

Análisis del talento e iniciativas en el sector de la ciberseguridad

Diana Núñez Martínez

Técnico del Departamento Talento en Ciberseguridad

27 de enero de 2026



**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**



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Agenda

Análisis del Talento



Estado de la ciberseguridad



Iniciativas





Entidad dependiente del **Ministerio para la Transformación Digital y Función Pública**.

MISIÓN mejorar la ciberseguridad y la **confianza digital** de ciudadanos, menores y empresas privadas

VISIÓN posicionar a España como un **referente**

- ☐ Protegemos a la **ciudadanía** (incluyendo a los menores y su entorno) y a las **empresas privadas** frente a amenazas digitales. INCIBE-CERT, el equipo de respuesta a incidentes de seguridad
- ☐ Promover la **cultura de ciberseguridad**
- ☐ Fomentamos el **talento y la innovación**.
- ☐ Trabajamos en **cooperación con organismos** nacionales e internacionales.

2024

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

BALANCE DE CIBERSEGURIDAD

+16,6%
más que en 2023

97.348
incidentes de
ciberseguridad

! Cualquier problema digital que ponga en riesgo los datos o la seguridad de los dispositivos, como, por ejemplo, un virus informático.

183.851
sistemas vulnerables

Un sistema vulnerable es como una casa con una cerradura rota. Es más fácil para los intrusos entrar y causar problemas.



BALANCE DE LA LÍNEA DE AYUDA

017

Incremento del **21,8%** más que en 2023

98.546

Consultas y problemas de
la Línea de Ayuda de INCIBE

54% de
las llamadas fueron
para prevenir un
incidente.

46% de
las llamadas fueron
para solucionar un
incidente.

38.236

4 de cada 10
incidentes son
fraude online
35% más que en 2023

21.571

incidentes son **phishing***

*Suplantación a empresas o personas de confianza que se ponen en contacto con las posibles víctimas, a través de correos electrónicos falsos, intentando engañarles para proporcionar información personal o bancaria.

2.122

incidentes relacionados con
tiendas online
fraudulentas

CONSULTAS DE EMPRESAS

19,1%

12,6%

10,8%

- Suplantación de identidad
- Phishing
- Fraude Business Email Compromise (BEC)



Acercar la profesión de ciberseguridad a toda la sociedad y despertar vocaciones desde edades tempranas hacia un sector con gran proyección futura y grandes oportunidades.

PUNTO DE PARTIDA

- ❑ Estudio de Análisis y diagnóstico de Ciberseguridad llevado a cabo por INCIBE y *Observaciber* en marzo 2022 pone de manifiesto que existirá un gap de profesionales de 40.000 en el sector.



ACTUACIONES

- ❑ Despertar vocaciones; generar referentes, divulgación de la ciberseguridad, etc.
- ❑ Formación nuevos profesionales y capacitación de los activos.



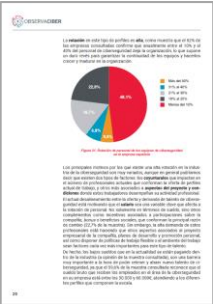
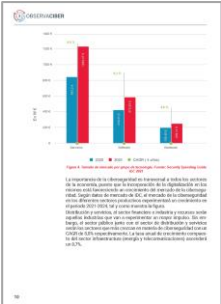
OBJETIVO PRTR CID 294 – Formar a 10.260 personas en cursos de 250h

Análisis del talento en CS



Análisis y diagnóstico del talento en ciberseguridad en España

Objetivo: ofrecer una vision clara de la situación del talento en ciberseguridad en España en este momento asi como recomendaciones y conclusiones para mejorar la situacion.



Análisis del talento en CS en España



Oferta de talento de ciberseguridad



Volumen total de oferta de talento de ciberseguridad que el propio sistema es capaz de generar funcionando a pleno rendimiento

(Grados, máster, FP)



Volumen de personal existente en las organizaciones que se recicla hacia posiciones de ciberseguridad

39.072 personas

41.123 personas

41.677 personas

42.283 personas

Oferta

2021

2022

2023

2024

Demanda

63.191 personas

67.147 personas

74.904 personas

83.007 personas

Demanda de talento de ciberseguridad



Empleo generado por incremento de PIB



Empleo generado en TI (seguridad)



Demanda actual

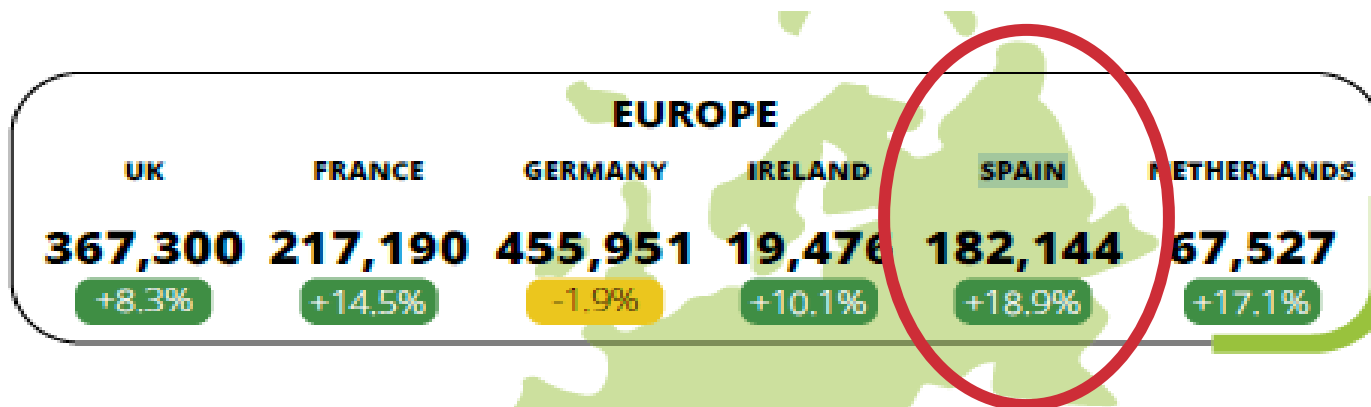
Fuente: <https://observaciber.es/#estudios>

Fuente: <https://observaciber.es/sites/observaciber/files/media/documents/EstudioDiagnosticoTalento2022.pdf>

Estado de la ciberseguridad

Estimación actual (2024) de 5,5 millones de profesionales a nivel mundial.
(Crecimiento de un 8,7% anual)

En España:

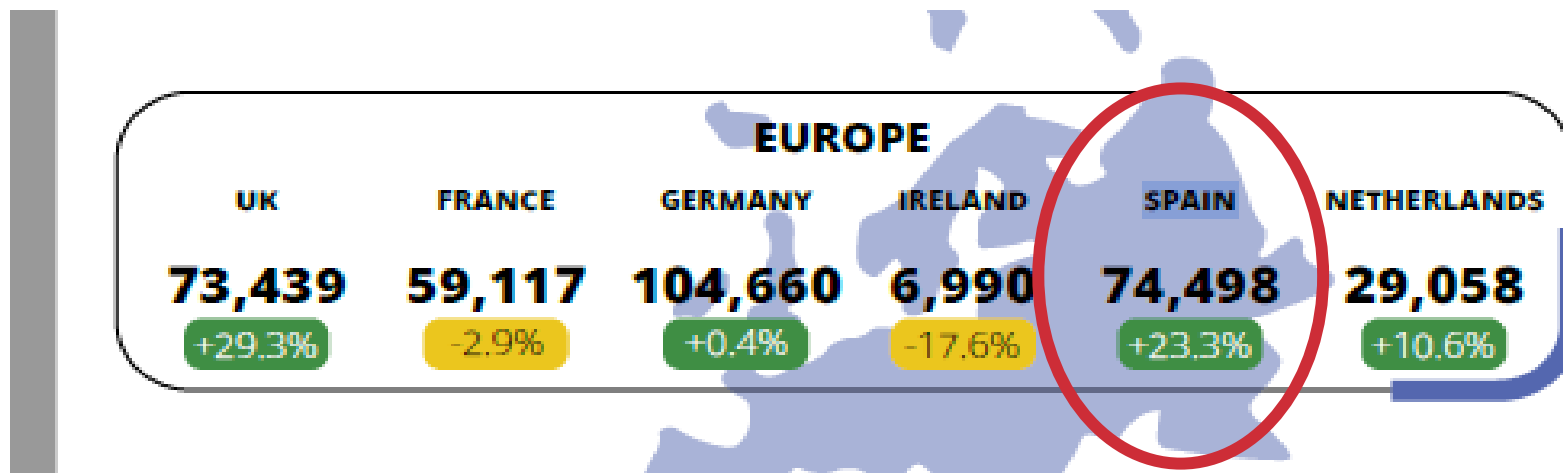


Fuente:
https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4

Estado de la ciberseguridad

Brecha laboral actual (2024) estimada en 4,7 millones de profesionales a nivel mundial. (Crecimiento de un 12,6%)

En España:



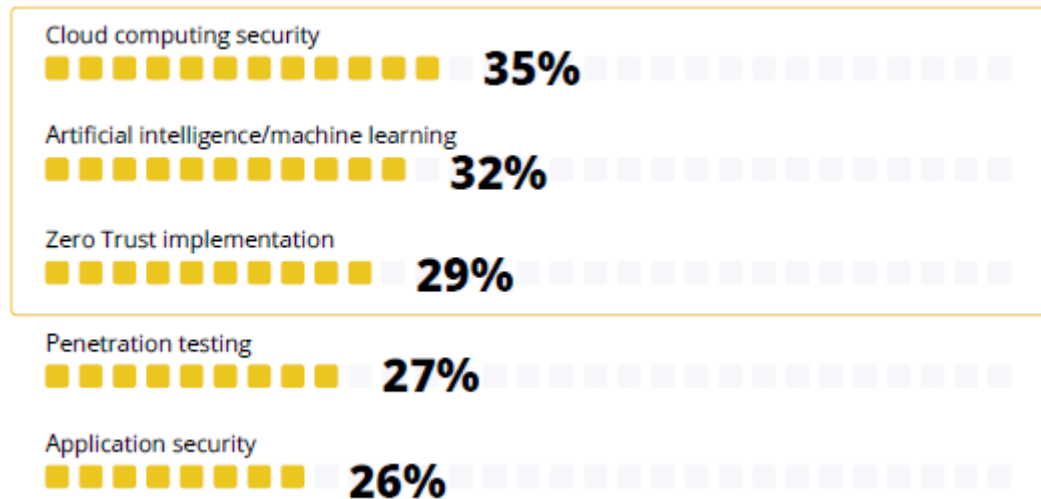
La demanda sigue superando a la oferta

Fuente:

https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4

Estado de la Ciberseguridad

Escasez de capacidades técnicas en áreas críticas



- Seguridad de implementación en la nube → 35%
- Inteligencia Artificial/*Machine learning* → 32%
- *Zero Trust* (redes de confianza cero) → 29%
- *Penetration Testing* → 27%
- Seguridad en las aplicaciones → 26%

Base: 11.473 profesionales de ciberseguridad

Nota: Solo se muestran las diez capacidades más respondidas; No se muestran respuestas tipo no sabe / no responde

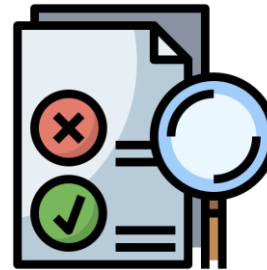
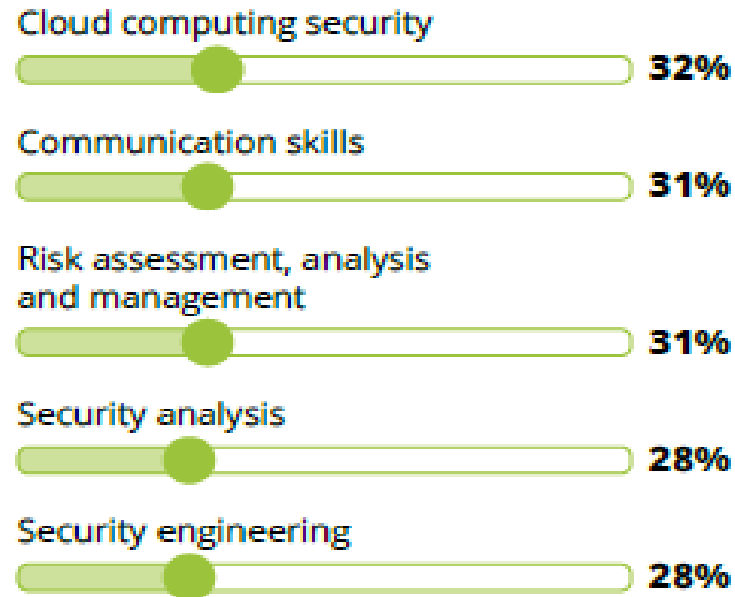
Fuente:

https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4

Estado de la Ciberseguridad

Demanda de conocimientos y habilidades

ASKED TO HIRING MANAGERS



- Brecha de habilidades en ciberseguridad a nivel mundial para 2025
- GAP entre la tecnología disponible y las habilidades para gestionarla
- 48% Conocimientos IA

Fuente: Base: 7.143-7.184 global cybersecurity professionals

<https://media.isc2.org/->

[/media/Project/ISC2/Main/Media/documents/research/ISC2 Cybersecurity Workforce Study 2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4](https://media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4)

<https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2025/fortinet-annual-report-indicates-ai-skillsets-critical-to-cybersecurity-skills-gap-solution>

Estado de la Ciberseguridad

Cualificaciones y habilidades más importantes en ciberseguridad

● 2022 ● 2023

LARGEST INCREASES IN TRENDS

Strong communication skills



Cybersecurity certifications



Curiosity/eagerness to learn



Knowledge of basic cybersecurity and cybersecurity concepts



Cybersecurity qualifications (e.g., trainings, etc.) other than certifications or a degree



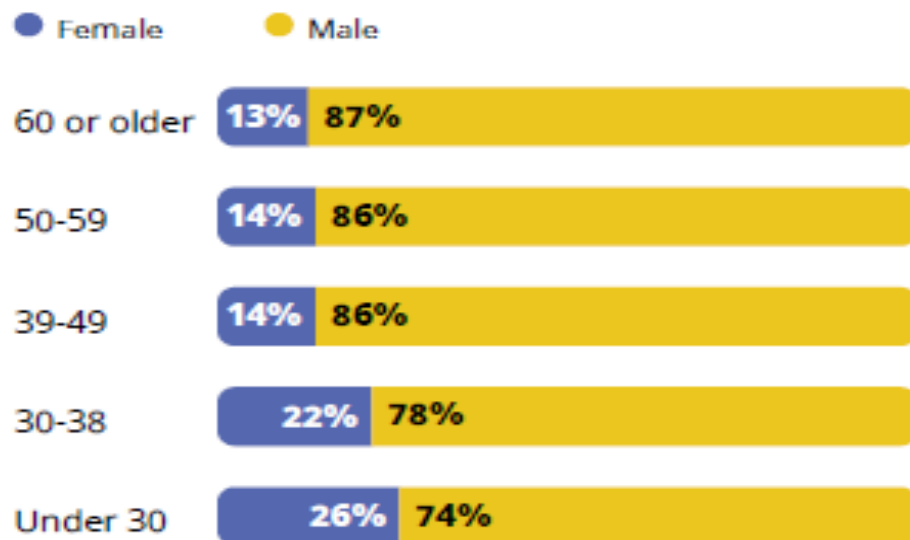
- Curiosidad / Ganas de aprender → 39%
- Habilidades comunicativas → 38%
- Conocimiento de ciberseguridad en general → 35%
- Certificaciones de ciberseguridad → 32%

Base: 14.865 profesionales de ciberseguridad

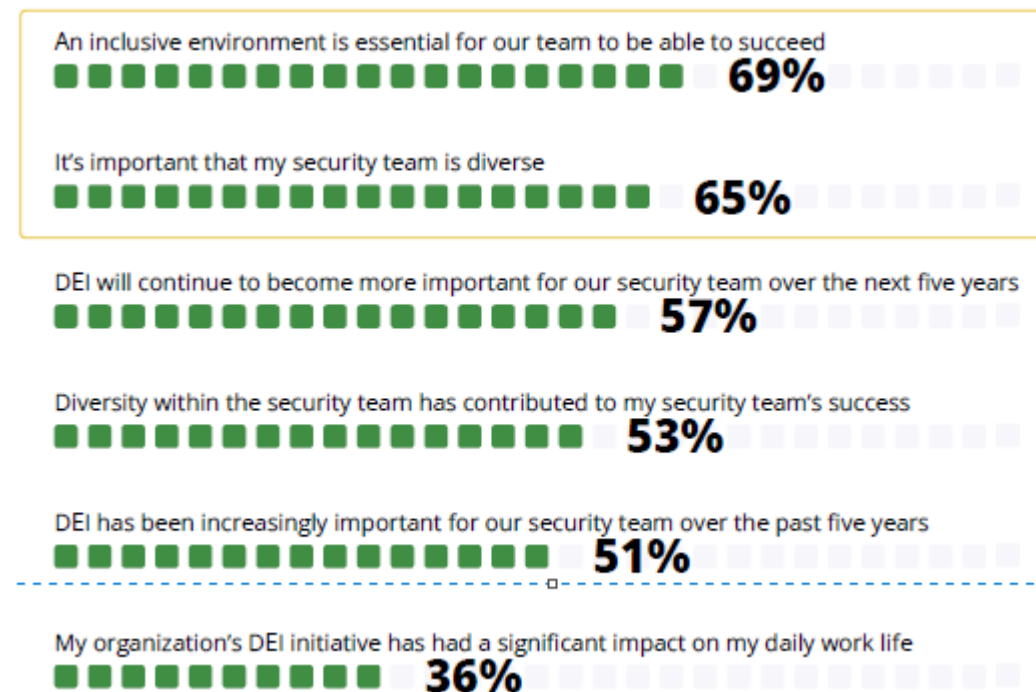
Se observa que la **curiosidad**, la **comunicación** y las **certificaciones** son cada vez más importantes. Esto es un reflejo de las necesidades del panorama actual.

Estado de la Ciberseguridad

Diversidad, igualdad e inclusión en la ciberseguridad



Base: 13.682 global cybersecurity professionals



Base: 11.373-13.041 global cybersecurity professionals
DEI: Diversity, Equity and Inclusion (Diversidad, Igualdad e Inclusión)

Fuente:

https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4

Estado de la Ciberseguridad

Certificaciones y experiencia laboral muy valiosas

Certifications are more valuable than independent experience

Base: 13,222

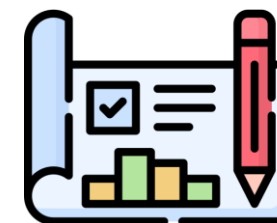


46%

Independent competition experience (e.g., hackathon, capture the flag, etc.)

54%

Cybersecurity certification



Certifications are more valuable than entry-level degrees

Base: 13,496



34%

Bachelor's degree in related field

66%

Cybersecurity certification

2025- Estrategia centrada en
formación, certificación y
concienciación

89% certificaciones

Base: 13.222-13.742 profesionales de ciberseguridad

Medidas a adoptar



Retención de talento

Condiciones laborales atractivas
Planes de Desarrollo Profesional
Flexibilidad laboral



Programas especializados

Cursos, certificaciones y programas educativos específicos (ingenieros, operadores y analistas en CS)



Inclusión y diversidad

Promoción de la participación de mujeres y jóvenes (becas, mentorías, programas de sensibilización)



Colaboraciones internacionales

Alineación de estándares formativos con marcos y atracción de talento extranjero



Alianzas público-privadas

Colaboraciones entre empresas, instituciones académicas y organismos públicos



Inversión en CS

Asignación de fondos a iniciativas de ciberseguridad y desarrollo de talento

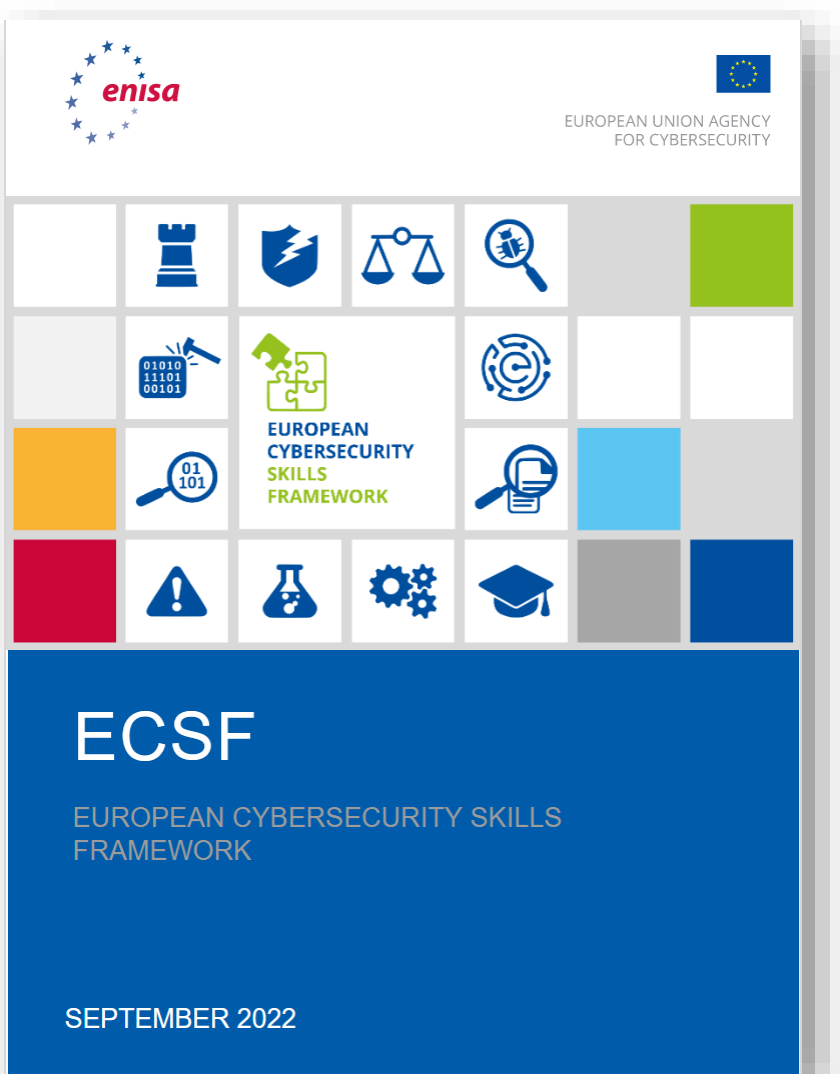
Tendencias 2025

**5.000 profesionales del sector*



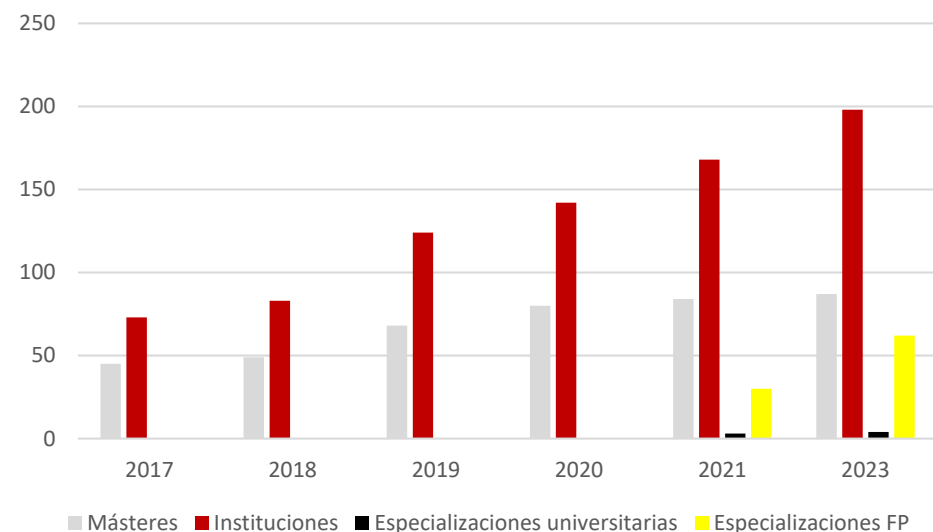
- ❖ **Altos niveles de satisfacción laboral** (51% satisfechos-93% nuevas oportunidades)
- ❖ **IA cambio de habilidades** (pensamiento crítico, adaptabilidad o creatividad)
- ❖ **Desarrollo profesional** (44% cambiaría por promoción)
- ❖ **Propósito** (cultura, valores y ética)
- ❖ **Flexibilidad** (modelos híbridos, desconexión y salud mental)

A nivel Europeo

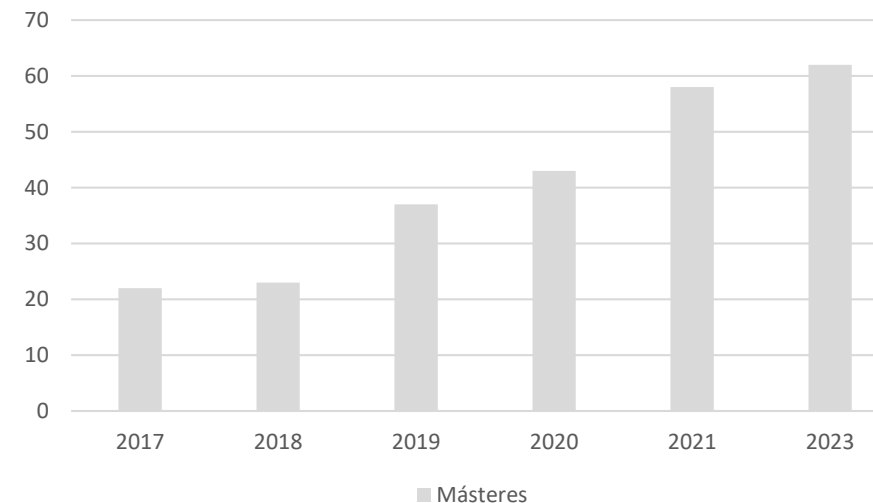


- | | | | |
|---|---|----|--------------------------------------|
| 1 | Chief Information Security Officer (CISO) | 7 | Incident Responder |
| 2 | Legal, Policy and Compliance Officer | 8 | Digital Forensics Investigator |
| 3 | Cibersecurity Architect | 9 | Penetration Tester |
| 4 | Cibersecurity Implementer | 10 | Cybersecurity Auditor |
| 5 | Researcher | 11 | Cybersecurity Risk Manager |
| 6 | Educator | 12 | Cyber Threat intelligence specialist |

Evolución de la formación en CS



Evolución Másteres Ciberseguridad modalidad online



2025

- ❑ Más de 240 instituciones en España imparten formación en ciberseguridad.
- ❑ +120 centros educativos ofrecen titulaciones de Formación Profesional.
- ❑ 87 másteres, 11 grados y 9 especializaciones universitarias disponibles.
- ❑ Consulta los catálogos en: www.incibe.es/formacion.
- ❑ ENISA Education map: <https://www.enisa.europa.eu/topics/cybersecurity-education/education-map>

Acciones



Eventos CyerCamp

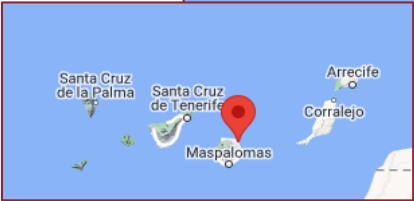
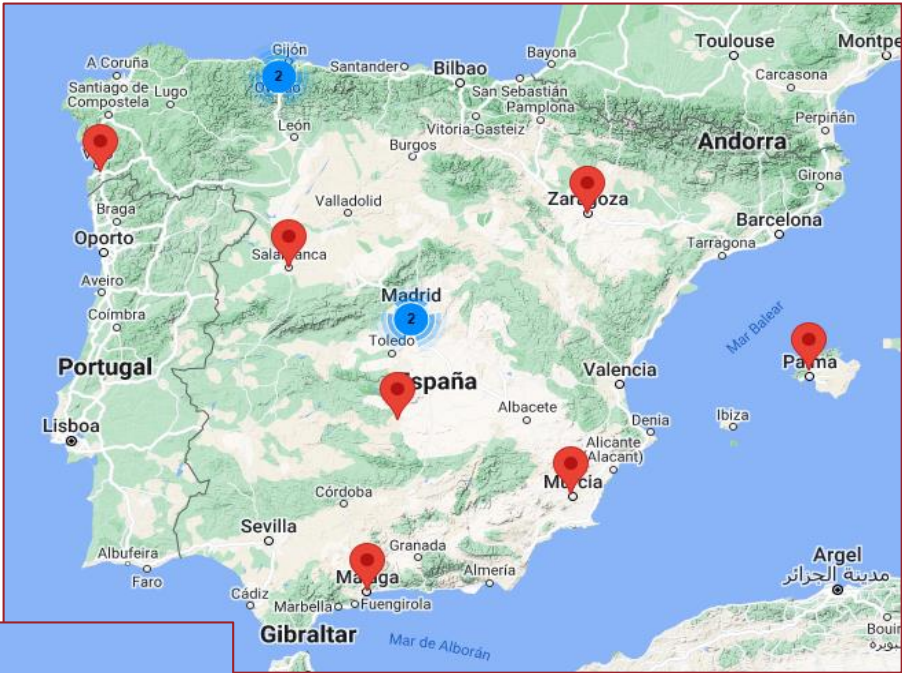
Objetivo: Promover el desarrollo de los conocimientos y competencias de las personas y organizaciones en el ámbito de la ciberseguridad.

12 convenios UNIVERSIDADES territorio nacional

Principales actividades: Conferencias, convenciones, reuniones de expertos, concursos, espacios de exposición, cursos, talleres o clases magistrales, entre otras iniciativas

Inversión: 2.471.374.00€ (INCIBE:1.647.582,00€)

AÑO	nº actividades	nº asistentes	nº horas
2022	22	957	55
2023	130	12080	698
2024	220	9150	920
2025	127	8737	318
total	499	30.924	1.991



Acciones



Inclusión y Diversidad

Objetivo: Impulsar el desarrollo de actividades formativas especializadas en ciberseguridad para colectivos vulnerables e infrarrepresentados en el sector. En colaboración con asociaciones, entidades y/o fundaciones que trabajen con estos colectivos.

7 convenios durante 3 años

Cursos de formación especializados: Red Team, Blue Team, Bootcamp, Forense, etc

Inversión: 5.227.605 € (INCIBE 2.613.803 €)

Nº alumnos formados: más de 1.400 alumnos

Entidades: Fundación Prevent, Fundación Eurofirms, Fundación Universia, Fundación ONCE



Acciones

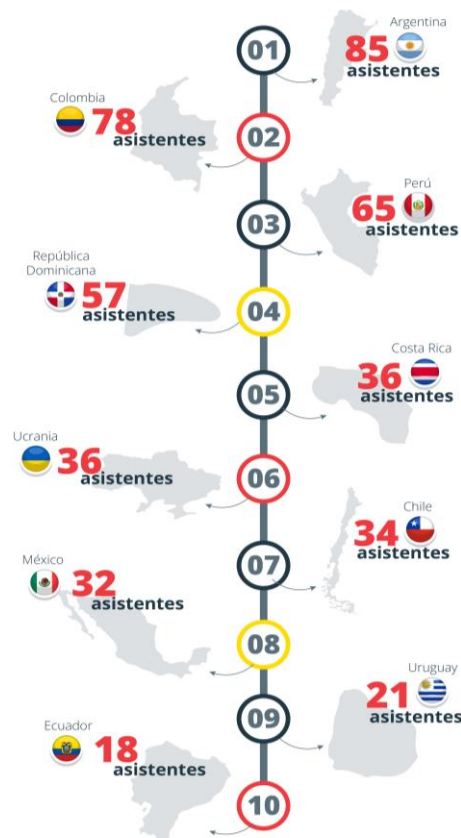


Programa Especializado

Objetivo: Programa de capacitación especializado dirigido a Fuerzas y Cuerpos de Seguridad, Ministerio Fiscal, Jueces y Magistrado, Actores Políticos, reguladores, legislativos o ciberdiplomáticos y Especialistas de Centros de Respuesta a Incidentes Cibernéticos

5 tracks diferentes y 200 horas de formación

Principales países asistentes



❖ Cybersecurity Summer BootCamp:

- 14–24 julio 2025
- 507 profesionales de 27 países.
- 104 expertos, incluidos 5 **keynotes** internacionales.
- Incluyó:
 - **Formación ECSC** (16–18 julio).
 - **Dialogue on Cybersecurity (León, 2025)**: foro internacional centrado en diplomacia digital y cooperación multilateral, con retos globales y fortalecimiento de la confianza entre regiones.

Acciones

Curso ciberseguridad sector energético



❖ Objetivos

- ❖ Entrenamiento de la toma de decisiones en crisis cibernéticas en **infraestructuras energéticas**, concebido para situar a los participantes en el centro de una crisis realista en un entorno crítico.

❖ Público Objetivo

- ❖ Estudiantes interesados en **ciberseguridad OT** o profesionales de ciberseguridad de entidades que operan infraestructuras del sector de la energía o aguas

❖ Convocatorias

- ❖ Modalidad mixta (presencial/online)
- ❖ Duración 16 horas
- ❖ 80 plazas por edición

Asesoramiento preventivo y reactivo en incidentes de ciberseguridad

❖ Objetivos

- ❖ Capacitar y especializar a los participantes en aspectos clave de ciberseguridad (preventivo y reactivo de incidentes)

❖ Público Objetivo

- ❖ Profesionales y estudiantes del ámbito de las Tecnologías de la Información y la Comunicación (TIC)
- ❖ Personas con formación académica o experiencia laboral en el sector, incluyendo experiencia en atención a usuarios en entornos tecnológicos

❖ Convocatorias

- ❖ Modalidad presencial
- ❖ Duración de 32 horas
- ❖ 50 plazas por edición

Gracias



**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**