PLAN ANUAL DE ACTIVIDAD INCIBE 2022

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

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 informafición 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. CONTRIBUCIÓN A LAS METAS 2025

El Plan Estratégico incorpora metas de cumplimiento para los 7 objetivos estratégicos que permitirán evaluar de manera global el impacto de la estrategia. Durante 2021 se diseñaran las líneas de base así como los mecanismos para la medición de estas metas o KGI (Key Goal Indicator).

LÍNEA DE ACTUACIÓN		META 2025
1.1	Promoción de la concienciación y la información	**Incremento del 20%** de las capacidades de ciberseguridad de la Sociedad tomando como referencia las líneas base que se establecerán en el primer año del plan.
1.2	Impulso de la colaboración público-privada y de la RSC	**10 Iniciativas Público Privadas** de colaboración a través del Foro Nacional de Ciberseguridad
1.3	Impulso de la Generación de Conocimiento sobre Ciberseguridad	Establecimiento de **Líneas de Base** (2021) e Incremento generación de **productos de conocimiento: +20%**
2.1	Capacidades para la detección	**Incremento del 20%** de las capacidades de detección tomando como referencia las líneas base que se establecerán en el primer año del plan.
2.2	Capacidades para la inteligencia	**Incremento del 20%** de las capacidades para la medición del riesgo tomando como referencia las líneas base que se establecerán en el primer año del plan.
2.3	Explotación de la información	**20 acuerdos difusión de información** de ciberinteligencia para la accionabilidad de terceros
3.1	Capacidades para la ayuda, soporte y respuesta	Incremento de capacidad mensual de la Línea de Ayuda en Ciberseguridad 017 **Nº Llamadas: 20.000** **Nº Incidentes: 15.000**
3.2	Servicios especializados para empresas	**Incremento del 20%** de los servicios especializados y/o herramientas desarrolladas tomando como referencia las líneas base que se establecerán en el primer año del plan.

3.3	Capacidades para la gestión de crisis cibernéticas	**Incremento del 20%** de las capacidades de gestión de crisis tomando como referencia las líneas base que se establecerán en el primer año del plan.
4.1	Diseño, implantación y operación de medidas de ciberdefensa activa de menores en Internet	**Incremento del 20%** de las medidas de ciberdefensa activa para menores tomando como referencia las líneas base que se establecerán en el primer año del plan.
4.2	Diseño, implantación y operación de medidas de ciberdefensa activa de ciudadanos y empresas	**Incremento del 20%** de las medidas de ciberdefensa activa para ciudadanos y empresas tomando como referencia las líneas base que se establecerán en el primer año del plan.
4.3	Avances normativos para la protección de ciudadanos y empresas	N.A.
5.1	**Potenciación de la industria española de ciberseguridad**	**Impulso para la creación de 800** Empleos en Ciberseguridad
5.2	Impulso a la I+D+i española en ciberseguridad	Desarrollo de **8 Programas de Compra Pública Innovadora**
5.3	Impulso a la inversión empresarial en ciberseguridad	Desarrollo de **5 Programas de Atracción de Inversión a la Industria de CS**
6.1	Fomento, detección y aprovechamiento del talento en ciberseguridad	Identificación y generación de **15.000 profesionales de ciberseguridad**
6.2	Fomento de la capacitación del Talento en ciberseguridad	Transformación de **5.000 profesionales de ciberseguridad**, provenientes de otros sectores productivos
7.1	El reconocimiento y posicionamiento de INCIBE como impulsor de la ciberseguridad y la confianza digital	**Incrementar la cooperación** con entidades nacionales e internacionales de ciberseguridad: **+25%**
7.2	Impulso de España como nodo internacional de ciberseguridad	Crear una comunidad de ciberseguridad con **100 Empresas**

4. OBJETIVOS Y GRADO DE CUMPLIMIENTO

El presente Plan Anual incorpora un plan de trabajo que desarrolla las 39 medidas del plan estratégico. En la siguiente tabla se desarrolla la actividad que se pondrá en marcha con una de las medidas, su objetivo y contribución al cumplimiento de las líneas de acción y los objetivos

Para cada medida se ha incorporad un indicador de la misma, que se desarrolla en subindicadores o componentes para cada una de las tareas asignadas, a las que se le otorga un grado de cumplimiento para 2021 con metas objetivo, aceptable y mínimas. El grado de cumplimiento del plan anual estará por tanto vinculado a estos indicadores. El detalla de los mismos se encuentra en el anexo de "Marco de Resultados" de este documento.

Objetivo	Linea de actuación		Medida		Descripción y Objeto de la Medida
Promover una cultura de ciberseguridad en España	1.1.	Promoción de la concienciación y la información	1.1.1.	Fortalecimiento de las capacidades de ciberseguridad de la Sociedad	Incrementar las capacidades de ciberseguridad de los ciudadanos, con especial atención a los menores al ser un público de significativamente vulnerable.
			1.1.2	Fortalecimiento de capacidades de empresas	Trabajar sobre las capacidades de ciberseguridad de las empresas españolas, con especial atención a las medianas y pequeñas empresas, y a los profesionales y autónomos (que disponen de menos recursos)
			1.1.3	Incremento de capacidades de ciberseguridad de "actores intermedios"	Aumentar la capilaridad de las actuaciones a través de agentes intermedios (organizaciones públicas o privadas, entidades asociativas de diferentes ámbitos, o ciudadanos colaboradores), que permitirán obtener un efecto multiplicador. Incrementar las capacidades de estos actores intermedios.
			1.1.4	Fortalecimiento de Servicios Públicos, Canales y Herramientas para la extensión de la Cultura de Ciberseguridad	Consolidar servicios y herramientas para la extensión de la cultura de la ciberseguridad. Estos recursos estarán alineados con las actuaciones de fortalecimiento de capacidades de ciberseguridad que desarrolla INCIBE.

	1.2.	Impulso de la colaboración público-privada y de la RSC	1.2.1	Desarrollo del Foro Nacional de Ciberseguridad (contribución)	Fomentar, a través del FNC, la cooperación público-privada en la búsqueda de sinergias que redundan en una mayor protección para ciudadanos, empresas y gobierno en el ciberespacio.
			1.2.2.	Identificación y Desarrollo de "mecanismos de multiplicación" de los esfuerzos de fortalecimiento	Desarrollar los mecanismos de multiplicación de las actuaciones y programas de INCIBE, a través de la colaboración público-privada, más allá de las actuaciones que se desarrollen en el marco del FNC.
			1.2.3	Desarrollo de la Responsabilidad Social Empresarial de INCIBE	Activar las acciones de Responsabilidad Social Empresarial de INCIBE, que además estarán alineadas con las actuaciones y compromisos de España en materia de objetivos 2030.
	1.3.	Impulso de la Generación de Conocimiento sobre Ciberseguridad	1.3.1.	Desarrollo del Conocimiento de la Ciberseguridad en España	Generar conocimiento profundo de la ciberseguridad en España, y transformar ese conocimiento en líneas de trabajo para mejorar aspectos clave. Apoyar la investigación sobre ciberseguridad en sectores estratégicos de la industria, o colectivos vulnerables.
Aumentar y fortalecer las capacidades para detectar las ciberamenazas	2.1.	Capacidades para la detección	2.1.1.	Optimización y desarrollo continuado de las capacidades de detección	Ampliar de manera continuada las capacidades para la detección de amenazas, sistemas expuestos, sistemas comprometidos y eventos de ciberseguridad relevantes, y su alineamiento con las necesidades de los servicios a los públicos objetivo.
	2.2.	Capacidades para la inteligencia	2.2.1.	Optimización y desarrollo continuado de las capacidades de inteligencia	Mejorar las capacidades de inteligencia de INCIBE, así como la implementación de las herramientas necesarias para la consecución de este objetivo.
			2.2.2.	Desarrollo de capacidades para la medición del riesgo	Desarrollar herramientas o soluciones que permitan evaluar y medir el riesgo cibernético, segmentado por sectores de interés.
	2.3.	Explotación de la información	2.3.1.	Desarrollo y fortalecimiento de las capacidades para la accionabilidad de informafición de ciberinteligencia	Transformar en acción toda la información recabada en la línea de actuación anterior, y por lo tanto, permitir la toma de decisiones para la mejora de la protección de los públicos objetivo.
			2.3.2.	Difusión de la información de ciberinteligencia para la accionabilidad de terceros	Uso por terceros de la información de ciberinteligencia obtenida por INCIBE. Se explotará la información de ciberseguridad disponible en los servicios existentes o nuevos, que aporten valor a los públicos objetivo.

Potenciar las capacidades de ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes	3.1.	Capacidades para la ayuda, soporte y respuesta	3.1.1.	Fortalecimiento de las capacidades de soporte y respuesta a incidentes	Aumentar las capacidades de ayuda, soporte y respuesta, coordinando 017, buzones de consulta y servicios de respuesta a incidentes. Incorporar las capacidades necesarias por la normativa nacional o europea y ofrecer apoyo técnico a las FCSE.
			3.1.2.	Fortalecimiento de los servicios de soporte y respuesta a incidentes	Mejorar los servicios para dar respuesta al incremento de consultas, incidentes. Ampliar y reforzar el número las capacidades de los diferentes niveles de gestión de incidentes.
	3.2.	Servicios especializados para empresas	3.2.1.	Fortalecimiento de las capacidades de respuesta de empresas y pymes ante incidentes de ciberseguridad	Diseñar y activar servicios para el fortalecimiento de las capacidades de respuesta de empresas ante incidentes de Ciberseguridad, todos ellos dirigidos al ámbito de actuación de empresas en general (entidades estratégicas, entidades de interés, etc.).
			3.2.2.	Fortalecimiento de las capacidades de resiliencia y recuperación de los Operadores de Servicios Críticos y Proveedores de Servicios Digitales	Diseñar y activar servicios, herramientas o actuaciones que sirvan para construcción y fortalecimiento de capacidades de resiliencia y recuperación, específicamente para el ámbito de los operadores de Servicios Críticos y Proveedores de Servicios Digitales.
			3.2.3.	Protección de activos de empresas	Diseñar y activar servicios para facilitar mayor protección de los activos tecnológicos, en el ámbito de actuación de empresas en general (entidades estratégicas, entidades de interés, etc.) a que INCIBE presta servicio.
	3.3.	Capacidades para la gestión de crisis cibernéticas	3.3.1.	Desarrollo y optimización de las capacidades de gestión de crisis	Consolidar el procedimiento de gestión de crisis con recursos propios disponibles para poder respuesta y soporte a terceros. Realizar simulaciones y entrenar los diferentes roles y responsabilidades en situaciones de crisis simuladas.
Desarrollar las capacidades necesarias para proteger y defender activamente a ciudadanos y empresas	4.1.	Diseño, implantación y operación de medidas de ciberdefensa activa de menores en Internet	4.1.1.	Fortalecimiento y optimización de las capacidades de prevención	Trabajar en el fortalecimiento de capacidades de prevención de riesgos cibernéticos específicamente orientados a menores.
			4.1.2.	Fortalecimiento y optimización de las capacidades de defensa activa	Desarrollar las acciones de ciberdefensa activa para menores por parte de INCIBE, no solo centrados en medidas de autoprotección que estos puedan tomar para protegerse en el ciberespacio
			4.1.3.	Operación de herramientas y soluciones	Desarrollar herramientas específicas y soluciones de INCIBE para el cumplimiento de las anteriormente señaladas.

	4.2.	Diseño, implantación y operación de medidas de ciberdefensa activa de ciudadanos y empresas	4.2.1.	Implementación y desarrollo de soluciones y medidas de defensa activa	Potenciar la defensa activa para de manera general para ciudadanos y empresas, alineándose con el resto de actuaciones similares por otras entidades.
	4.3.	Avances normativos para la protección de ciudadanos y empresas	4.3.1.	Proposición de modificaciones normativas para la protección de ciudadanos y empresas	Realizar cualquier propuesta de modificación normativa o reglamentaria que permita el desarrollo de las actuaciones del objetivo 4.
Impulsar la industria española y la I+D+i de ciberseguridad	5.1.	Potenciación de la industria española de ciberseguridad	5.1.1.	Impulso al emprendimiento en Ciberseguridad	Desarrollar las iniciativas, actuaciones y programas necesarios para el incremento de la iniciativa empresarial en ciberseguridad.
			5.1.2.	Desarrollo y fortalecimiento de la industria de ciberseguridad	Fomentar la industria existente, a través del conjunto de acciones destinadas al desarrollo de la industria española actual. Esta medida desarrollará las iniciativas, actuaciones y programas necesarios
			5.1.3.	Internacionalización de la industria de ciberseguridad	Apoyar el crecimiento en otros mercados, tanto europeos como extracomunitarios, de la industria española. Desarrollar las actuaciones para el incremento de la cuota de mercado internacional de nuestra industria.
	5.2.	Impulso a la I+D+i española en ciberseguridad	5.2.1.	Fortalecer e incrementar las capacidades de I+D+i	Incorporar las actividades orientadas al fortalecimiento de las capacidades de I+D+i y el sector de la ciberseguridad española. Implantar iniciativas que eleven las capacidades y habilidades necesarias para el desarrollo de la actividad innovadora.
			5.2.2.	Transformación de la I+D+i en activos de alto valor añadido	Transformar las actividades I+D+I en productos, servicios o cualquier otro activo de valor añadido. Incrementar el catálogo de soluciones de ciberseguridad españolas, aumentar la visibilidad de nuestra oferta, o la dinamización de la cooperación.
			5.2.3.	Potenciar la posición española en I+D+i relacionado con la ciberseguridad	Desarrollar actividades para incrementar el peso de las soluciones y productos ciber “made in Spain”
	5.3.	Impulso a la inversión empresarial en ciberseguridad	5.3.1.	Atracción de inversión para el crecimiento y desarrollo de la Industria de Ciberseguridad	Potenciar las iniciativas de INCIBE para apoyar la captación de inversiones destinadas a la industria de ciberseguridad española.

Promover y detectar talento en ciberseguridad	6.1.	Fomento, detección y aprovechamiento del talento en ciberseguridad	6.1.1.	Mejoras las capacidades de empresas para la identificación y desarrollo del talento en ciberseguridad	Mejorar las capacidades de las empresas, con especial atención a pymes y profesionales, para la detección de necesidades de talento en ciberseguridad, y su desarrollo.
			6.1.2.	Generación e identificación de talento en ciberseguridad	Generar nuevos profesionales para el sector de la ciberseguridad. Fomentar las condiciones necesarias para la aparición de este talento en los niveles formativos multidisciplinares vinculados al sector.
	6.2.	Fomento de la capacitación del Talento en ciberseguridad	6.2.1.	Transformación de talento en ciberseguridad	Transformar perfiles profesionales de otros ámbitos al sector de la ciberseguridad. Desarrollar una estrategia definida para este tránsito desde diferentes ámbitos profesionales.
			6.2.2.	Fortalecer la cooperación público-privada para la generación y desarrollo del talento en ciberseguridad	Promocionar actores públicos y privados en esta estrategia de transformación de talento, para su posterior desarrollo y crecimiento.
Posicionar INCIBE como referente europeo de ciberseguridad	7.1.	El reconocimiento y posicionamiento de INCIBE como impulsor de la ciberseguridad y la confianza digital	7.1.1.	Posicionamiento de INCIBE como actor de referencia en el ámbito nacional e internacional	Consolidar la posición de INCIBE como actor clave en el desarrollo de una cultura de ciberseguridad, con especial atención al contexto europeo e internacional. Contribuir al desarrollo y posicionamiento internacional de la industria.
			7.1.2.	Desarrollo del relacionamiento estratégico de INCIBE	Desarrollar el plan de relacionamiento estratégico para el acompañamiento institucional de las acciones y objetivos, a nivel nacional e internacional.
	7.2.	Impulso de España como nodo internacional de ciberseguridad	7.2.1.	Impulso del Centro Espejo de Ciberseguridad en España	Desarrollar las actuaciones relacionadas con la puesta en marcha y desarrollo del Centro Espejo nacional del Centro Europeo de Competencias, Tecnología e Investigación en Ciberseguridad.
			7.2.2.	Impulso y coordinación de la comunidad de ciberseguridad	Realizar las actuaciones necesarias para la coordinación de la comunidad de ciberseguridad española y comunitaria.

5. RECURSOS

Para el desarrollo de presente Plan Anual y la consecución de los objetivos de su marco de resultados esperados, INCIBE dispone de los medios y recursos que se agrupan en torno a 4 conceptos: Personas, Presupuesto y Conocimiento.

Personas

A fecha 1 de enero de 2022 INCIBE cuenta con una plantilla de **130 personas**, más la colaboración de asistencias técnicas. La estructura organizativa busca dar respuesta a los 3 ejes estratégicos mencionados al inicio de este documento.

Presupuesto

Para el desarrollo de las actuaciones previstas en este Plan, INCIBE, obtiene financiación principalmente de una aportación patrimonial directa del accionista (Entidad Pública Empresarial Red.es), por transferencias verticales de los Presupuestos Generales del Estado (con cargo al presupuesto de la SEDIA), en las que se incluyen partidas con cargo a los Fondos del Plan de Recuperación de la UE, a través del Mecanismo de Recuperación y Resiliencia (MRR), parcialmente con los correspondientes ingresos por prestación de servicios derivados de encargos (actualmente de la SEDIA) y por la imputación de subvenciones derivados de la ejecución de proyectos europeos relacionados con la actividad de ciberseguridad. **En 2022 el presupuesto destinado para INCIBE asciende a un total de: 258.705.000,00 €.**

En la primera tabla se encuentra todo el gasto para actividad en 1 línea; mientras que en la segunda y se desglosa la actividad según las partidas presupuestarias consignadas en los Presupuestos Generales del Estado 2022.

Presupuesto 2022 (en miles de €)	Presupuesto ordinario	Fondos europeos	Presupuesto Total 2022
Gastos de explotación relacionados con la actividad	57.928	182.780	240.708
Gastos corrientes de funcionamiento+inversiones inmovilizado	9.598	0	9.598
Gastos de Personal	8.409	0	8.409
Ingresos (prestación de servicios, subv.explotac. y otros ing.)	-309	0	-309
Otros gastos (amortizaciones, financieros, etc)	298	0	298
Total 2022	**75.924**	**182.780**	**258.705**

6. ANEXO: MARCO DE RESULTADOS ESPERADOS

A continuación se incorpora el marco de resultados esperado del plan anual 2021. Los indicadores y subindicadores configuran el plan de trabajo vinculados a las medidas, y se establece unos resultados esperados para el presente ejercicio:

OBJETIVO 1: Promover una cultura de ciberseguridad en España			
Peso (LA)	**Medida**	**Peso (MED s/LA)**	**Indicador de medida**
LÍNEA 1.1. Promoción de la concienciación y la información			
10%	MEDIDA 1. Fortalecimiento de las capacidades de ciberseguridad de la Sociedad	30%	Acciones para el fortalecimiento de las capacidades de ciberseguridad de ciudadanos y menores
	MEDIDA 2. Fortalecimiento de capacidades de empresas	35%	Acciones para el fortalecimiento de las capacidades de ciberseguridad de empresas, especialmente pymes
	MEDIDA 3. Incremento de capacidades de ciberseguridad de “actores intermedios”	15%	Desarrollo de capacidades de ciberseguridad a través de "agentes intermedios"
	MEDIDA 4. Fortalecimiento de Servicios Públicos, Canales y Herramientas para la extensión de la Cultura de Ciberseguridad	20%	Evolución de la operación del canal de la Línea de Ayuda en Ciberseguridad
LÍNEA 1.2. Impulso de la colaboración público-privada y de la RSC			
8%	MEDIDA 5. Desarrollo del Foro Nacional de Ciberseguridad (contribución)	40%	Coordinación y contribución a los Grupos de Trabajo del Foro Nacional de Ciberseguridad
	MEDIDA 6. Identificación y Desarrollo de “mecanismos de multiplicación” de los esfuerzos de fortalecimiento	50%	Actuaciones para la identificación y desarrollo de mecanismos de multiplicación de las actividades de INCIBE
	MEDIDA 7. Desarrollo de la Responsabilidad Social Empresarial de INCIBE	10%	Actuaciones para el desarrollo de la RSE de INCIBE
LÍNEA 1.3. Impulso de la Generación de Conocimiento sobre Ciberseguridad			

2%	MEDIDA 8. Desarrollo del Conocimiento de la Ciberseguridad en España	100%	Iniciativas de Conocimiento
OBJETIVO 2: Aumentar y fortalecer las capacidades para detectar las ciberamenazas			
Peso (LA)	**Medida**	**Peso (MED s/LA)**	**Indicador de medida**
LÍNEA 2.1. Capacidades para la Detección			
6%	MEDIDA 9. Optimización y desarrollo continuado de las capacidades de detección	100%	Desarrollar y optimizar las capacidades de detección de INCIBE
LÍNEA 2.2. Capacidades para la Inteligencia			
3%	MEDIDA 10. Optimización y desarrollo continuado de las capacidades de inteligencia	60%	Optimizar y desarrollar las capacidades de inteligencia de INCIBE
	MEDIDA 11. Desarrollo de capacidades para la medición del riesgo	40%	Desarrollar capacidades de INCIBE para la medición del riesgo
EA 2.3. Explotación de la Información			
3%	MEDIDA 12. Desarrollo y fortalecimiento de las capacidades para la accionabilidad de informafición de ciberinteligencia	70%	Desarrollar y fortalecer las capacidades de INCIBE para la accionabilidad de información de ciberinteligencia
	MEDIDA 13. Difusión de la información de ciberinteligencia para la accionabilidad de terceros	30%	Análisis y propuesta de la estrategia para la difusión de información de ciberinteligencia para la accionabilidad de terceros
Peso (LA)	**Medida**	**Peso (MED s/LA)**	**Indicador de medida**
LÍNEA 3.1. Capacidades para la ayuda, soporte y respuesta			
8%	MEDIDA 14. Fortalecimiento de las capacidades de soporte y respuesta a incidentes	50%	Evolución y mejora de las capacidades de soporte y respuesta a incidentes
	MEDIDA 15. Fortalecimiento de los servicios de soporte y respuesta a incidentes	50%	Fortalecer las capacidades y servicios de soporte y respuesta a incidentes de INCIBE
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%	Fortalecimiento de las capacidades y servicios de INCIBE para respuesta de empresas a incidentes de ciberseguridad
	MEDIDA 17. Fortalecimiento de las capacidades de resiliencia y recuperación de los Operadores de Servicios Críticos y Proveedores de Servicios Digitales	50%	Desarrollar actividades y servicios para el fortalecimiento de las capacidades de resiliencia y recuperación de OSP y PSD
	MEDIDA 18. Protección de activos de empresas	25%	Operación y evolución de servicios IGA y TIRESIAS

LÍNEA 3.3. Capacidades para la gestión de crisis cibernéticas			
1%	MEDIDA 19. Desarrollo y optimización de las capacidades de gestión de crisis	100%	Mejora de los procesos de la gestión de crisis
OBJETIVO 4: Desarrollar las capacidades necesarias para proteger y defender activamente a ciudadanos y empresas			
Peso (LA)	**Medida**	**Peso (MED s/LA)**	**Indicador de medida**
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	100%	Recursos para la prevención del riesgo de acoso y abuso infantil
	MEDIDA 21. Fortalecimiento y optimización de las capacidades de defensa activa	0%	Desarrollar soluciones y medidas de defensa activa
	MEDIDA 22. Operación de herramientas y soluciones	0%	Desarrollar y optimizar las capacidades de detección de INCIBE
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%	Soluciones y Medidas de defensa activa
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%	Análisis de mejoras normativas para la defensa activa
OBJETIVO 5: Impulsar la industria española y la I+D+i de ciberseguridad			
Peso (LA)	**Medida**	**Peso (MED s/LA)**	**Indicador de medida**
LÍNEA 5.1. Potenciación de la industria española de ciberseguridad			
11%	MEDIDA 25. Impulso al emprendimiento en Ciberseguridad	35%	Impulso al emprendimiento
	MEDIDA 26. Desarrollo y fortalecimiento de la industria de ciberseguridad	40%	Acciones de fortalecimiento e impulso a la industria de ciberseguridad
	MEDIDA 27. Internacionalización de la industria de ciberseguridad	25%	Acciones de Internacionalización
LÍNEA 5.2. Impulso a la I+D+i española en ciberseguridad			
12%	MEDIDA 28. Fortalecer e incrementar las capacidades de I+D+i	10%	Acciones de apoyo promovidas por INCIBE de impacto en Investigación nacional en CS
	MEDIDA 29. Transformación de la I+D+i en activos de alto valor añadido	85%	Actividades de Transformación de I+D+i en activos de alto valor añadido
	MEDIDA 30. Potenciar la posición española en I+D+i relacionado con la ciberseguridad	5%	Acciones de apoyo promovidas por INCIBE para fortalecer y elevar la posición española en I+D+i en Ciberseguridad

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%	Atracción de inversión para el crecimiento y desarrollo de la Industria de Ciberseguridad
OBJETIVO 6: Promover y detectar talento en ciberseguridad			
Peso (LA)	**Medida**	**Peso (MED s/LA)**	**Indicador de medida**
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%	Fomento de la identificación y desarrollo de talento en ciberseguridad
	MEDIDA 33. Generación e identificación de talento en ciberseguridad	65%	Generación e identificación y capacitación de talento en ciberseguridad
LÍNEA 6.2. Fomento de la capacitación del Talento en ciberseguridad			
3%	MEDIDA 34. Transformación de talento en ciberseguridad	70%	Transformación del talento en ciberseguridad
	MEDIDA 35. Fortalecer la cooperación público-privada para la generación y desarrollo del talento en ciberseguridad	30%	Fomento de la cooperación para el desarrollo de talento en ciberseguridad
OBJETIVO 7: Posicionar INCIBE como referente europeo de ciberseguridad			
Peso (LA)	**Medida**	**Peso (MED s/LA)**	**Indicador de medida**
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%	Actuaciones para el posicionamiento de INCIBE como actor de referencia
	MEDIDA 37. Desarrollo del relacionamiento estratégico de INCIBE	35%	Acciones para desarrollo del relacionamiento estratégico de INCIBE
LÍNEA 7.2. Impulso de España como nodo internacional de ciberseguridad			
2%	MEDIDA 38. Impulso del Centro Espejo de Ciberseguridad en España	70%	Puesta en marcha el Centro de Coordinación Nacional en Ciberseguridad
	MEDIDA 39. Impulso y coordinación de la comunidad de ciberseguridad	30%	Coordinación de la comunidad nacional de ciberseguridad