NCC-ES
SPAIN CYBERSECURITY COORDINATION CENTRE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPAIN

LAND OF CYBERSECURITY

Agenda y logística

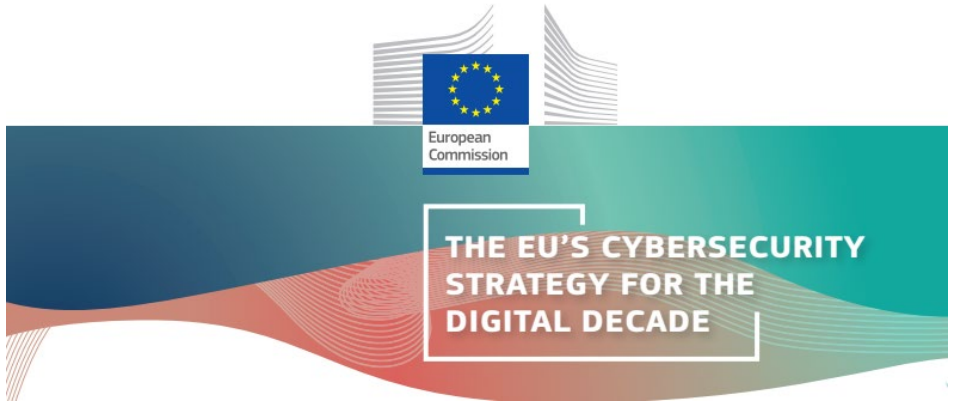
09:30-09:35	Presentación y bienvenida a la jornada Miguel Ángel Cañada, INCIBE
09:35-10:10	Presentación del NCC-ES, ecosistema ECCC y DIGITAL Miguel Ángel Cañada, INCIBE
10:10-10:40	Nuevas convocatorias DIGITAL-ECCC-2024-DEPLOY-CYBER-06 Héctor Laiz, INCIBE
10:40-10:55	Horizon Europe Maite Boyero, CDTI
10:55-11:10	Cómo lograr una propuesta exitosa Marco Lozano, INCIBE
11:10-11:25	Ruegos y preguntas
11:25-11:30	Cierre de la jornada Miguel Ángel Cañada, INCIBE

nccspain@incibe.es

www.incibe.es/ncc-es

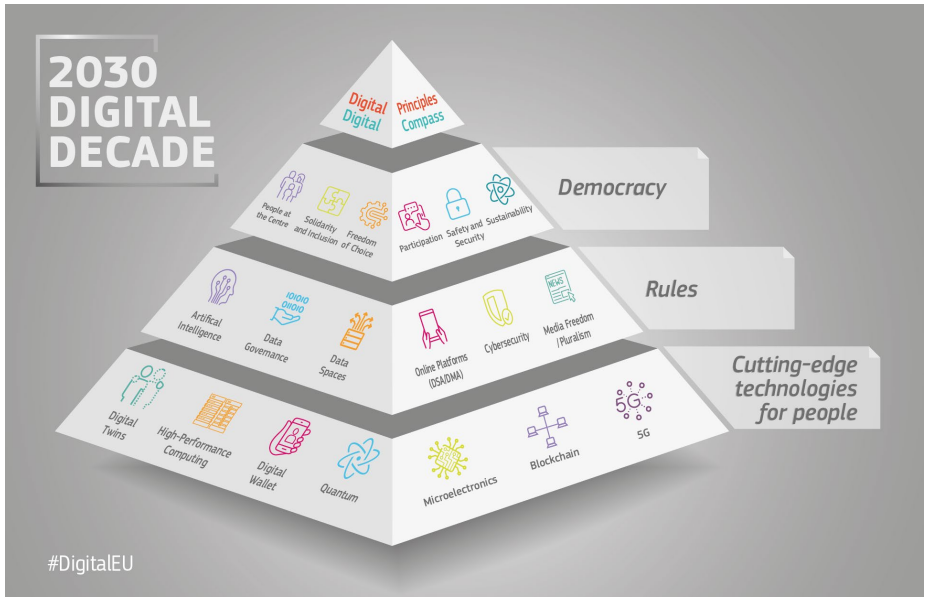
Estrategia Europea de Ciberseguridad para la Década Digital

- La estrategia describe cómo la UE puede aprovechar y reforzar todos sus instrumentos y recursos para **ser tecnológicamente soberana**. También expone cómo la UE puede intensificar su cooperación con socios de todo el mundo que comparten nuestros **valores de democracia, Estado de Derecho y derechos humanos**.



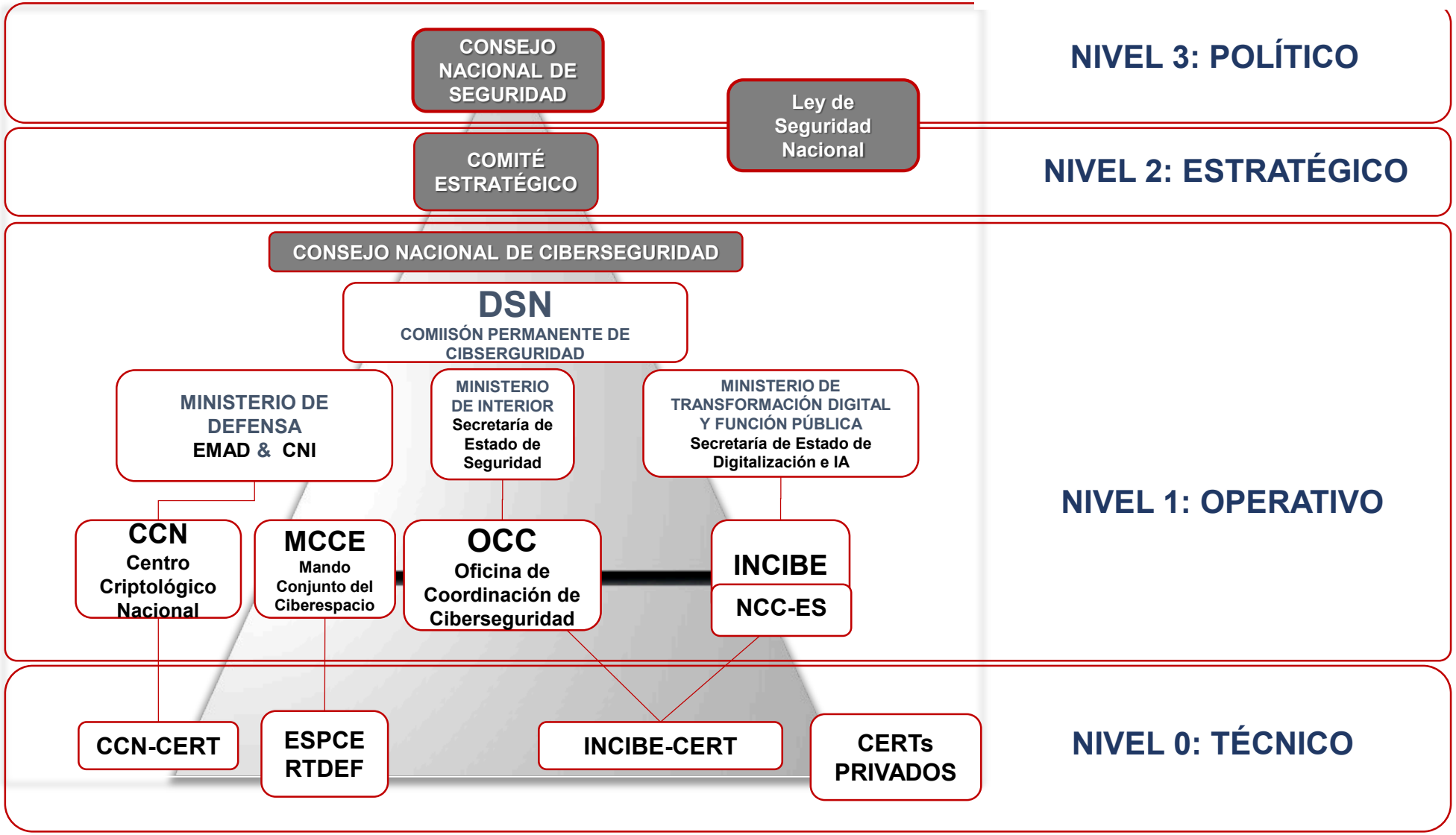
Ámbitos de actuación

- **Resiliencia, soberanía tecnológica y liderazgo**
- **Capacidad operativa** para prevenir, disuadir y responder
- **Cooperación** para promover un ciberespacio global y abierto.



Cofinanciado por la Unión Europea
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Gobernanza Ciberseguridad en España



Cofinanciado por la Unión Europea

Horizonte 2026

Digitalización

Conectividad

Inteligencia Artificial

Disrupción

IoT

e-Life

Superficie Riesgo

Gestión del riesgo

Oportunidad

Cofinanciado por la Unión Europea

Alcance de la Iniciativa

Alcance

- **Reforzar las capacidades** europeas en materia de ciberseguridad
- **Proteger** nuestra economía y a la sociedad frente a los **ciberataques**,
- Mantener y promover la **excelencia en la investigación** y reforzar la **competitividad de la industria** de la UE

Septiembre 2017	Cumbre Jefes de Estado Tallín 2017: Mandato de convertir la UE en **líder mundial de ciberseguridad en 2025**
Septiembre 2018	La Comisión presenta la **propuesta de Reglamento**
Diciembre 2020	Estos Estados miembros **confirman el acuerdo**
Enero 2021	**Adopción formal** por parte del Parlamento Europeo y del Consejo
Junio 2021	**Entrada en vigor** del reglamento
2021-2022	**Puesta en macha** del ECCC y de los NCCs (designación de INCIBE)

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026

Estructura y Gobernanza

Estructura Operativa

- **Centro Europeo de Competencia en Ciberseguridad** con sede en **Bucarest (ECCC)**
- **Centros de Coordinación Nacional (NCC)** en cada uno de los estados miembros (27)
- Mantener y promover la **Comunidad de Competencias en Ciberseguridad,** formada por las 27 Comunidades Nacionales en torno a los NCCs

Gobernanza

- Miembros: **Comisión Europea** (DG Connect) + **Estados Miembros** (ECCC+NCCs)
- **Consejo de Administración**
- **Director Ejecutivo**
- **Grupo Consultivo Estratégico**

Otros aspectos relevantes

- Papel fundamental en el **Programa Europa Digital** [Reglamento (UE) 2021/694, síntesis]
- Contribuye al programa **Horizonte Europa**, y otros programas
- El reglamento crea el marco para **coordinar la inversiones en ciberseguridad** y los Estados miembros.

Cofinanciado por la Unión Europea

Misión del ECCC y la Red

El Centro Europeo de Competencia en Ciberseguridad (ECCC), ubicado en Bucarest, fortalecerá las **capacidades** de la comunidad tecnológica de ciberseguridad, protegerá nuestra economía y sociedad de los **ciberataques**, mantendrá la excelencia en la **investigación** y reforzará la **competitividad** de la industria de la UE en este campo.

Es misión del ECCC (art. 3):

- Apoyar la **resiliencia y la fiabilidad de las redes y los sistemas de información.**
- Apoyar las **capacidades, las competencias y los medios tecnológicos** de la Unión en relación con la **resiliencia y la fiabilidad de las infraestructuras de las redes y sistemas de información.**
- Aumentar la **competitividad y liderazgo de la UE** en materia de ciberseguridad

Debe contribuir:

- La aparición de **soluciones para los retos de ciberseguridad** a los que se enfrentan los sectores público y privado y apoyar el despliegue efectivo de estas soluciones.
- Tomar **decisiones estratégicas de inversión**, poniendo en común los recursos de la UE, de los Estados miembro y de la Industria.
- **Aplicar el apoyo financiero**, relacionado con la ciberseguridad, de los programas Horizonte Europa y Europa Digital.

Cofinanciado por la Unión Europea

Funciones ECCC (Art. 5)

Funciones Estratégicas

- Elaborar y supervisar la ejecución del **programa estratégico**
- Crear **sinergias entre la Comunidad de Competencias** en la ejecución de programas europeos: prioridades de trabajo, reforzar la excelencia del sector (especialmente las pymes), apoyo y asistencia a empresas emergentes, pymes…
- Crear **sinergias entre instituciones y organismos de la UE**, especialmente ENISA
- **Coordinar los NCCs** y asegurar el **intercambio de información** entre ellos y entre miembros de la Comunidad
- Proporcionar **asesoramiento especializado** industria, tecnológico y de IDi en ciberseguridad
- Facilitar el **uso de los resultados de los proyectos** de investigación e innovación, y su aplicabilidad

Funciones de Ejecución

- Establecer y ejecutar el **plan programa de trabajo anual**, así como coordinar y administrar los trabajo de la Red
- Prestar **asesoramiento especializado** a impulsar la generación de **competencias digitales avanzadas**
- Impulsar la **implantación de infraestructuras TIC**
- Potenciar las **sinergias y coordinación entre el ámbito civil y militar** en ciberseguridad

Cofinanciado por la Unión Europea
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Centro Nacional de Coordinación (NCC-ES)

INCIBE designado como Centro de Coordinación Nacional (NCC-ES) por el *Consejo de Nacional de Ciberseguridad*

Funciones (art. 7)

- Actuar como **punto de contacto y coordinación** a nivel nacional para apoyar al Centro de Competencia en su misión y objetivos, cooperar con el resto de agentes competentes, la industria, el sector público, la comunidad académica y de investigación y la ciudadanía, teniendo en cuenta los retos en ciberseguridad.
- **Puesta en marcha de proyectos transfronterizos** y acciones conjuntas financiados a través de la UE.
- Proporcionar **conocimientos especializados** teniendo en cuenta los retos específicos en ciberseguridad, a nivel nacional y regional.
- **Establecer sinergias** con actividades pertinentes a nivel nacional, regional y local, en particular las políticas enunciadas en las estrategias nacionales de ciberseguridad.
- Prestar **asistencia técnica** para los proyectos gestionados por el ECCC en relación a su misión y objetivos.
- Promover **programas educativos** de ciberseguridad.
- Evaluar las **solicitudes Nacionales para formar parte de la Comunidad**.
- Crear una **Comunidad de Competencia público-privada** a escala nacional.

Cofinanciado por la Unión Europea

Comunidad Nacional de Competencia en Ciberseguridad

La Comunidad involucrará a un grupo amplio, interdisciplinario, abierto y diverso de partes interesadas europeas del ámbito de la tecnología de ciberseguridad, incluyendo en particular a **entidades de investigación, industria de la oferta y la demanda y el sector público**.

Contará con la participación de los **centros nacionales de coordinación**, de los **centros europeos de innovación digital**, cuando proceda, así como de las instituciones, órganos y **organismos con conocimientos especializados** de la Unión, como ENISA.

Funciones de los miembros de la Comunidad

- **Apoyar al Centro de Competencia** a cumplir su misión y realizar sus objetivos.
- Trabajarán en estrecha **colaboración** con el Centro de Competencia y los Centros Nacionales de Coordinación.
- Participarán, cuando proceda, en los **grupos de trabajo** para llevar a cabo actividades específicas previstas en el programa de trabajo anual.
- Apoyarán al Centro de Competencia y a los NCCs en la **promoción de proyectos específicos**.

Cofinanciado por la Unión Europea

Agenda Estratégica (1)

Declaraciones de impacto a corto plazo

- Para 2027, el ECCC y la Red de NCCs habrán financiado a las **PYME europeas en el desarrollo y uso de tecnologías, servicios y procesos estratégicos de ciberseguridad** mediante un mecanismo coordinado de financiación en cascada a través de las NCC y la cofinanciación nacional que reduce el umbral de solicitud para las PYMEs.
- Para 2027, el ECCC y la Red de NCCs habrán apoyado y **aumentado la mano de obra profesional en ciberseguridad**, tanto en cantidad como en calidad, mediante la normalización y la certificación de competencias en ciberseguridad e inversiones en educación y formación de profesionales de la ciberseguridad.
- Para 2027, el ECCC y la Red de NCCs habrán **reforzado la experiencia en investigación, desarrollo e innovación y la competitividad** de la comunidad de ciberseguridad de la UE mediante el desarrollo y la aplicación de un plan de acción eficaz y coherente.

Cofinanciado por la Unión Europea

Agenda Estratégica (2)

Prioridades. Eje 1. Procesos y herramientas de gestión de la información sobre ciberseguridad y gestión de riesgos

- 1.1.1 Desarrollar y aplicar tecnologías, servicios y procesos para apoyar el **intercambio de información**, la **prevención** coordinada y colaborativa, la **detección y respuesta/recuperación** y la **investigación de incidentes** de ciberseguridad
- 1.1.2 Apoyar la concienciación y posterior adopción en la gestión de vulnerabilidades de las organizaciones y el desarrollo de iniciativas de **divulgación coordinada de vulnerabilidades (CVD)** para corregir vulnerabilidades, en consonancia con las soluciones de ENISA
- 1.1.3 Desarrollar y aplicar soluciones innovadoras de **modelización y simulación**
- 1.1.4 Garantizar la disponibilidad de **herramientas de ciberseguridad de fácil acceso y uso para las PYME**
- 1.2.1 Aumentar la **resiliencia de las entidades esenciales e importantes** definidas en NIS2
- 1.2.2 Apoyar el desarrollo y la adopción de **herramientas de automatización** para los procesos de ciberseguridad mediante el desarrollo y despliegue de soluciones de ciberseguridad **basadas en IA**
- 1.2.3 Promover la **seguridad y la privacidad desde el diseño**
- 1.2.4 Apoyo a la implantación de soluciones de ciberseguridad en el **desarrollo de productos y su uso prolongado en entornos de TI/OT** (tanto antiguos como nuevos)
- 1.2.5 Apoyo al **desarrollo, la implantación y la garantía (uso de auditorías) de la criptografía post-cuántica** en productos y servicios seguros

Agenda Estratégica (3)

Prioridades. Eje 2. Apoyar y hacer crecer el talento en ciberseguridad

- 2.1.1 Garantizar el desarrollo, el ajuste y la adopción de **currículos educativos alineados con las necesidades del mercado**
- 2.1.2 Desarrollar **herramientas comunes y plataformas de fácil acceso para la educación técnica práctica, la formación y las oportunidades de ensayo**
- 2.1.3 Desplegar campañas específicas para el **desarrollo de carreras en ciberseguridad**
- 2.1.4 Promover un enfoque de **seguridad y privacidad "desde el diseño" en la formación y la educación**
- 2.1.5 Promover el **desarrollo de capacidades de los ciberprofesionales en materia de gestión y prevención** previas a las amenazas
- 2.1.6 **Aumentar la concienciación** sobre las amenazas a la ciberseguridad, el modus operandi de los actores de las amenazas y el impacto potencial
- 2.2.1 Garantizar la **adopción y aplicación de marcos de competencias de ciberseguridad**
- 2.2.2 Apoyar el desarrollo y la difusión de **sistemas de evaluación y certificación de competencias**

Agenda Estratégica (4)

Prioridades. Eje 3. Refuerzo de la I+D+i en el ecosistema europeo de ciberseguridad

- 3.1.1 **Apoyar a las organizaciones expertas y a los profesionales de la criptografía post-cuántica** para que lideren el desarrollo de algoritmos de criptografía post-cuántica adecuados y robustos
- 3.1.2 Desarrollar una **estrategia de adopción de la criptografía post-cuántica** con prioridades basadas en análisis de riesgos
- 3.2.1 Fomentar y facilitar la **adopción por parte de la industria, incluidas las PYME, de sistemas europeos maduros de certificación de la ciberseguridad** y evaluaciones de la conformidad de los requisitos esenciales para los productos y servicios de ciberseguridad
- 3.2.2 Mejorar los sistemas paneuropeos de **evaluación de la conformidad**
- 3.3.1 Desarrollar la comprensión de la **comunidad de ciberseguridad** mediante una **cartografía dinámica de sus capacidades** y posibilidades y la identificación de posibles oportunidades de colaboración
- 3.3.2 Apoyo a la **adopción de tecnologías y productos de ciberseguridad de la UE**
- 3.3.3 Apoyo a un **mercado abierto de ciberseguridad en toda la UE**
- 3.4.1 Fomentar la **colaboración entre instituciones de enseñanza superior, investigación interdisciplinar e innovación**
- 3.4.2 Promover la **creación y capacitación de iniciativas de cooperación** del estilo de los Centros de Análisis e Intercambio de Información (ISAC)
- 3.4.3 Fomentar la **colaboración para mejorar la ciberresiliencia**

Cofinanciado por la Unión Europea
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ECCC: Una Oportunidad para la I+D+i en ciberseguridad

Impulso Financiero

Mecanismos directos y *financiación en Cascada*

Real Decreto 204/2023, de 28 de marzo, por el que se modifica el Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital.

1.650 M€

(financiación ciberseguridad 2021-2027)

1.600 M€

(Cluster III ciberseguridad 2021-2027)

8.000 M€

(2021-2027)

Apoyo y Dinamización

- I+D+i tecnologías emergentes
- Pymes e Industria Ciber
- Impacto Multisectorial (energía, salud, telco, manufacturero, público, financiero, espacio…)
- Soluciones de uso civil y militar
- Fomento del Empleo y desarrollo del Talento
- Sinergias con Comunidad y órganos europeos

Cofinanciado por la Unión Europea

INSTITUTO NACIONAL DE CIBERSEGURIDAD

DIGITAL EUROPE PROGRAMME: Qué es el DEP

Transformación digital & resiliencia & soberanía digital

5 áreas

- SUPERCOMPUTACION
- INTELIGENCIA ARTIFICIAL
- CIBERSEGURIDAD
- HABILIDADES DIGITALES AVANZADAS
- USO TECNOLOGIA SOCIEDAD Y EMPRESAS

7.600 M€
DEP

1.650 M€
DEP Ciber

Cerrar la brecha entre la **investigación** en tecnología digital y su **implementación** en el mercado.

Beneficiará a los **ciudadanos y empresas del ámbito europeo** con especial énfasis en las **PYMEs**.

Cofinanciado por la Unión Europea
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DIGITAL EUROPE PROGRAMME: Objetivos

- Desplegar, coordinar y explotar una infraestructura integrada de **supercomputación y datos**, orientada a la demanda y a las aplicaciones, que sea fácilmente accesible para los usuarios públicos y privados.

- Desarrollar y reforzar las **capacidades y los conocimientos en materia de IA en la Unión**, incluida la creación y el refuerzo de recursos de datos de calidad y de los mecanismos de intercambio correspondientes, así como de bibliotecas de algoritmos, garantizando al mismo tiempo un enfoque centrado en el ser humano.

- Apoyar la **creación y adquisición de equipos, herramientas e infraestructuras de datos avanzados en materia de ciberseguridad**.
- Apoyar el **desarrollo de competencias digitales avanzadas** para aumentar el talento, reducir la brecha digital y fomentar una mayor profesionalidad, especialmente en lo que respecta a la computación de alto rendimiento y en la nube, el análisis de macrodatos, la ciberseguridad, las tecnologías de libro mayor distribuido,las tecnologías cuánticas, la robótica y la inteligencia artificial.
- Apoyar al **sector público y a los ámbitos de interés público**, para que **despliegen y accedan a las tecnologías digitales de vanguardia**, como la computación de alto rendimiento, la IA y la ciberseguridad.

DIGITAL EUROPE PROGRAMME

PLAN DE TRABAJO

2021-2022

- Creación de **SOCs europeos** interconectados
- Apoyo para ciberseguridad en el **sector salud**
- Despliegue de la **red de Centros de Coordinación Nacionales** (NCC)
- Ciberresiliencia, coordinación y **cyber ranges** europeos
- Securización de **infraestructuras estratégicas y tecnologías de 5G**
- Adopción de **soluciones innovadoras de ciberseguridad**
- Apoyo a la **implementación de la directiva NIS** y **Estrategias Nacionales** de ciberseguridad
- Capacidades de **testeo y certificación**

Cofinanciado por la Unión Europea

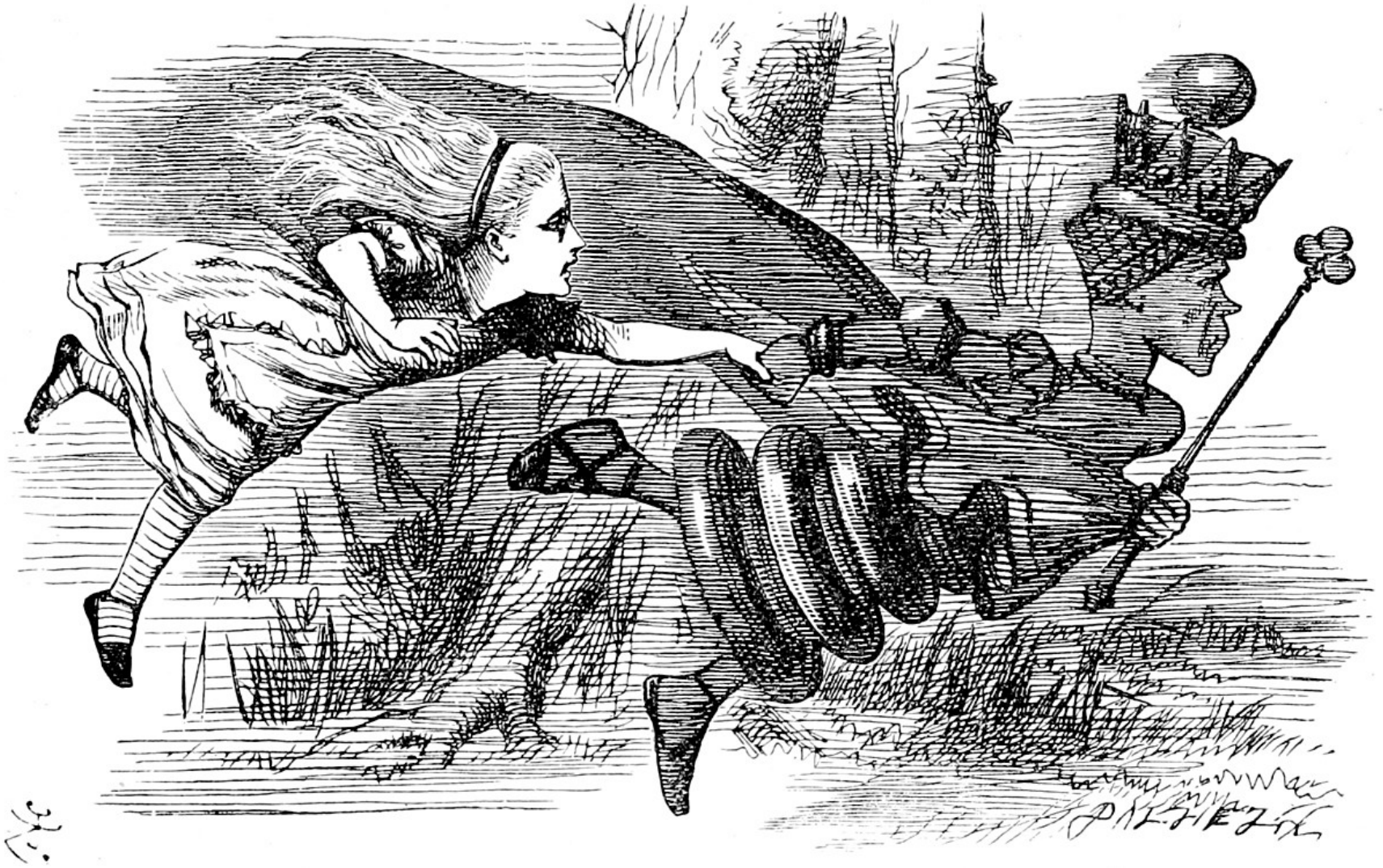
DIGITAL EUROPE PROGRAMME

PLAN DE TRABAJO

2023-2024

- Desarrollo de **capacidades de los SOCs europeos**
- **Inteligencia Artificial y tecnologías habilitadoras** en ciberseguridad
- Acciones relacionadas con la **Implementación de la Ley de Ciberresiliencia** (CRA)
- Transición hacia la **criptografía post cuántica** (PQC)
- Acciones relacionadas con el **Mecanismo de Emergencia de Ciberseguridad**, en línea con la Ley de Cibersolidaridad
- **Coordinación entre las esferas civil y de defensa**
- **Estandarización** en el área de ciberseguridad
- Apoyo a la **implementación de legislación europea** en ciberseguridad y **Estrategias Nacionales de Ciberseguridad**
- Acciones a desplegar por los **Centros de Coordinación Nacionales**
- **Soporte al programa**, evaluaciones y revisiones

Cofinanciado por la Unión Europea



«Para quedarte donde estás tienes que correr lo más rápido que puedas. Si quieres ir a otro sitio, deberás correr, por lo menos, dos veces más rápido».

A través del espejo y lo que Alicia encontró allí

(Lewis Carroll, 1871).

Cofinanciado por la Unión Europea

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Cofinanciado por la Unión Europea

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

NCC-ES INCIBE
Edificio INCIBE. Av. José Aguado 41.
24005 León. España
Tel: +34 987 877 189
nccspain@incibe.es

NCC-ES
SPAIN CYBERSECURITY COORDINATION CENTRE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD