PLAN ANUAL DE ACTIVIDAD INCIBE 2024

Resultados conseguidos

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. PRESENTACIÓN

Qué es INCIBE

El S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE), sociedad dependiente del Ministerio para la Transformación Digital y de la Función Pública a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

Como centro de excelencia, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

INCIBE-CERT es además el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el Instituto Nacional de Ciberseguridad. En el caso de la gestión de incidentes que afecten a operadores críticos del sector privado, INCIBE-CERT está operado conjuntamente por INCIBE y OCC, Oficina de Coordinación de Ciberseguridad del Ministerio del Interior. INCIBE-CERT es uno de los equipos de respuesta de referencia ante incidentes que se coordina con el resto de los equipos nacionales e internacionales para mejorar la eficacia en la lucha contra los delitos que involucran a las redes y sistemas de información, reduciendo sus efectos en la seguridad pública.

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.

Las metas previstas para que INCIBE pueda desarrollar su misión y pueda acercarse a su visión son los objetivos estratégicos. En el Plan Estratégico Plurianual (PEP) de INCIBE, dichos objetivos se han procedido a establecer conforme a las medidas y los ejes

establecidos para INCIBE en agenda España Digital 2026 y en el PRTR. En base a dichos criterios, los objetivos establecidos son:

- **Objetivo 1. Fortalecimiento de la ciberseguridad de la ciudadanía, pymes y profesionales.** Para fortalecer las capacidades en ciberseguridad y la confianza digital de la ciudadanía, menores, empresas y profesionales, se hace necesario implementar una cultura de ciberseguridad. Para ello, es recomendable invertir en la concienciación de los riesgos asociados a la digitalización y la modernización del tejido empresarial, así como en la formación en competencias digitales de ciberseguridad.
- **Objetivo 2. Estímulo del ecosistema empresarial del sector de la ciberseguridad.** Este objetivo responde a la necesidad de contribuir a la soberanía digital europea tomando como eje principal la generación de riqueza, empleo e impulso de las empresas del sector de la ciberseguridad en España.
- **Objetivo 3. Impulso de España como nodo internacional en el ámbito de la ciberseguridad.** Con este objetivo se persigue contribuir a la soberanía digital en este campo respondiendo a la Estrategia de Ciberseguridad de la Unión Europea para la Década Digital.

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

2. PLAN ESTRATÉGICO 2023-2025

El Plan Estratégico de INCIBE para el periodo 2023-2025, 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 3 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.

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

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

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

Fruto del desarrollo del conjunto de objetivos, medidas y actuaciones desarrolladas, en el anterior plan estratégico de INCIBE se han lanzado tanto el **Programa de Impulso a la Industria de la Ciberseguridad Nacional**, como el **Programa Global de Innovación en Seguridad**. El primero, contribuye en el aspecto clave de la industria: Impulsar la industria nacional de la ciberseguridad para el surgimiento, crecimiento y desarrollo de empresas en este sector. Por otra parte, el Programa Global tiene como misión particular el impulso de las capacidades en ciberseguridad de la sociedad y la economía en general a través de un programa que persigue la promoción y generación del conocimiento y la transferencia del mismo al sector productivo, especialmente estableciendo sinergias entre los ámbitos sociales y económicos de la ciberseguridad. Ambos programas, están plenamente vinculados con los objetivos del PRTR (fortalecer las capacidades de ciberseguridad de ciudadanos y empresas, impulsar la industria, I+D+i y talento en ciberseguridad y poner en marcha el nodo nacional de la red europea de centros de competencia industrial

tecnológica y de investigación en ciberseguridad) y se materializan en cuatro grandes iniciativas en las que se enmarcan todas las actividades de INCIBE: CONFIA, Ciberinnova, INCIBE emprende y Talento Hacker.

- 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 2026**.
  - La **Estrategia Nacional contra el Crimen Organizado** y la Delincuencia Grave 2019-2023, entre cuyas prioridades se encuentra la lucha contra el cibercrimen.

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

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 2024, 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 **3 objetivos estratégicos para el período 2023-2025**:

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

OBJETIVO ESTRATÉGICO 1. Fortalecimiento de la ciberseguridad de la ciudadanía, pymes y profesionales

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

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

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

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

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

Como complemento de estas iniciativas y en consonancia con el PRTR, en concreto con los CID 246 y 247, en este objetivo se plantea la realización de recursos para sus públicos objetivos y la capacidad de gestionar hasta 20.000 consultas en la Línea de Ayuda de Ciberseguridad 017. Con esa perspectiva el presente objetivo persigue llevar a cabo actuaciones focalizadas en las siguientes líneas de actuación.

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 los profesionales

LÍNEA DE ACTUACIÓN 1.2: Capacidades para la ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes

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

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

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

LÍNEA DE ACTUACIÓN 1.3: Impulso de la colaboración público-privada y público-públicos y de la RSE

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

MEDIDA 5. Consolidación del programa de trabajo de ciberseguridad nacional

MEDIDA 6. Desarrollo de la Responsabilidad Social Empresarial de INCIBE

OBJETIVO ESTRATÉGICO 2. Impulso del ecosistema empresarial del sector de la ciberseguridad

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

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

LÍNEA DE ACTUACIÓN 2.1: Impulso y fortalecimiento de la industria de ciberseguridad

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

MEDIDA 7. Promoción de iniciativas emprendedoras de ciberseguridad

MEDIDA 8. Internacionalización de la industria de ciberseguridad

LÍNEA DE ACTUACIÓN 2.2: Fomento de la I+D+i en ciberseguridad

Los instrumentos establecidos por INCIBE para canalizar esta línea de actuación el fortalecimiento, impulso y transformación de la I+D+i en ciberseguridad son (i) la compra pública de innovación, como instrumento esencial de las políticas públicas para impulsar la innovación y la competitividad desde los poderes públicos empleando la demanda pública de productos, servicios y suministros como instrumentos mediante el que ejecutar los mandatos de las entidades compradoras; (ii) el programa para el impulso de certificaciones en ciberseguridad que permita capacitar a las empresas permitiéndolas adquirir una madurez a la hora de participar en procesos de contratación pública; (iii y iv) la invitación pública para la colaboración en la promoción de cátedras y de proyectos estratégicos de ciberseguridad en España respectivamente.

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

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

LÍNEA DE ACTUACIÓN 2.3: Promoción del talento en ciberseguridad

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

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

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

OBJETIVO ESTRATÉGICO 3. Estímulo de España como nodo internacional en el ámbito de la ciberseguridad

El ecosistema empresarial identificado en el anterior objetivo es clave para el posicionamiento en línea con la visión de INCIBE. Con este objetivo se persigue contribuir a la soberanía digital en este campo respondiendo a la Estrategia de Ciberseguridad de la Unión Europea para la Década Digital. Este itinerario persigue garantizar que la Unión Europea alcance sus objetivos y metas de transformación digital de nuestra sociedad y economía en consonancia con los valores de la UE, que refuerce nuestro liderazgo digital y promueva políticas centradas en el ser humano, inclusivas y sostenibles que capaciten a los ciudadanos y las empresas.

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

LÍNEA DE ACTUACIÓN 3.1: Consolidación del programa de trabajo de ciberseguridad europeo

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

MEDIDA 13. Apoyo técnico y económico a las empresas españolas

MEDIDA 14. Alineamiento con el marco regulatorio y legislativo europeo

LÍNEA DE ACTUACIÓN 3.2: Desarrollo del nodo de ciberseguridad nacional y autonómico

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

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

MEDIDA 15. Impulso y asesoramiento a la innovación en ciberseguridad

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

LÍNEA DE ACTUACIÓN 3.3: Identificación e implantación de actuaciones y controles para reducir la exposición al riesgo

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

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

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

MEDIDA 17. Identificación y desarrollo de instrumentos jurídicos

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

MODELO DE GOBERNANZA

La ejecución del presente plan dispone de un modelo de gobernanza, el cual se constituye en una herramienta que permite permitir asegurar la correcta gestión de las actuaciones previstas en el PEP 2023-2025 a través del control, seguimiento y evaluación de las actividades previstas en este marco temporal, junto con la revisión de los niveles de coordinación en la estructura organizativa de INCIBE y de los mecanismos para la correcta coordinación y alineamiento operativo. A finales de 2024 con la incorporación de nuevos gerentes se procede a elevar en primera instancia a la Comisión de Personal y Retribución del Consejo de Administración y posteriormente a este órgano una versión actualizada de este modelo de gobernanza, que tiene como principal característica la incorporación de un nivel más de coordinación, el Comité de Dirección Extendido. Por tanto, el control y seguimiento del PEP 2023-2025 se realiza incorporando un nuevo nivel, mecanismo e instrumento de coordinación conforme se puede comprobar en la siguiente imagen.

Antes

Ahora

Este modelo de gobernanza para la gestión se basa, principalmente, en la identificación de los niveles de seguimiento y control necesarios y el establecimiento de los responsables de la ejecución de dicho seguimiento.

Para conseguir dicho propósito deben disponer de las capacidades técnicas, funcionales y organizativas necesarias para poder realizar una adecuada gobernanza de la estrategia de INCIBE. Por ello, el plan tiene previsto llevar a cabo al comienzo de cada uno de los años una revisión de las actividades, actuaciones y, si fuese necesario de las líneas de actuación previstas al comienzo del plan para, en su caso, proceder a la oportuna actualización de las mismas, alineando como no podía ser de otra forma la actividad con lo que se requiere de INCIBE siguiendo los mandatos del Gobierno.

El Modelo de Gobernanza completo se puede consultar en:
https://www.incibe.es/incibe/informacion-corporativa/que-hacemos

MODIFICACION DE OBJETIVOS

El Consejo de Administración de INCIBE llevó a cabo el 28 de abril de 2023 la aprobación de la modificación del Plan Estratégico Plurianual de INCIBE, y la aprobación del Plan de Actuación Anual y del Modelo de Gobernanza, tras haberse elevado previamente a la Comisión de Personal y Retribución de este órgano.

Fruto de esta aprobación, INCIBE ha estado ejecutando y reportando la realización del presente Plan de Actuación Anual con carácter mensual conforme al Modelo de Gobernanza.

Proceso de aprobación y elevación al socio único

El proceso que se muestra a continuación es la relación de aprobaciones que deben darse para que los objetivos de INCIBE queden completamente validados y aprobados. Este proceso deberá repetirse, en caso de que tuvieran que ser modificados (como es el caso de los Objetivos de Empresa en 2023).

1. Identificación de objetivos. Identificación de líneas de actuación y medidas, así como propuestas de indicadores.
2. Aprobación por la Dirección General de INCIBE. Aprobación de la propuesta del PEP 2023-2025. Aprobación de la propuesta del Plan de Actuación Anual
3. Comisión de personal y retribuciones. Emisión del informe o adoptación de propuestas relativa al cumplimiento de objetivos conforme a lo establecido en el Reglamento Interno del Consejo de Administración de INCIBE en su artículo 23. Aprobación de los objetivos generales de la empresa.
4. Consejo de Administración. Aprobación de la modificación del PEP. Aprobación del Plan de Actuación Anual y del Modelo de Gobernanza
5. Red.es. Elevación al socio único la propuesta del Plan de Actuación Anual y aprobación de los objetivos de empresa de INCIBE

Motivación del cambio: informe de la DGCAG

En este marco de actuación, a finales del mes de julio se recibió un informe de la Dirección General de lo Consultivo de la Abogacía General del Estado por el cual se determinaba que INCIBE, como sociedad mercantil estatal, no podía dar ayudas ni subvenciones y limitaba, en los mismos términos, el uso de nuestros fondos PRTR con esos fines, a las entidades con las que firmemos convenios.

En este contexto y tomando como perspectiva que en el desarrollo de algunas medidas identificadas y aprobadas en el mes de abril estaba previsto iban enfocadas a disponer de dicha capacidad.

La propuesta modificación de Objetivos se lleva a cabo tanto por el informe del consultivo antes referenciado como, por el hecho de que INCIBE ha estado esperando a disponer de una respuesta oficial sobre las ayudas concedidas, pero, ha llegado una situación en la que hay que elevar la solicitud de cambio para adecuar la realidad y para eliminar factores exógenos que repercuten en la consecución de los objetivos del plan.

En cualquier caso, el Plan de Actuación Anual 2023 mantendría el mismo número de objetivos, medidas, líneas de actuación y pesos aprobados en el Consejo de Administración del 28 de abril de 2023.

Siendo por consiguiente el alcance de esta propuesta de modificación dos cuestiones.

- Por un lado, la eliminación de aquellos subindicadores afines con actuaciones vinculadas a las ayudas
- Por otro la modificación de alguno de los subindicadores afines al programa RETECH al estar esté vinculado inicialmente con la posibilidad de que las entidades con las que se prevén la firma de convenios de colaboración pudieran ejecutar ayudas.

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 (en el momento de elaboración del cambio) Ministerio de Asuntos Económicos y Transformación Digital, 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.

Resumen de los cambios introducidos

Eliminación de aquellos subindicadores afines con actuaciones vinculadas a la concesión de ayudas:

- INCIBE no ha llegado a recibir una respuesta oficial del consultivo sobre las ayudas concedidas hasta la fecha de emisión del oficio de lo consultivo.
- Son subindicadores vinculados con actuaciones que estaban previstas inicialmente pero que finalmente no van a poder ejecutarse en la actualidad.
- Esta eliminación no supone dejar de ejecutarse sino que los componentes de los subindicadores y las metas no son posible ser alcanzadas.
- Implica el redimensionamiento de los subindicadores de las medidas 7, 8 y 9.

Modificación de alguno de los subindicadores afines al programa RETECH, al estar este vinculado inicialmente con la posibilidad de que las entidades con las que se prevén la firma de convenios de colaboración pudieran ejecutar ayudas.

- El informe del consultivo ha supuesto que los convenios que se habían negociado previamente con las comunidades autónomas no se hayan firmado en su totalidad.
- Por ello, es necesario modificar el alcance de esta medida y no plantearse una eliminación completa.

- Esa modificación que se plantea se ha de traducir en la matización de los componentes y metas y, en la eliminación de alguno de ellos.
- Implica al subindicador de las medida 16.

3. RESULTADOS CONSEGUIDOS

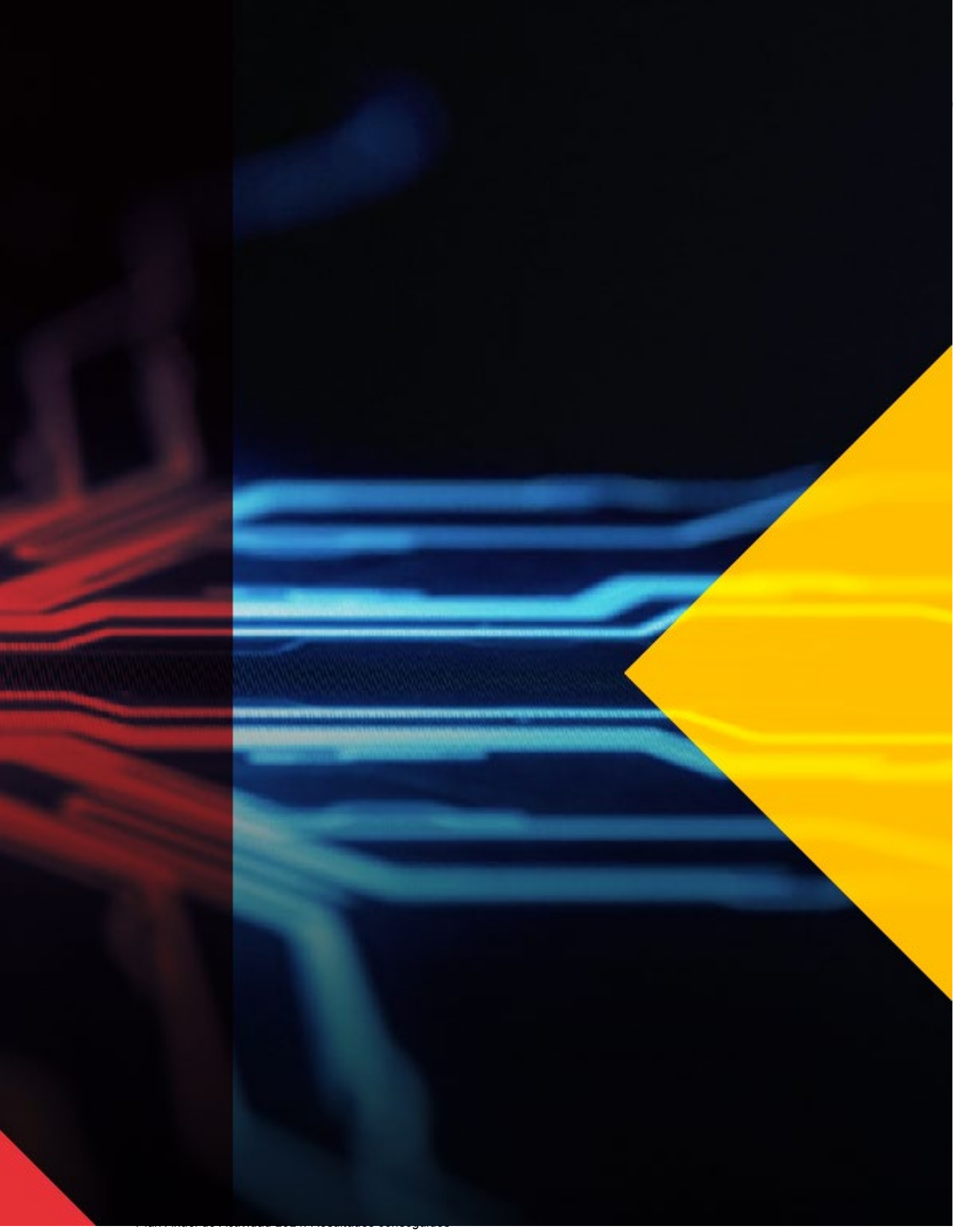
A continuación, se incorpora el marco de resultados finalmente conseguidos del plan anual 2024. Los indicadores y subindicadores configuran el plan de trabajo vinculados a las medidas, y se identifican los resultados finalmente alcanzados para el ejercicio que trata este documento.

OBJETIVO 1: Fortalecimiento de la ciberseguridad de la ciudadanía, pymes y profesionales								
Peso (LA)	**Línea de acción de Actuación y Medida**	**Peso (MED)**	**Indicador de medida**	**Valor Meta**	**IMPACTO (outcome)**	**Subindicador (componentes del Indicador)**	**Valor Cierre**	**VF fijo**
LÍNEA 1.1. Promoción de la concienciación y la información								
13%	**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	Transformación digital cibersegura de la ciudadanía		
						Sub 1. Coordinación mensual con las universidades firmantes de convenios al amparo de la IP de CyberCamp	0,80%	0,80%
						Sub 2. Desarrollo del nuevo portal web de CyberCamp	0,60%	0,60%
						Sub 3. Puesta en operación de la nueva versión mejorada del APP CONAN mobile	0,60%	0,60%
						Dinamización de la red territorial de concienciación y formación en ciberseguridad		
						Sub 1. Gestión de las experiencias itinerantes (Roadshow, Realidad virtual y Stand)	0,80%	0,80%
						Sub 2. Desarrollo del espacio web de experiencia itinerantes	0,60%	0,60%
						Sub 3. Cooperación con la red de centros de FP para la formación en ciberseguridad	0,60%	0,60%
						IS4k		
						Sub 1. Evolución de la línea de reporte para alineamiento con la DSA	0,80%	0,80%
						Sub 2. Programa de apoyo al análisis forense para victimas de ciberacoso	0,60%	0,60%
						Sub 3. Estudio sobre la ciberseguridad del menor en España	0,60%	0,60%
	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%		Transformación digital cibersegura de actores claves		
						Sub 1. Acuerdos de colaboración con asociaciones y entidades profesionales de los sectores estratégicos identificados por la NIS 2 (coordinación mensual)	1,00%	1,00%
						Sub 2. Coordinación mensual con la IP de colectivos infrarrepresentados y personas con discapacidad	1,00%	1,00%
						Sub 3. Cooperación internacional con organismos público-privados (OEA, multinacionales, WEF)	1,00%	1,00%
						Sub 4. Ampliación del Summer Bootcamp a norte de África, Oriente Medio y este de Europa	1,00%	1,00%
						Competiciones de hacking ético territoriales		
						Sub 1. Colaboración con las asociaciones y entes locales para la organización de CTF	1,50%	1,50%
						Sub 2. Reuniones con los organizadores de las asociaciones	1,50%	1,50%

LÍNEA 1.2. Capacidades para la ayuda, soporte y respuesta frente a riesgos, amenazas e incidentes								
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	Respuesta incidentes de ciberseguridad para ciudadanos y entidades de derecho privado		
						Sub 1. Refuerzo de las capacidades del departamento de gestión de crisis y emergencias	0,32%	0,32%
						Sub 2. Refuerzo de las capacidades del 017, mediante colaboración con la FEMP	0,32%	0,32%
						Sub 3. Impulso a la colaboración con los CERT autonómicos y la red de CERTS privados	0,34%	0,34%
						Sub 4. Impulso a las capacidades de IA aplicadas en INCIBE-CERT	0,34%	0,34%
						Sub 5. Desarrollo de guía para aplicación en la gestión de crisis en empresas	0,34%	0,34%
						Sub 6. Diseño y puesta en marcha de un nuevo procedimiento de escalado a la DG de incidentes de alto interés en 24x7	0,34%	0,24%
						Respuesta incidentes de ciberseguridad para operadores críticos y esenciales		
						Sub 1. Lanzamiento y ejecución del portfolio de servicios para sectores estratégicos	1,00%	1,00%
						Sub 2. Ampliación del servicio de divulgación de vulnerabilidades	1,00%	1,00%
						Fortalecimiento capacidades internas soporte y respuesta		
						Sub 1. Adecuación del SGSI a la nueva versión de la norma UNE ISO/IEC 27001:2023	1,00%	1,00%
						Sub 2. Diseño y construcción del mapa normativo en ciberseguridad con actualización periódica según evolución de las diferentes normativas	1,00%	1,00%
	MEDIDA 4 Fortalecimiento de las capacidades de resiliencia y recuperación de los operadores de servicios críticos y proveedores de sectores estratégicos	6%	Acciones para el fortalecimiento de las capacidades de resiliencia y recuperación de los operadores de servicios críticos y proveedores de sectores estratégicos	100%		Operadores de servicios críticos y proveedores de sectores estratégicos		
						Sub 1. Incremento de la difusión de alertas de incidentes por sectores estratégicos en régimen 24 horas	0,48%	0,48%
						Sub 2. Diseño y definición del modelo de guía de gestión de incidentes por sectores estratégicos adaptadas a la NIS 2	0,48%	0,48%
						Sub 3. Creación y desarrollo del laboratorio de gestión de incidentes del sector de transporte viario y ferroviario	0,51%	0,51%
						Sub 4. Lanzamiento del nuevo servicio de ciber ejercicios nacionales	0,51%	0,51%
						Sub 5. Implantación de mejoras en la seguridad de los mecanismos de control de acceso	0,51%	0,51%
						Sub 6. Migración de herramientas o servicios al nuevo entorno orientado a microservicios basado en microservicios	0,51%	0,51%
						Nuevas capacidades tecnológicas para mejorar la prestación de los servicios		
						Sub 1. Desarrollo de una nueva versión de la plataforma de acceso a los servicios que INCIBE presta a entidades estratégicas	1,50%	1,50%
						Sub 2. Desarrollo de una nueva versión del sistema de descubrimiento y monitorización de la seguridad de activos de entidades estratégicas (y generación de informes tiresias)	1,50%	1,50%
LÍNEA 1.3. Impulso de la colaboración público-privada y público-públicos y de la RSE								
10%	**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	Acciones para consolidar el entorno de ciberseguridad nacional		
						Sub 1. Seguimiento de convenios Fiscalía General del Estado y el Ministerio del Interior, y firma con CGPJ	3,00%	3,00%
						Sub 2. Impulsar las actuaciones internacionales en el seno del Consejo Nacional de ciberseguridad	3,00%	3,00%
	MEDIDA 6 Desarrollo de la Responsabilidad Social Empresarial de INCIBE	4%	Acciones para el desarrollo de la Responsabilidad Social Empresarial	100%		Acciones para el desarrollo de la RSE		
						Sub 1. Impulso a los programas de prácticas de formación de la FP y universitario	2,00%	2,00%
						Sub 2. Impulso a proyectos de participación ciudadanía en ciberseguridad (Tu barrio Ciber)	2,00%	2,00%

OBJETIVO 2: Impulso del ecosistema empresarial del sector de la ciberseguridad								
Peso (LA)	**Línea de acción de Actuación y Medida**	**Peso (MED)**	**Indicador de medida**	**Valor Meta**	**IMPACTO (outcome)**	**Subindicador (componentes del Indicador)**	**Valor Cierre**	**VF fijo**
LÍNEA 2.1. Impulso y fortalecimiento de la industria de ciberseguridad								
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	Desarrollo de un programa de acompañamiento a nuevos proyectos		
						Sub 1. Programa de apoyo a la creación de spin-off universitarias en ciberseguridad	3,50%	3,50%
						Sub 2. Gestión de la IP de Emprendimiento - conversión de proyectos	3,50%	3,50%
	MEDIDA 8 Internacionalización de la industria de ciberseguridad	7%	Acciones de internacionalización	100%		Incorporación de acciones de internacionalización		
						Sub 1. Acciones de apoyo a las empresas de la industria nacional de ciberseguridad que impulsen su crecimiento internacional	1,75%	1,75%
						Sub 2. Apoyo a la inversión extranjera en el lanzamiento de proyectos de ciberseguridad en España	1,75%	1,75%
						Sub 3. Acciones de refuerzo a los fondos de inversión nacionales en ciberseguridad	1,75%	1,75%
						Sub 4. Atracción de compradores, inversores y delegaciones internacionales	1,75%	1,75%
LÍNEA 2.2. Fomento de la I+D+i en ciberseguridad								
14%	**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%	Compra Pública Innovadora		
						Sub 1. Desarrollo de la 4ª convocatoria de la CPI	2,80%	2,80%
						Sub 2. Despliegue de una estrategia de recuperación de la inversión del programa CPI	2,10%	2,10%
						Sub 3. Lanzamiento de las convocatorias de financiación en cascada del NCC	2,10%	2,10%
	MEDIDA 10 Desarrollo de programas de I+D+i y fortalecimiento de las capacidades en ciberseguridad por universidades	7%	Acciones de fortalecimiento e impulso de la I+D+i	100%		Invitación pública para la colaboración en la promoción de Cátedras de Ciberseguridad en España		
						Sub 1. Coordinación mensual con los responsables de Cátedras de Universidades	3,50%	3,50%
						Sub 2. Coordinación mensual con los responsables de Proyectos Estratégicos de Universidades	3,50%	3,50%
LÍNEA 2.3. Promoción del talento en ciberseguridad								
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	Actuaciones formativas especializadas en ciberseguridad		
						Sub.1 Despliegue de la oferta formativa de 10.260 plazas en ciberseguridad a través de la red académica	4,00%	4,00%
	MEDIDA 12 Identificación e impulso de acciones formativas	4%	Fomento e integración del talento	100%		Programa de retención de talento en INCIBE		
						Sub 1. Incremento de la inversión en formación del personal de INCIBE	2,00%	2,00%
						Sub 2. Actualización del estudio Análisis y diagnóstico del mercado de la ciberseguridad y talento de ciberseguridad en España	2,00%	2,00%

OBJETIVO 3: Estímulo de España como nodo internacional en el ámbito de la ciberseguridad								
Peso (LA)	**Línea de acción de Actuación y Medida**	**Peso (MED)**	**Indicador de medida**	**Valor Meta**	**IMPACTO (outcome)**	**Subindicador (componentes del Indicador)**	**Valor Cierre Diciembre**	**VF fijo**
LÍNEA 3.1. Consolidación del programa de trabajo de ciberseguridad europeo								
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	NCC-ES INCIBE		
						Sub 1. Liderazgo de iniciativas con las Agencias Europeas relacionadas con la ciberseguridad y ciberdefensa	1,60%	1,60%
						Sub 2. Participación activa en los WG del NCC	1,20%	1,20%
						Sub 3. Impulso a la oficina de proyectos europeos	1,20%	1,20%
	MEDIDA 14 Alineamiento con el marco regulatorio y legislativo europeo	4%	Acciones para el desarrollo del posicionamiento de INCIBE	100%		Actuaciones para facilitar el alineamiento y las capacidades de INCIBE		
						Sub 1. Cooperación internacional en el refuerzo de las capacidades de respuesta en sectores estratégicos en el marco de la OTAN y aliados estratégicos	4,00%	4,00%
LÍNEA 3.2. Desarrollo del nodo de ciberseguridad nacional								
14%	**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	Centros Demostradores de ciberseguridad		
						Sub 1. Puesta en marcha del centro demostrador de León siguiendo el programa operativo (TEST CENTER)	3,50%	3,50%
						Sub 2. Comenzar los procesos de acreditación en la ISO 17025 como laboratorio de ensayo y calibración (CENTRO ACREDITADOR)	3,50%	3,50%
	MEDIDA 16 Puesta en marcha de proyectos territoriales de transformación digital	7%	Acciones para apoyar proyectos tractores fomentando el intercambio de conocimiento	100%		RETECH		
						Sub 1. Completar el despliegue de RETECH en el conjunto de las CCAA	3,50%	3,50%
						Sub 2. Desarrollo de los programas operativos	3,50%	3,50%
LÍNEA 3.3. Identificación e implantación de actuaciones y controles para reducir la exposición al riesgo								
7%	**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	Desarrollo de instrumentos jurídicos		
						Sub 1. Adecuación de los mecanismos de INCIBE a los requisitos del MRR (transformación EPE, adendas convenios)	3,00%	3,00%
	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%		Seguimiento y ejecución del PRTR		
						Sub 1. Adecuación de los procedimientos a los requisitos del MRR	0,80%	0,80%
						Sub 2. Diseño y supervisión del Plan Antifraude	0,80%	0,80%
						Sub 3. Diseño del procedimiento de comunicación del PRTR para entidades	0,80%	0,80%
						Sub 4. Supervisión del cumplimiento del procedimiento de comunicación del PRTR para entidades	0,80%	0,80%
						Sub 5. Análisis de la evolución mensual de impactos en comunicación	0,80%	0,80%



Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD