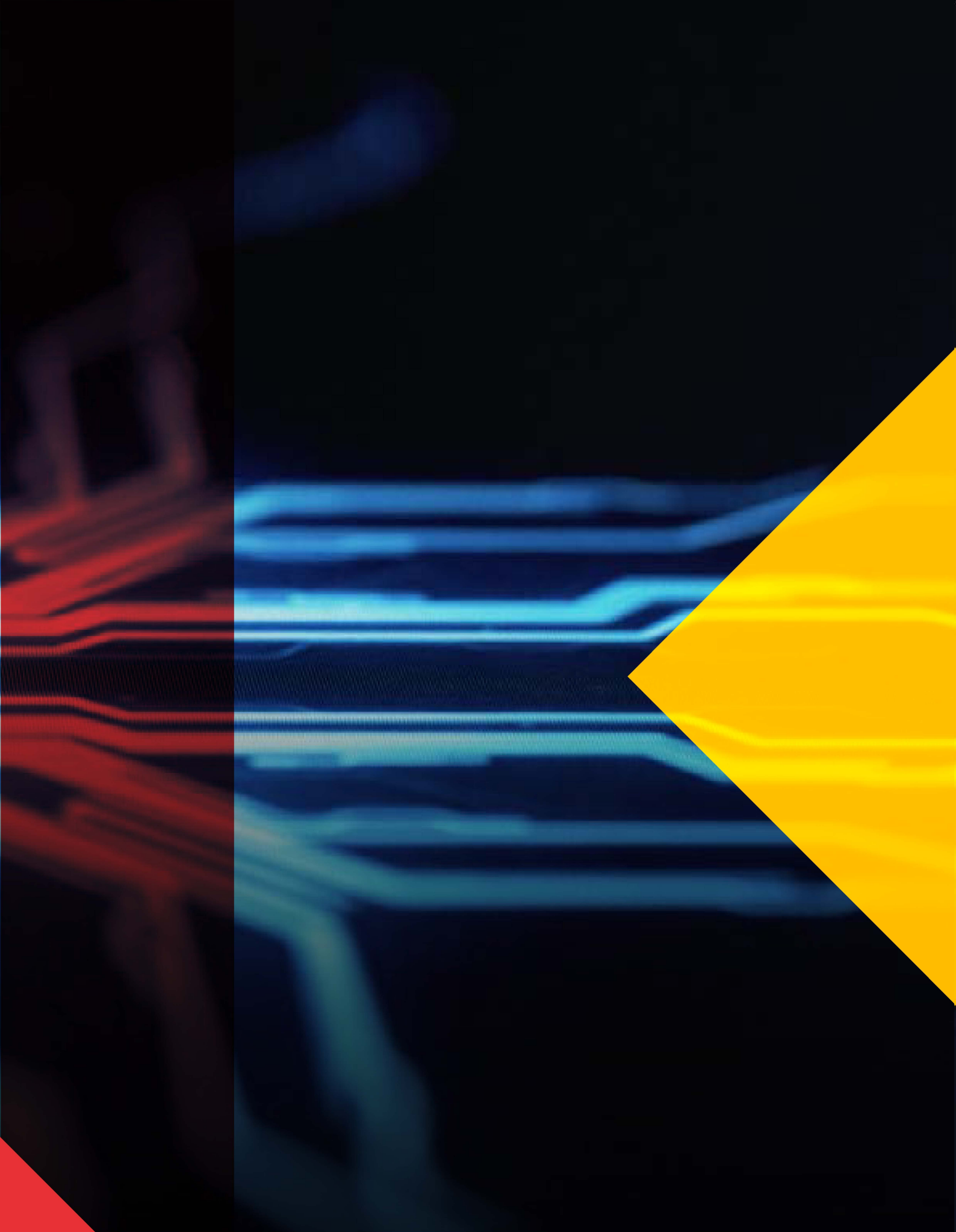
MEDIDA 39. Impulso y coordinación de la comunidad de ciberseguridad.

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