

# PLAN ESTRATÉGICO INCIBE 2023-2025

Plan de actuación anual 2024

## ÍNDICE

---

<b>1. Objeto y alcance del presente documento .....</b>	<b>3</b>
<b>2. Objetivo 1. Fortalecimiento de la ciberseguridad .....</b>	<b>4</b>
<b>3. Objetivo 2. Impulso del ecosistema empresarial del sector de la ciberseguridad .....</b>	<b>6</b>
<b>4. Objetivo 3. Estímulo de España como nodo internacional en el ámbito de la ciberseguridad .....</b>	<b>7</b>

## 1. OBJETO Y ALCANCE DEL PRESENTE DOCUMENTO

---

El objeto del presente documento es identificar el plan de actuación anual 2024 que emana del Plan Estratégico Plurianual 2023-2025 de INCIBE.

INCIBE, como entidad integrante del sector público estatal, está sometida al control de eficacia y supervisión continua, quedando sometida al régimen presupuestario regulado por la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

De acuerdo con dicha ley, INCIBE elaborará un presupuesto de explotación que detallará los recursos y dotaciones anuales correspondientes y un presupuesto de capital con el mismo detalle. Los presupuestos de explotación y de capital se integrarán en los Presupuestos Generales del Estado. Asimismo, y cumpliendo con lo dispuesto en esta ley se formulará anualmente un programa de actuación plurianual.

Con esta finalidad y a fin de poder alinear el Plan Estratégico de INCIBE con el programa plurianual ministerial del Ministerio para la Transformación Digital y de la Función Pública, a principios de cada año se presentará al Consejo de Administración una propuesta de contribución de las líneas de actuación a dichos objetivos, la cual estará condicionada por la dotación presupuestaria de INCIBE como sociedad mercantil estatal y a la ejecución del Plan de Recuperación, Transformación y Resiliencia.

## 2. OBJETIVO 1. FORTALECIMIENTO DE LA CIBERSEGURIDAD DE LA CIUDADANÍA, PYMES Y PROFESIONALES

Peso (LA)	Línea de actuación y medida	Peso (M)	Indicador de medida	Valor Meta	IMPACTO (outcome)	Subindicador (componentes del Indicador)	Valor Meta	Valor Aceptable	Valor Mínimo	Peso	
<b>LÍNEA 1.1. Promoción de la concienciación y la información</b>											
12%	MEDIDA 1 Fortalecimiento de las capacidades de ciberseguridad de la ciudadanía y menores	6%	Acciones para el fortalecimiento de las capacidades de ciberseguridad de ciudadanos y menores	100%	KGI 1.1.: Desarrollo de 300 acciones desarrolladas para incrementar la concienciación	<b>Transformación digital cibersegura de la ciudadanía</b>				2%	
						Sub 1. Coordinación mensual con las universidades firmantes de convenios al amparo de la IP de CyberCamp	100%	80%	60%	40%	
						Sub 2. Desarrollo del nuevo portal web de CyberCamp	100%	80%	60%	30%	
						Sub 3. Puesta en operación de la nueva versión mejorada del APP CONAN mobile	100%	80%	60%	30%	
						<b>Dinamización de la red territorial de concienciación y formación en ciberseguridad</b>				2%	
						Sub 1. Gestión de las experiencias itinerantes (Roadshow, Realidad virtual y Stand)	100%	80%	60%	40%	
						Sub 2. Desarrollo del espacio web de experiencia itinerantes (donde puedas apuntarte, descargártelo, compartirlo, suscribirte)	100%	80%	60%	30%	
						Sub 3. Cooperación con la red de centros de FP para la formación en ciberseguridad	100%	80%	60%	30%	
						<b>IS4k</b>				2%	
	Sub 1. Evolución de la línea de reporte para alineamiento con la DSA	100%	80%	60%	40%						
	Sub 2. Programa de apoyo al análisis forense para víctimas de ciberacoso	100%	80%	60%	30%						
	Sub 3. Estudio sobre la ciberseguridad del menor en España	100%	80%	60%	30%						
	MEDIDA 2 Fortalecimiento de las capacidades de ciberseguridad de los profesionales	7%	Acciones para el fortalecimiento de las capacidades de ciberseguridad de los profesionales	100%	KGI 1.1.: Desarrollo de 300 acciones desarrolladas para incrementar la concienciación	<b>Transformación digital cibersegura de actores claves</b>					4%
						Sub 1. Acuerdos de colaboración con asociaciones y entidades profesionales de los sectores estratégicos identificados por la NIS 2 (coordinación mensual)	100%	80%	60%	25%	
						Sub 2. Coordinación mensual con la IP de colectivos infrarrepresentados y personas con discapacidad	100%	80%	60%	25%	
Sub 3. Cooperación internacional con organismos público-privados (OEA, multinacionales, WEF)						100%	80%	60%	25%		
Sub 4. Ampliación del Summer Bootcamp a norte de África, Oriente Medio y este de Europa						100%	80%	60%	25%		
<b>Competiciones de hacking ético territoriales</b>										3%	
Sub 1. Colaboración con las asociaciones y entes locales para la organización de CTF						100%	80%	60%	50%		
Sub 2. Reuniones con los organizadores de las asociaciones						100%	80%	60%	50%		
<b>LÍNEA 1.2. Capacidades para la ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes</b>											
12%	MEDIDA 3 Fortalecimiento de las capacidades de soporte y respuesta a incidentes	6%	Acciones para el fortalecimiento de las capacidades de soporte y respuesta a incidentes	100%	KGI 1.2.: Desarrollo de 50 actuaciones para el fortalecimiento de las capacidades de soporte y respuesta a incidentes	<b>Respuesta incidentes de ciberseguridad para ciudadanos y entidades de derecho privado</b>				2%	
						Sub 1. Refuerzo de las capacidades del departamento de gestión de crisis y emergencias	100%	80%	60%	16%	
						Sub 2. Refuerzo de las capacidades del 017, mediante colaboración con la FEMP	100%	80%	60%	16%	
						Sub 3. Impulso a la colaboración con los CERT autonómicos y la red de CERTS privados	100%	80%	60%	17%	
						Sub 4. Impulso a las capacidades de IA aplicadas en INCIBE-CERT	100%	80%	60%	17%	
						Sub 5. Desarrollo de guía para aplicación en la gestión de crisis en empresas	100%	80%	60%	17%	
						Sub 6. Diseño y puesta en marcha de un nuevo procedimiento de escalado a la DG de incidentes de alto interés en 24x7	100%	80%	60%	17%	
						<b>Respuesta incidentes de ciberseguridad para operadores críticos y esenciales</b>					2%
						Sub 1. Lanzamiento y ejecución del portfolio de servicios para sectores estratégicos	100%	80%	60%	50%	
						Sub 2. Ampliación del servicio de divulgación de vulnerabilidades	100%	80%	60%	50%	
						<b>Fortalecimiento capacidades internas soporte y respuesta</b>					2%
						Sub 1. Adecuación del SGSI a la nueva versión de la norma UNE ISO/IEC 27001:2023	100%	80%	60%	50%	
						Sub 2. Diseño y construcción del mapa normativo en ciberseguridad con actualización periódica según evolución de las diferentes normativas	100%	80%	60%	50%	

						<b>Operadores de servicios críticos y proveedores de sectores estratégicos</b>					<b>3%</b>	
						Sub 1. Incremento de la difusión de alertas de incidentes por sectores estratégicos en régimen 24 horas	100%	80%	60%		16%	
						Sub 2. Diseño y definición del modelo de guía de gestión de incidentes por sectores estratégicos adaptadas a la NIS 2	100%	80%	60%		16%	
						Sub 3. Creación y desarrollo del laboratorio de gestión de incidentes del sector de transporte viario y ferroviario	100%	80%	60%		17%	
						Sub 4. Lanzamiento del nuevo servicio de ciber ejercicios nacionales	100%	80%	60%		17%	
						Sub 5. Implantación de mejoras en la seguridad de los mecanismos de control de acceso	100%	80%	60%		17%	
						Sub 6. Migración de herramientas o servicios al nuevo entorno orientado a micros servicios basado en micros servicios	100%	80%	60%		17%	
						<b>Nuevas capacidades tecnológicas para mejorar la prestación de los servicios</b>					<b>3%</b>	
						Sub 1. Desarrollo de una nueva versión de la plataforma de acceso a los servicios que INCIBE presta a entidades estratégicas	100%	80%	60%		50%	
						Sub 2. Desarrollo de una nueva versión del sistema de descubrimiento y monitorización de la seguridad de activos de entidades estratégicas	100%	80%	60%		50%	
<b>LÍNEA 1.3. Impulso de la colaboración público-privada y público-públicos y de la RSE</b>												
<b>12%</b>	MEDIDA 5 Consolidación del programa de trabajo de ciberseguridad nacional	6%	Acciones para la consolidación del programa de trabajo de ciberseguridad nacional	100%	KGI 1.3.: Desarrollo de 60 acciones público privadas de colaboración y/o para el desarrollo de la RSE	<b>Acciones para consolidar el entorno de Ciberseguridad nacional</b>					<b>6%</b>	
						Sub 1. Seguimiento de convenios Fiscalía General del Estado y el Ministerio del Interior, y firma con CGPJ	100%	80%	60%		50%	
						Sub 2. Impulsar las actuaciones internacionales en el seno del Consejo Nacional de Ciberseguridad	100%	80%	60%		50%	
						<b>Programa formativo</b>						<b>4%</b>
						Sub 1. Impulso a los programas de prácticas de formación de la FP y universitario	100%	80%	60%		50%	
	MEDIDA 6 Desarrollo de la Responsabilidad Social Empresarial de INCIBE	4%	Acciones para el desarrollo de la Responsabilidad Social Empresarial	100%		Sub 2. Impulso a proyectos de participación ciudadanía en ciberseguridad (Tu barrio Ciber)	100%	80%	60%		50%	

## 3. OBJETIVO 2. IMPULSO DEL ECOSISTEMA EMPRESARIAL DEL SECTOR DE LA CIBERSEGURIDAD

Peso (LA)	Línea de actuación y medida	Peso (M)	Indicador de medida	Valor Meta	IMPACTO (outcome)	Subindicador (componentes del Indicador)	Valor Meta	Valor Aceptable	Valor Mínimo	Peso	
<b>LÍNEA 2.1. Impulso y fortalecimiento de la industria de ciberseguridad</b>											
14%	MEDIDA 7 Promoción de iniciativas emprendedoras de ciberseguridad	7%	Impulso al emprendimiento	100%	KGI 2.1.: Desarrollo de 50 actuaciones que impulsen la visibilidad de las empresas españolas	<b>Desarrollo de un programa de acompañamiento a nuevos proyectos</b>				7%	
						Sub 1. Programa de apoyo a la creación de spin-off universitarias en ciberseguridad	100%	80%	60%	50%	
						Sub 2. Gestión de la IP de emprendimiento - conversión de proyectos	100%	80%	60%	50%	
						<b>Incorporación de acciones de internacionalización</b>					7%
						Sub 1. Acciones de apoyo a las empresas de la industria nacional de ciberseguridad que impulsen su crecimiento internacional	100%	80%	60%	25%	
						Sub 2. Apoyo a la inversión extranjera en el lanzamiento de proyectos de ciberseguridad en España	100%	80%	60%	25%	
	MEDIDA 8 Internacionalización de la industria de ciberseguridad	7%	Acciones de internacionalización	100%		Sub 3. Acciones de refuerzo a los fondos de inversión nacionales en ciberseguridad	100%	80%	60%	25%	
						Sub 4. Atracción de compradores, inversores y delegaciones internacionales	100%	80%	60%	25%	
<b>LÍNEA 2.2. Fomento de la I+D+i en ciberseguridad</b>											
13%	MEDIDA 9 Transformación de la I+D+i en activos de alto valor añadido	7%	Actuaciones de transformación de la I+D+i	100%	KGI 2.2.: Compromisos del gasto del 100%	<b>Compra Pública Innovadora</b>				7%	
						Sub 1. Desarrollo de la 4ª convocatoria de la CPI	100%	80%	60%	40%	
						Sub 2. Despliegue de una estrategia de recuperación de la inversión del programa CPI	100%	80%	60%	30%	
						Sub 3. Lanzamiento de las convocatorias de financiación en cascada del NCC	100%	80%	60%	30%	
						<b>Desarrollo de la red de Cátedras y Proyectos Estratégicos de ciberseguridad en España</b>					7%
						Sub 1. Coordinación mensual con los responsables de Cátedras de Universidades	100%	80%	60%	50%	
	MEDIDA 10 Desarrollo de programas de I+D+i y fortalecimiento de las capacidades en ciberseguridad por universidades	7%	Acciones de fortalecimiento o impulso de la I+D+i	100%		Sub 2. Coordinación mensual con los responsables de Proyectos Estratégicos de Universidades	100%	80%	60%	50%	
<b>LÍNEA 2.3. Promoción del talento en ciberseguridad</b>											
8%	MEDIDA 11 Fomento, detección y aprovechamiento del talento en ciberseguridad	4%	Actuaciones para la mejora del talento	100%	KGI 2.3.: 10.260 profesionales formados en ciberseguridad	<b>Actuaciones formativas especializadas en ciberseguridad</b>				4%	
						Sub 1. Despliegue de la oferta formativa de 10.260 plazas en ciberseguridad a través de la red académica	100%	80%	60%	100%	
						<b>Programa de retención de talento en INCIBE</b>					4%
						Sub 1. Incremento de la inversión en formación del personal de INCIBE	100%	80%	60%	50%	
	MEDIDA 12 Identificación e impulso de acciones formativas para favorecer la integración	4%	Fomento e integración del talento	100%		Sub 2. Actualización del estudio Análisis y diagnóstico del mercado de la ciberseguridad y talento de ciberseguridad en España.	100%	80%	60%	50%	

## 4. OBJETIVO 3. ESTÍMULO DE ESPAÑA COMO NODO INTERNACIONAL EN EL ÁMBITO DE LA CIBERSEGURIDAD

Peso (LA)	Línea de actuación y medida	Peso (M)	Indicador de medida	Valor Meta	IMPACTO (outcome)	Subindicador (componentes del Indicador)	Valor Meta	Valor Aceptable	Valor Mínimo	Peso
<b>LÍNEA 3.1. Consolidación del programa de trabajo de ciberseguridad europeo</b>										
8%	MEDIDA 13 Apoyo técnico y económico a las empresas españolas	4%	Posicionamiento del NCC-ES INCIBE	100%	KGI 3.1.: Desarrollo de 25 actuaciones para la consolidación del programa de trabajo	<b>NCC-ES INCIBE</b>				<b>4%</b>
						Sub 1. Liderazgo de iniciativas con las Agencias Europeas relacionadas con la ciberseguridad y ciberdefensa	100%	80%	60%	40%
						Sub 2. Participación activa en los WG del NCC	100%	80%	60%	30%
	Sub 3. Impulso a la oficina de proyectos europeos	100%	80%	60%		30%				
	<b>Actuaciones para facilitar el alineamiento y las capacidades de INCIBE</b>					<b>4%</b>				
MEDIDA 14 Alineamiento con el marco regulatorio y legislativo europeo	4%	Acciones para el desarrollo del posicionamiento de INCIBE	100%	Sub 1. Cooperación internacional en el refuerzo de las capacidades de respuesta en sectores estratégicos en el marco de la OTAN y aliados estratégicos	100%	80%	60%	100%		
<b>LÍNEA 3.2. Desarrollo del nodo de ciberseguridad nacional y autonómico</b>										
13%	MEDIDA 15 Impulso y asesoramiento a la innovación en ciberseguridad	7%	Actuaciones para apoyar a la creación de ecosistemas para la ciberseguridad	100%	KGI 3.2.: Desarrollo de 50 actuaciones que contribuyan al desarrollo del nodo de ciberseguridad nacional y autonómico	<b>Centros Demostradores de ciberseguridad</b>				<b>7%</b>
						Sub 1. Puesta en marcha del centro demostrador de León siguiendo el programa operativo	100%	80%	60%	50%
	Sub 2. Comenzar los procesos de acreditación en la ISO 17025 como laboratorio de ensayo y calibración	100%	80%	60%		50%				
	<b>RETECH</b>					<b>7%</b>				
	MEDIDA 16 Puesta en marcha de proyectos territoriales de transformación digital	7%	Acciones para apoyar proyectos tractores fomentando el intercambio de conocimiento	100%		Sub 1. Completar el despliegue de RETECH en el conjunto de las CCAA	100%	80%	60%	50%
Sub 2. Desarrollo de los programas operativos	100%	80%	60%	50%						
<b>LÍNEA 3.3. Identificación y desarrollo de actuaciones y controles para evitar la exposición al riesgo</b>										
8%	MEDIDA 17 Identificación y desarrollo de instrumentos jurídicos	3%	Actuaciones para favorecer la ejecución	100%	KGI 3.3.: 100% de actuaciones implantadas para mitigar el riesgo	<b>Desarrollo de instrumentos jurídicos</b>				<b>3%</b>
						Sub 1. Adecuación de los mecanismos de INCIBE a los requisitos del MRR	100%	80%	60%	100%
	<b>Seguimiento y ejecución del PRTR</b>					<b>4%</b>				
	Sub 1. Adecuación de los procedimientos a los requisitos del MRR	100%	80%	60%		20%				
	Sub 2. Diseño y supervisión del Plan Antifraude	100%	80%	60%		20%				
	Sub 3. Diseño del procedimiento de comunicación del PRTR para entidades	100%	80%	60%		20%				
Sub 4. Supervisión del cumplimiento del procedimiento de comunicación del PRTR para entidades	100%	80%	60%	20%						
MEDIDA 18 Identificación y desarrollo de actuaciones de seguimiento de ejecución del PRTR	4%	Actuaciones para controlar el riesgo de seguimiento y ejecución del PRTR	100%	Sub 5. Análisis de la evolución mensual de impactos en comunicación	100%	80%	60%	20%		