INSTITUTO NACIONAL DE CIBERSEGURIDAD

INCIBE: La perspectiva institucional de la ciberseguridad. El papel del Derecho

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

017 TU AYUDA EN CIBERSEGURIDAD incibe_

España: Un modelo consolidado

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

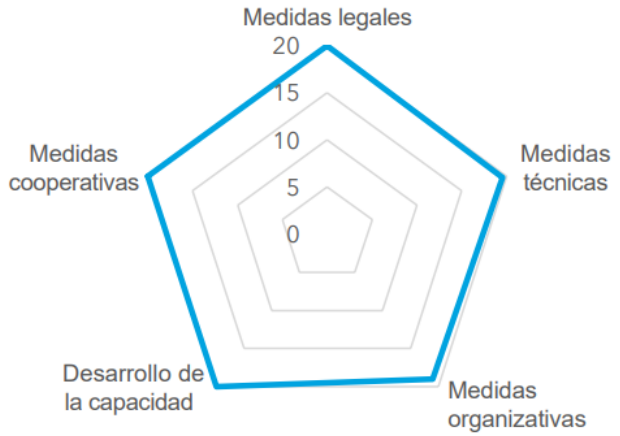
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Global Cybersecurity Index

4º Nivel global

2º Unión Europea

España



Nivel de desarrollo:
País desarrollado

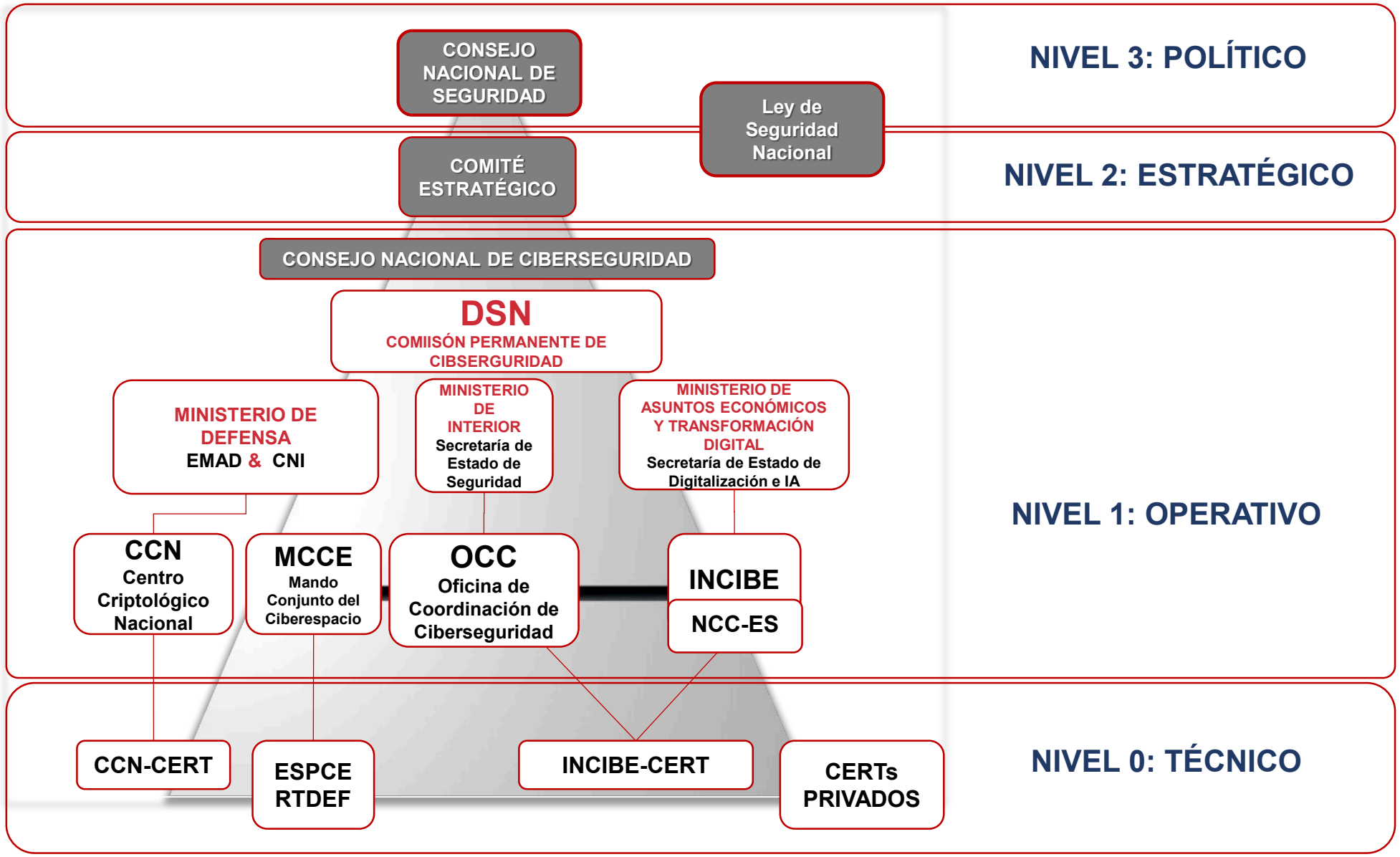
Área(s) de fortaleza relativa
Medidas legales, cooperativas, Desarrollo de la capacidad, Medidas técnicas

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
98,52	20,00	19,54	18,98	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Gobernanza Ciberseguridad en España



¿Dónde nos situamos?

Fuente: ILDEFE (Instituto Leonés de Desarrollo Económico, Formación y Empleo) https://www.ildefe.es

El viaje de INTECO a INCIBE

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

Nace INTECO

Instituto Nacional de
Tecnologías de la Comunicación

INTECO

Se focaliza en
el mundo de la ciberseguridad

Se transforma en INCIBE

Instituto Nacional
de Ciberseguridad de España

INCIBE-CERT

Trasposición Directiva NIS

Horizonte 2026

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

Digitalización

Conectividad
5G (76+ en 2020…) + Fibra (100% España en 2025)

Inteligencia Artificial
+otras tecnologías habilitadoras

Disrupción

IoT
Era post-latencia

e-Life
WEF 55% PIB global relacionado con lo digital en 2022

Superficie Riesgo

Gestión del riesgo
Más eventos de ciberseguridad

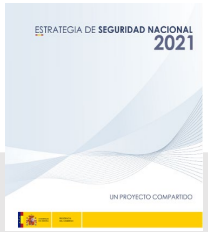
Oportunidad
Reforzar nuestras capacidades e industria de ciberseguridad

Apoyo a la Transformación Digital

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

MARCO ESTRATÉGICO SEGURIDAD NACIONAL



- Fortalecimiento de las capacidades de ciberseguridad de ciudadanos, pymes y profesionales
- Impulso del ecosistema empresarial del sector ciberseguridad
- **Fomento de España como nodo internacional en el ámbito de la ciberseguridad**

Plan estratégico

OBJETIVOS ESTRATÉGICOS (7)

LINEAS DE ACTUACIÓN (19)

MEDIDAS ESTRATÉGICAS (39)

PROGRAMAS

CONFÍA · incibe emprende · ciberinnova · talento HACKER

Iniciativas – Servicios - Soluciones

incibe-cert_ · 017 · is4k INTERNET SEGURA FORKiDS · protege tu empresa · OSI Oficina de Seguridad del Internauta · incibe emprende · enise Encuentro Internacional de Seguridad de la Información · Día Internet Segura · CIBERCOOPERANTES · summer bootcamp · cyber camp · Academia HACKER incibe_ · #mujeresciber

PERSONAS

- Personal de INCIBE
- Asistencias Técnicas

FINANCIACIÓN

- Presupuesto Ordinario
- Plan de Recuperación, Transformación y Resiliencia *España Puede*

CONOCIMIENTO

- Inteligencia Operaciones
- Productos de Conocimiento

Balance de ciberseguridad 2022

incibe_

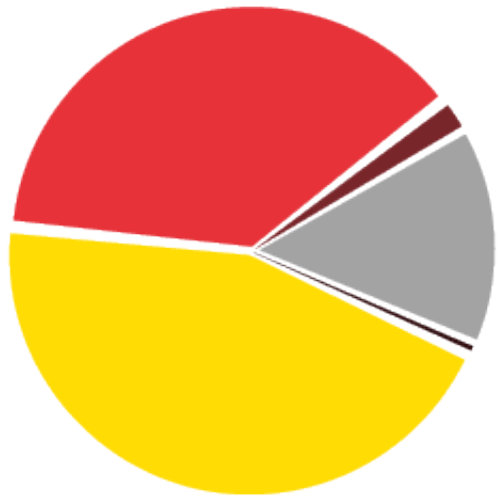
INSTITUTO NACIONAL DE CIBERSEGURIDAD

+118.820

incidentes gestionados

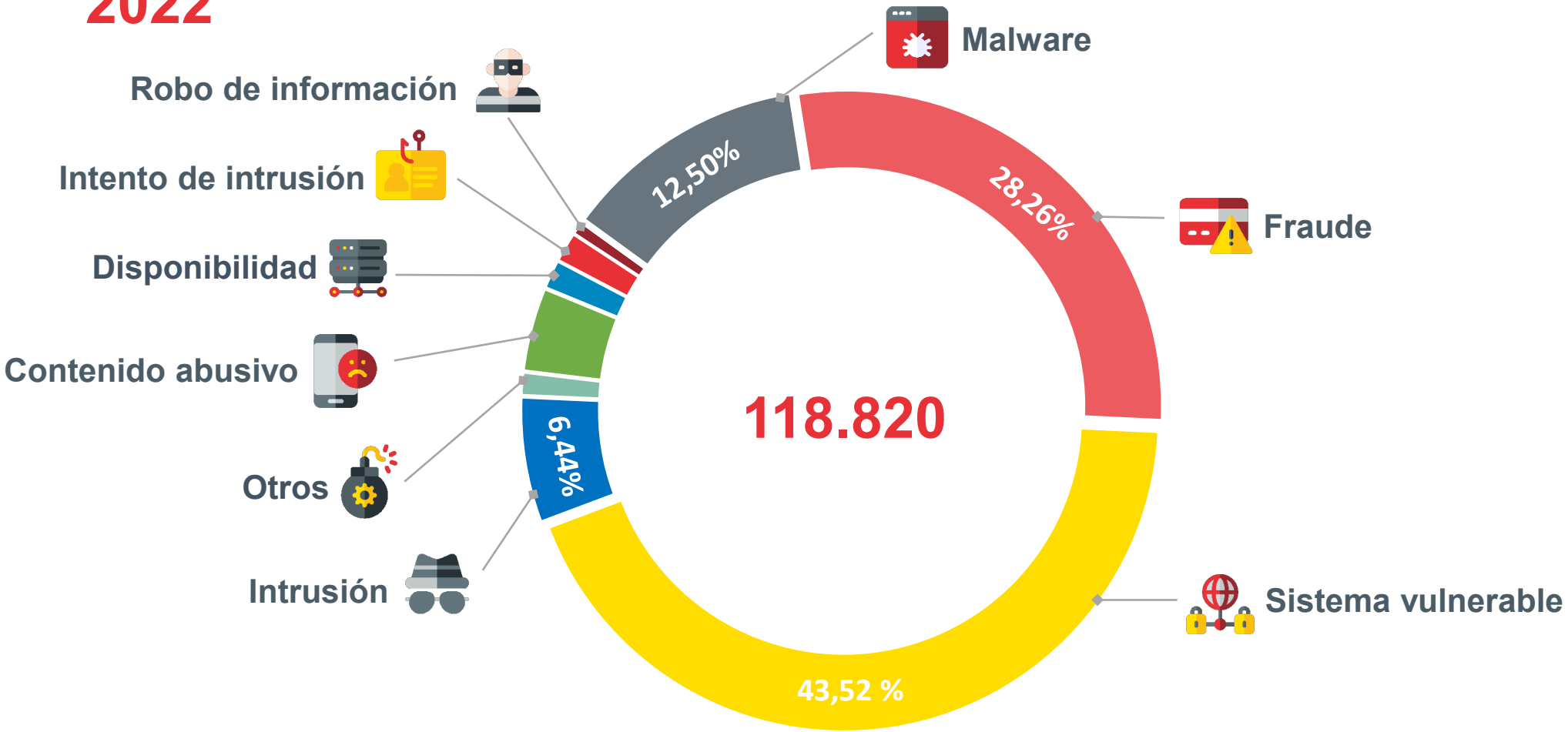
(+8,8% que en 2021)

Peligrosidad de los incidentes gestionados



- Baja 14,40%
- Media 47,72%
- Alta 38,08%
- Muy alta 1,81%
- Crítica 0,001%

Incidentes de Ciberseguridad 2022



Incidentes más destacados

110.294
(+22,3% que en 2021)

Ciudadanía y empresas

1 de cada 3
Filtración de datos
Datos sensibles, protegidos o confidenciales son copiados, transmitidos, vistos, robados o utilizados por una persona no autorizada.

2 de cada 5
Vulnerabilidades de sistemas tecnológicos
Fallo o debilidad de un sistema de información que pone en riesgo la seguridad del mismo.

48% Ciudadanos

2 de cada 3 son incidentes **relacionados con fraude** (por ejemplo, uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro).

52% Empresas

9 de cada 10 son incidentes **relacionados con sistemas vulnerables** (fallo o debilidad de un sistema de información que pone en riesgo la seguridad del mismo).

7.980
Red Académica

9 de cada 10
(87%) son incidentes relacionados con **sistemas vulnerables.**

*Sistema operativo de un dispositivo no actualizado o mal configurado.

546
Operadores críticos y esenciales*

- Energía **37,36%**
- Transporte **21,98%**
- Sistema financiero y tributario **17,77%**
- Agua **8,42%**

*Organización pública o privada responsable del funcionamiento de una infraestructura en la que exista una instalación, red, sistema o equipo físico o de tecnología de la información, catalogada como crítica por resultar indispensable.

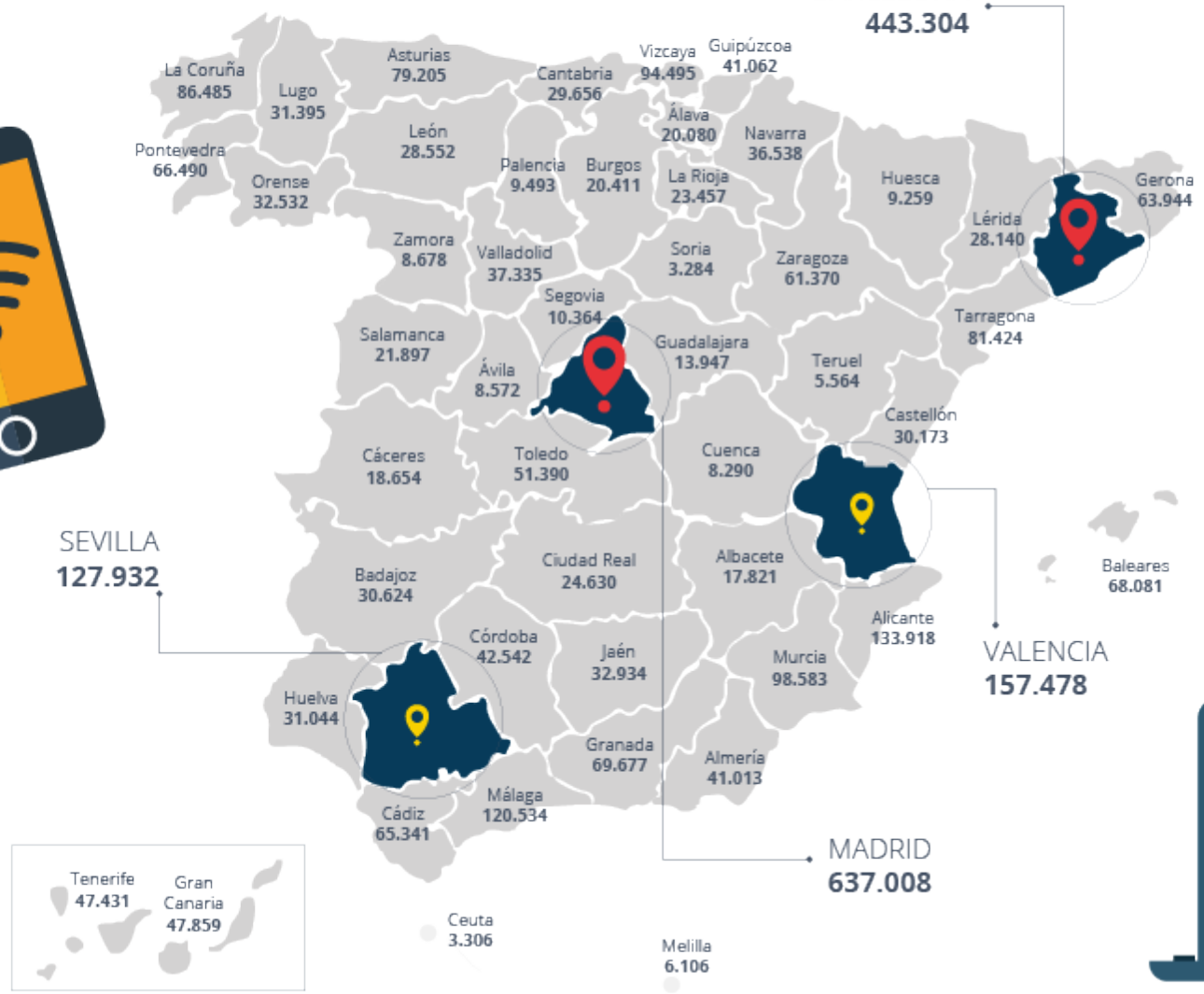
Peligrosidad de los incidentes gestionados

- Baja **2%**
- Media **54%**
- Alta **23%**
- Muy alta **21%**

3.309.302
dispositivos vulnerables*

*Puntos de conexión a Internet que han sido detectados como potencialmente expuestos, comprometidos o vulnerables (pueden estar afectados por algún software malicioso, mal configurados o expuestos en Internet de forma no deseada).

Vulnerabilidades destacadas



26.431
nuevas vulnerabilidades documentadas

* Número de vulnerabilidades descubiertas en dispositivos, tecnologías y productos de las que INCIBE dispone de información actualizada.

Consultas frecuentes 017

67.322

Consultas y problemas de la Línea de Ayuda de INCIBE

Un **55%** de las llamadas fueron para **prevenir un incidente**.

Un **45%** de las llamadas fueron para **solucionar un incidente**.

44.331 atendidas por vía telefónica

17.014 atendidas por canales de chat

5.977 atendidas por correo electrónico

1 de cada 4 consultas están relacionadas con ***phishing*** en sus dispositivos.

Un **10%** de la ciudadanía ha necesitado **asesoramiento sobre** la seguridad de sus **compras en Internet**.

5.098 personas han consultado al 017 por **suplantación de identidad**.

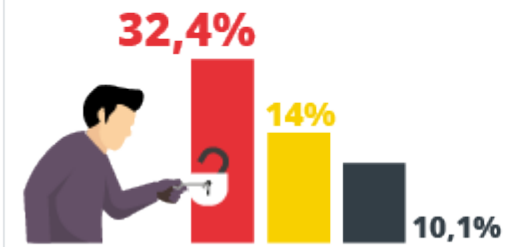
Un **5%** de la ciudadanía ha consultado sobre dudas de **privacidad y reputación online**.

788 usuarios han preguntado acerca de **falsas herencias, donaciones o premios**.

1.345 personas han llamado para exponer un problema de **sextorsión** (chantaje para que la víctima realice una acción o entregue dinero bajo la amenaza de publicar o compartir imágenes íntimas).

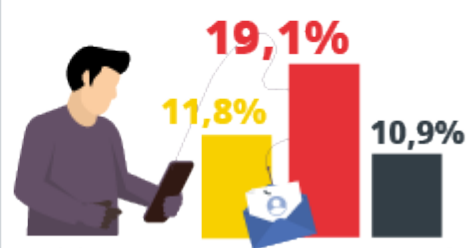
+700 personas han solicitado información acerca del acoso.

Consultas de menores y su entorno



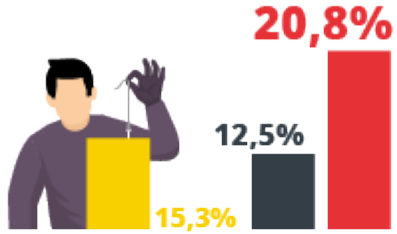
Completan el ranking: el *sexting*, la protección de dispositivos, los contenidos perjudiciales y la mediación parental, entre otras temáticas.

Consultas de la ciudadanía



Completan el ranking: el *vishing* (llamadas fraudulentas), la intrusión y la privacidad, entre otras.

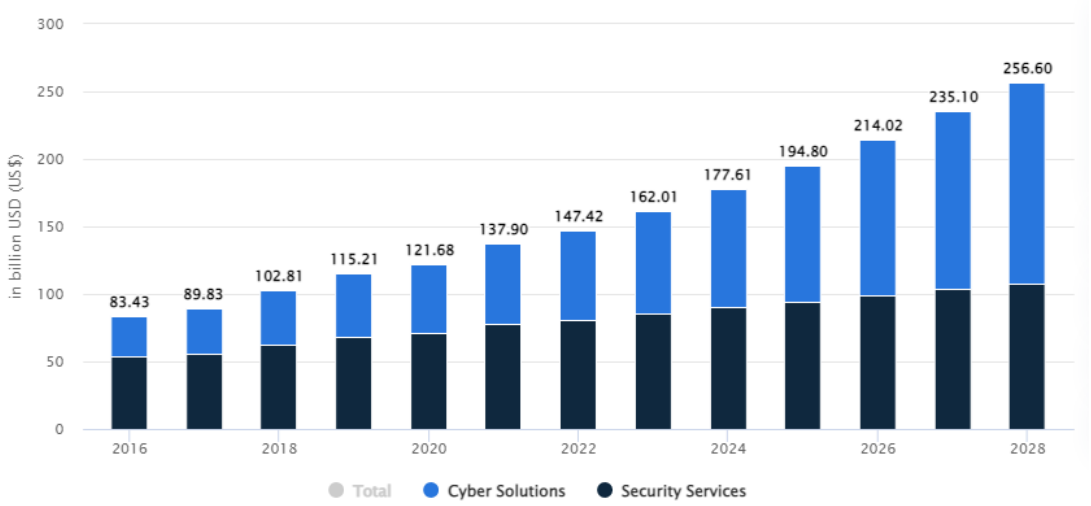
Consultas de empresas



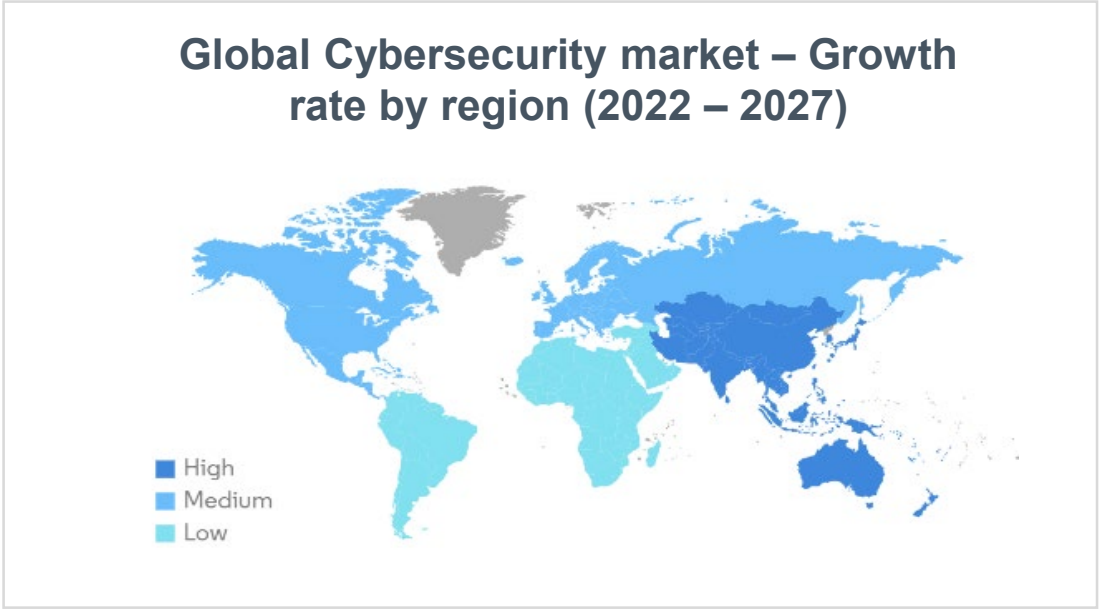
Completan el ranking: las llamadas fraudulentas, tanto de extorsión, como de estafas; el ciberataque tipo *ransomware*; la suplantación en redes sociales y los asuntos legales, entre otras.

Sector de la ciberseguridad en el mundo

- Se prevé que los ingresos del mercado de la ciberseguridad alcancen los 256.600 millones de dólares en 2028.
- El mayor segmento del mercado es el de soluciones ciber, con un volumen de mercado previsto de 148 700 millones de dólares en 2028.
- Se espera que los ingresos muestren una tasa de crecimiento anual (CAGR 2022-2026) del 9,68%.
- Se espera que Asia-Pacífico sea testigo del mayor crecimiento del mercado de soluciones de ciberseguridad (periodo 2022 - 2027).



Fuente: Statista



Fuente: Mordor Intelligence

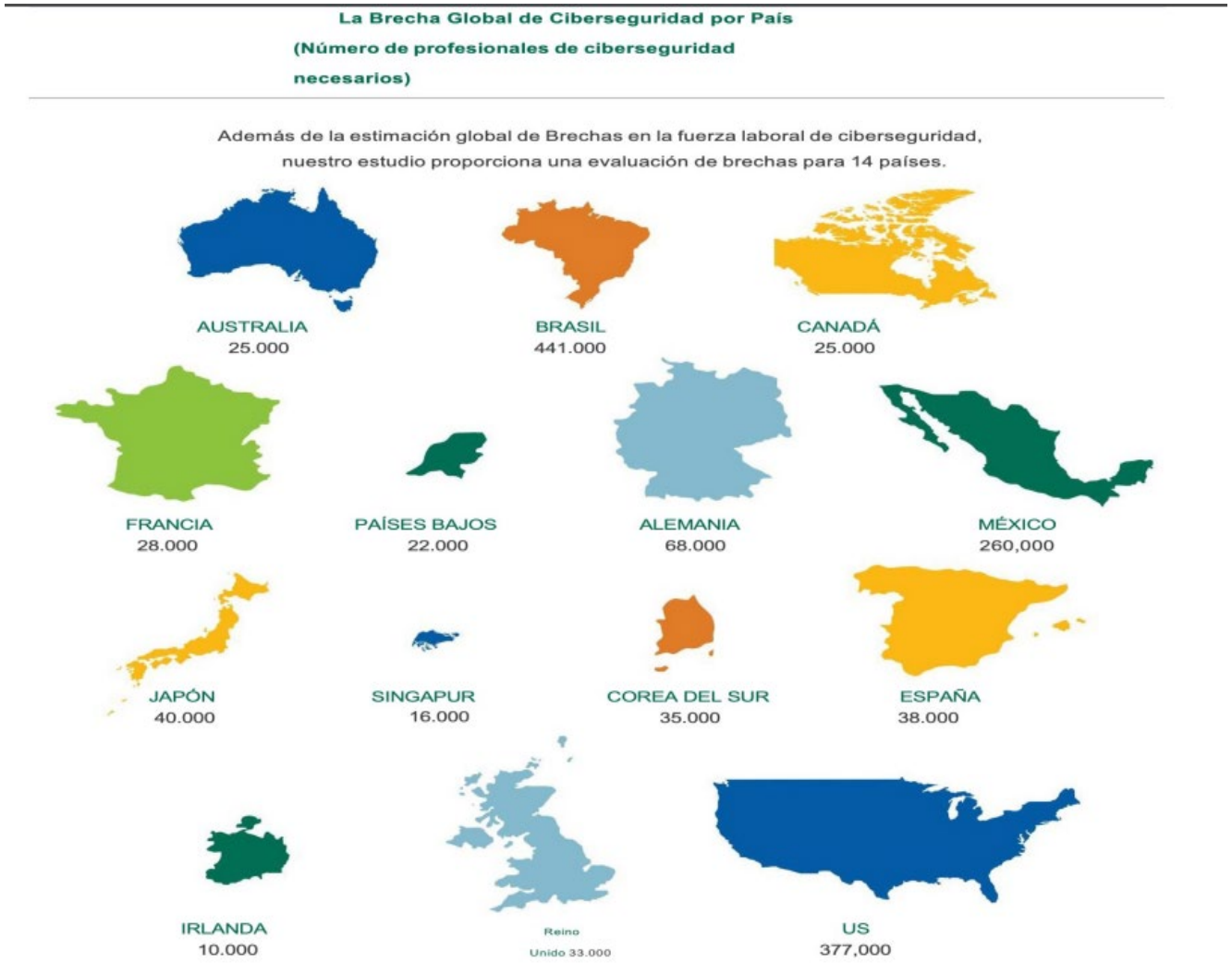
Sector de la ciberseguridad en Europa

Ranking GCI ITU		2016	2017	2018	2019	2020	2021	2022	2026
2	**UK**	$5,382.00	$5,692.00 *6%*	$6,566.00 *15%*	$7,238.00 *10%*	$7,588.00 *5%*	$8,641.00 *14%*	$9,518.00 *10%*	$13,580.00
13	**Germany**	$3,875.00	$4,390.00 *13%*	$5,076.00 *16%*	$5,527.00 *9%*	$5,849.00 *6%*	$6,571.00 *12%*	$7,178.00 *9%*	$9,574.00
9	**France**	$2,780.00	$3,119.00 *12%*	$3,605.00 *16%*	$3,913.00 *9%*	$4,100.00 *5%*	$4,611.00 *12%*	$5,073.00 *10%*	$6,790.00
16**	**Netherlands**	$1,244.00	$1,413.00 *14%*	$1,663.00 *18%*	$1,839.00 *11%*	$1,968.00 *7%*	$2,191.00 *11%*	$2,387.00 *9%*	$3,212.00
20	**Italy**	$1,221.00	$1,364.00 *12%*	$1,565.00 *15%*	$1,675.00 *7%*	$1,739.00 *4%*	$1,942.00 *12%*	$2,119.00 *9%*	$2,760.00
4	**Spain**	$966.80	$1,100.00 *14%*	$1,282.00 *17%*	$1,396.00 *9%*	$1,440.00 *3%*	$1,635.00 *14%*	$1,816.00 *11%*	$2,534.00
42**	**Switzerland**	$969.50	$1,051.00 *8%*	$1,181.00 *12%*	$1,311.00 *11%*	$1,412.00 *8%*	$1,560.00 *10%*	$1,696.00 *9%*	$2,341.00
15	**Sweden**	$841.70	$943.70 *12%*	$1,043.00 *11%*	$1,116.00 *7%*	$1,200.00 *8%*	$1,368.00 *14%*	$1,486.00 *9%*	$2,120.00
19	**Belgium**	$461.80	$520.70 *13%*	$605.00 *16%*	$662.20 *9%*	$693.20 *5%*	$776.70 *12%*	$847.70 *9%*	$1,137.00
8	**Portugal**	$117.00	$133.90 *14%*	$157.40 *18%*	$173.30 *10%*	$182.30 *5%*	$203.30 *12%*	$225.50 *11%*	$310.30

** No response to the questionnaire

Fuente: Statista

Brecha de talento en ciberseguridad por país



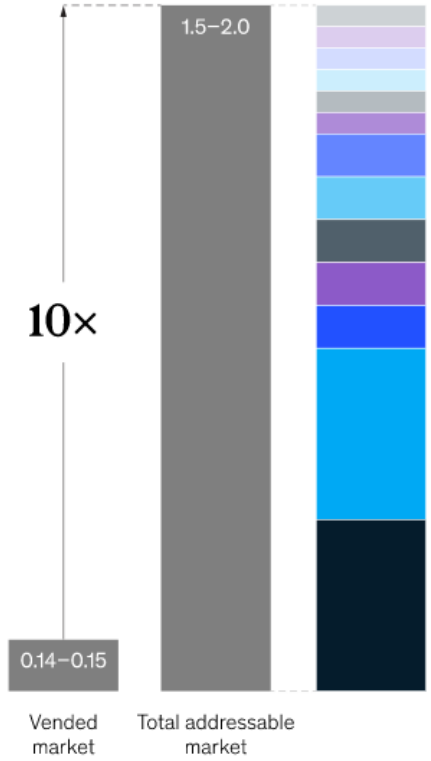
	2019	2020	2021
N / A	888,700	981,120	1,266,158
[illegible]	804,700	879,157	1,142,462
Canadá	84,000	101,963	123,696
LATAM	827,000	1,048,399	1,096,876
México	341,000	421,750	515,527
Brasil	486,000	626,650	581,349
EUROPA	543,000	830,187	1,086,146
[illegible]	289,000	365,823	300,087
Francia	121,000	118,302	146,808
Alemania	133,000	175,159	464,782
Irlanda	N / A*	14,212	15,028
España	N / A*	122,284	124,336
Países Bajos	N / A*	34,406	35,106
APAC	544.000	625,265	743,075
Australia	107,000	108,950	134,690
Japón	193,000	226,269	276,556
Singapur	43,000	57,765	92,744
Corea del Sur	201,000	232,281	239,085
GLOBAL	2,802,700	3.484.971	4,192,255

Fuente: (ISC)2

Ciberseguridad: Oportunidad de mercado de 2.000.000.000.000$

The global cybersecurity total addressable market may reach $1.5 trillion to $2.0 trillion, approximately ten times the size of the vended market.

Global cybersecurity market size, 2021, $ trillion



Segment	Total addressable market, $ billion	Current penetration, %
Data protection	50–100	30–35
Governance, risk, and compliance	50–100	30–35
Email security and awareness	50–100	10–15
Cloud security	50–100	1–5
Network security	50–100	15–20
Identity and access management	50–100	20–25
Security consulting	100–200	15–20
Web security	100–200	5–10
IoT/OT[1]	100–200	1–5
End point security	100–200	5–10
Application security	100–200	1–5
Security and operations management	400–500	1–5
MSSP[2]/outsourcing	400–500	5–10

[1]Internet of Things/operational technology.
[2]Managed security service provider.
Source: McKinsey Cyber Market Map 2022

Fuente: McKinsey

Estrategia Europea de Ciberseguridad para la Década Digital

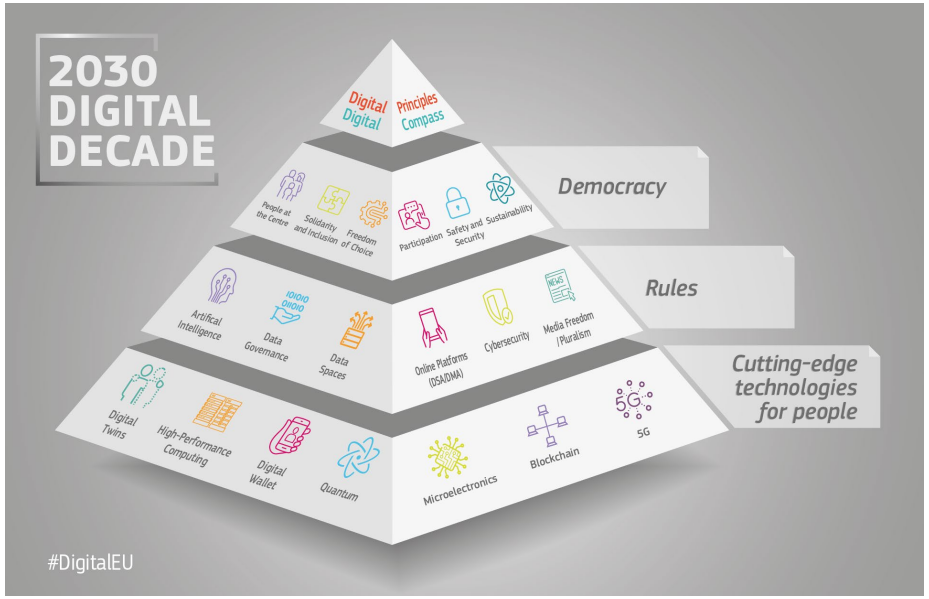
GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

- 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.



I+D+i en ciberseguridad en Europa

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

Impulso Financiero

Mecanismos directos y *financiación en Cascada*

BOE — *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.*

DIGITAL EUROPE PROGRAMME #DigitalEUprogramme #DigitalEU

1.650 M€
(financiación ciberseguridad 2021-2027)

HORIZON EUROPE

1.600 M€
(Cluster III ciberseguridad 2021-2027)

EUROPEAN UNION EUROPEAN DEFENCE FUND

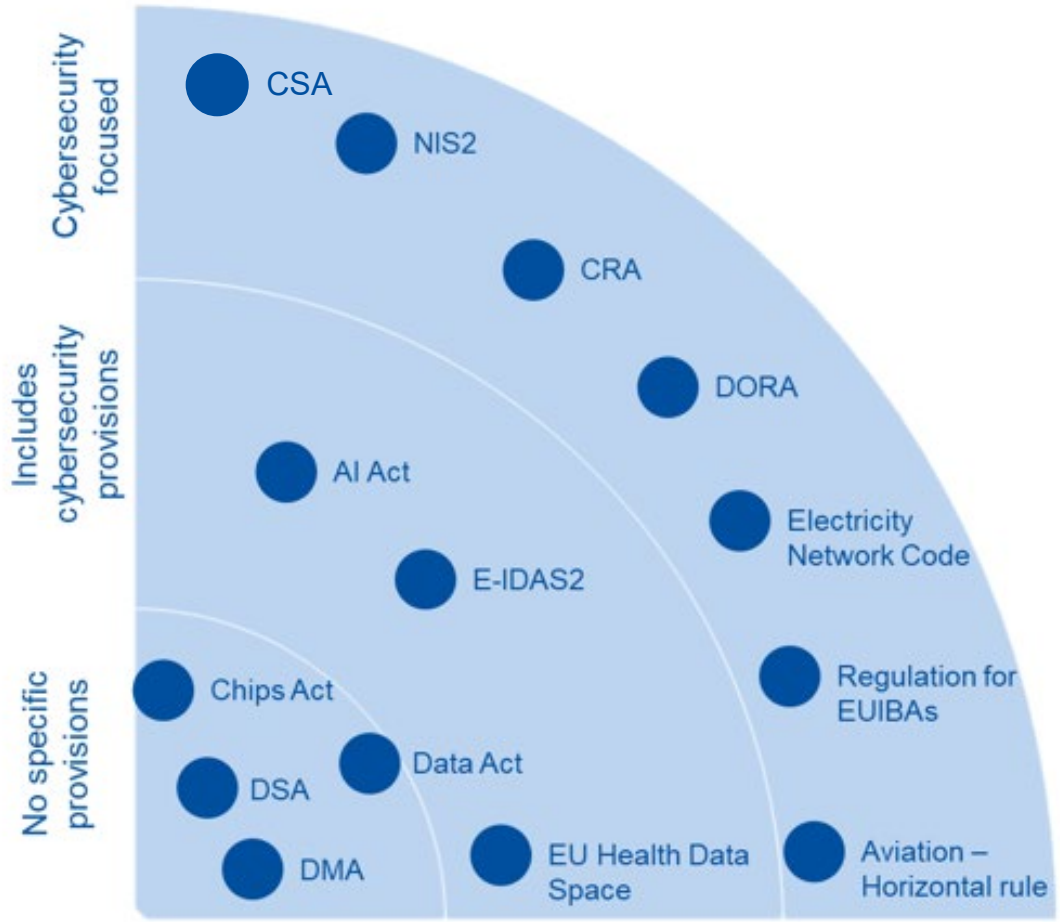
8.000 M€
(2021-2027)

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

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Regulaciones y ciberseguridad



Fuente: ENISA Policy Report 2022 (+CSA)

Detalle (1)

REGULACIÓN	ALCANCE	A QUIÉN AFECTA
◆ **NIS2**	Sectores esenciales: Energía, Transporte, Banca, Infraestructuras del mercado financiero, Sanidad, Agua potable, Aguas residuales, Infraestructuras digitales, Administración pública, Espacio Sectores importantes: Servicios postales y de mensajería, Gestión de residuos, Fabricación, producción y distribución de productos químicos, Producción, transformación y distribución de alimentos, Industria manufacturera, Proveedores digitales	Entidades públicas y privadas esenciales e importantes que alcancen o superen el umbral definido por la Comisión para las medianas empresas Proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público, proveedores de servicios de confianza y registros de nombres de dominio de primer nivel y proveedores de servicios de sistemas de nombres de dominio (DNS), independientemente de su tamaño También se prevén excepciones al umbral de tamaño basadas, por ejemplo, en las evaluaciones de riesgo nacionales de los Estados miembros Autoridades de NIS y CSIRT

Detalle (2)

REGULACIÓN	ALCANCE	A QUIÉN AFECTA
◆ CRA	Productos con elementos digitales	Fabricantes de productos con elementos digitales, operadores económicos en relación con estos productos En relación con la ciberseguridad (por ejemplo, importadores, distribuidores) Autoridades notificantes y autoridades de vigilancia del mercado Organismos notificados / Organismos de evaluación de la conformidad

Detalle (3)

REGULACIÓN	ALCANCE	A QUIÉN AFECTA
◆ **CSA**	Escudo Europeo de Ciberseguridad, compuesto por Centros de Operaciones de Seguridad interconectados en toda la UE Mecanismo de Emergencia de Ciberseguridad para mejorar la postura cibernética de la UE Mecanismo de revisión de incidentes de ciberseguridad	Estados Miembros – Autoridades nacionales y CSIRTs Centros de Operaciones de Seguridad (SOCs) Entidades de ensayo en sectores cruciales Proveedores “de confianza”

Detalle (4)

REGULACIÓN	ALCANCE	A QUIÉN AFECTA
◆ **DORA**	Sectores financiero y digital	Entidades financieras, incluidas: entidades de **crédito**, entidades de **pago**, entidades de **dinero electrónico**, empresas de **inversión**, proveedores de servicios de **criptoactivos**, depositarios centrales de **valores**, entidades de **contrapartida central**, centros de **negociación**, registros de **operaciones**, gestores de **fondos de inversión alternativos**, **sociedades gestoras**, proveedores de servicios de comunicación de datos, empresas de **seguros** y reaseguros, organismos de **pensiones de jubilación**, agencias de **calificación crediticia**, **auditores** legales y empresas de auditoría, administradores de **índices de referencia** críticos, proveedores de servicios de **crowdfunding**, registros de **titulización**, proveedores de servicios TIC a terceros.

Detalle (5)

REGULACIÓN	ALCANCE	A QUIÉN AFECTA
◆ **EUIBAs**	Instituciones, órganos y agencias de la UE	Instituciones, órganos y agencias de la UE CERT-EU
◆ **eIDAS 2**	Servicios de confianza electrónica (Trust Service Provider, TSP)	Estados miembros de la UE, TSPs, empresas de servicios públicos y grandes plataformas en línea.
◆ **Data Act**	Datos digitales	Proveedores de productos y servicios que generan datos, como los dispositivos **IoT**, proveedores de servicios en la nube y en los bordes, y organismos del sector público, incluidas las instituciones de la Unión Europea.

Detalle (6)

REGULACIÓN	ALCANCE	A QUIÉN AFECTA
◆ **AI Act**	Sistemas de IA	Diferentes actores implicados en IA: proveedores, implantadores, importadores, distribuidores y fabricantes de productos Todas las partes implicadas en el desarrollo, uso, importación, distribución o fabricación de modelos de IA tendrán que rendir cuentas Proveedores y usuarios de sistemas de IA ubicados fuera de la UE
◆ **Chips Act**	Sistemas de IA	Ecosistemas de semiconductores en la UE

Detalle (7)

REGULACIÓN	ALCANCE	A QUIÉN AFECTA
◆ **DSA**	Servicios digitales	Se aplica a los servicios de intermediación prestados a destinatarios del servicio que tengan su lugar de establecimiento o residencia en la Unión, independientemente del lugar de establecimiento de los prestadores de dichos servicios.
◆ **DMA**	Mercado único digital	Servicios básicos de plataforma prestados u ofrecidos por los gatekeepers a usuarios empresariales establecidos en la Unión o a usuarios finales establecidos o ubicados en la Unión.

Regulaciones: Resumen

Leyes	Directivas	Actos de Ejecución / Delegados y Procedimientos Legislativos Especiales
• CRA • DORA • EUIBAs • AI Act • eIDAS2 • Data Act • European Health Data Space • DMA • DSA • Chips Act	• NIS2	• Electricity Network Code for CS • Aviation – Horizontal Rule

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

España | digital 2026

GRACIAS

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

017 TU AYUDA EN CIBERSEGURIDAD incibe_