



INSTITUTO NACIONAL DE CIBERSEGURIDAD

¡Quiero ser hacker!



V CIBERLEAGUE – GUARDIA CIVIL

Sara García Bécares – Responsable RETECH



SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL





Contexto



Contexto ¿Por qué?

Evolución tecnológica: *Inteligencia artificial, big data, IoT*





Contexto ¿Por qué?

Digitalización y Globalización

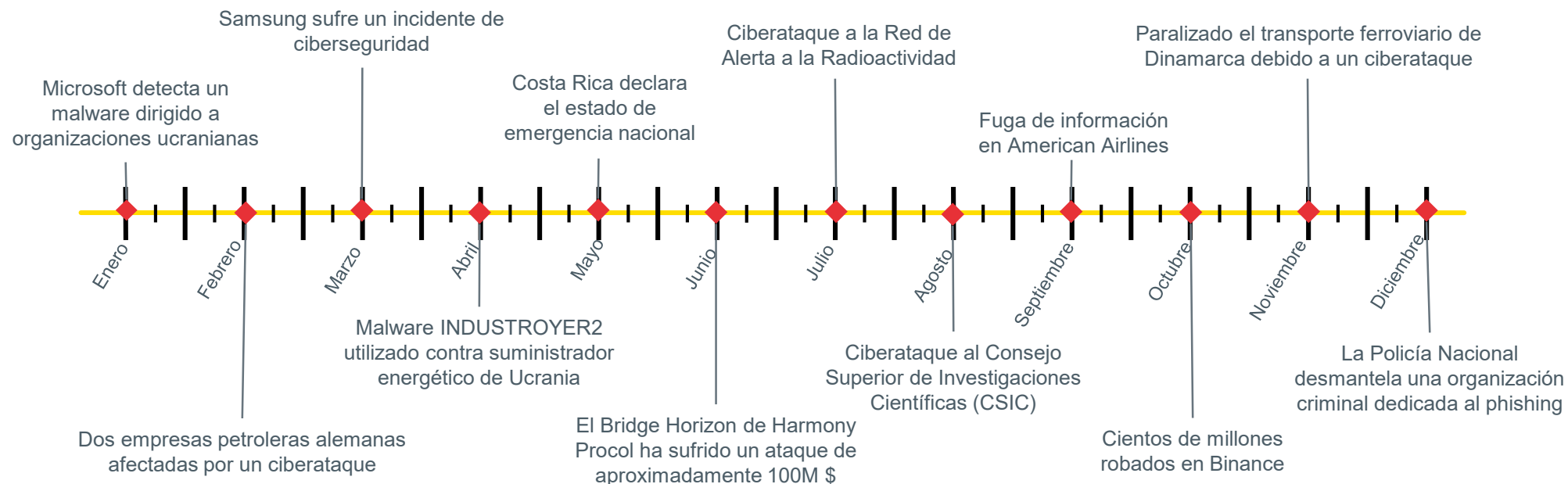




Contexto

Bitácora

Bitácora

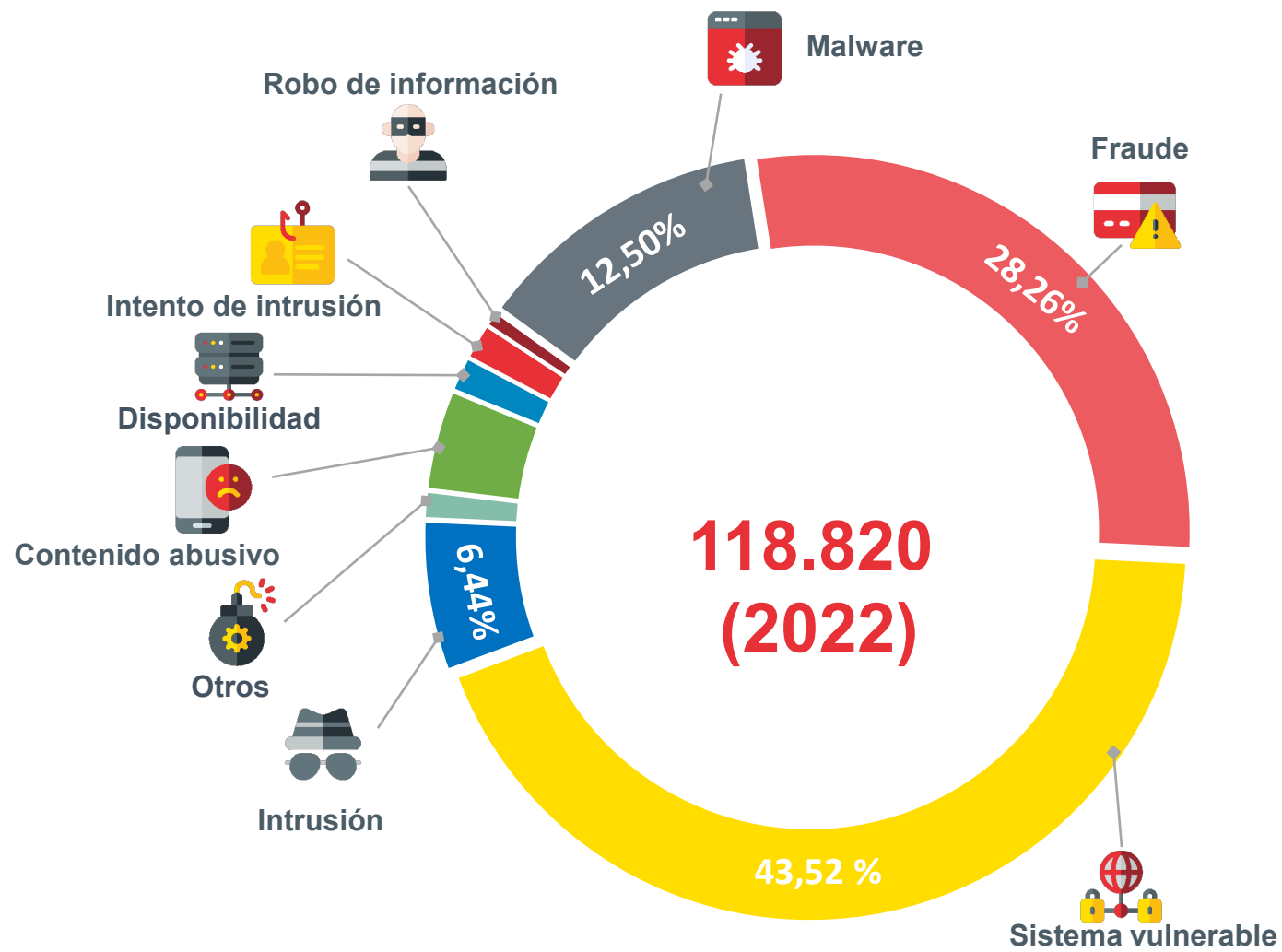
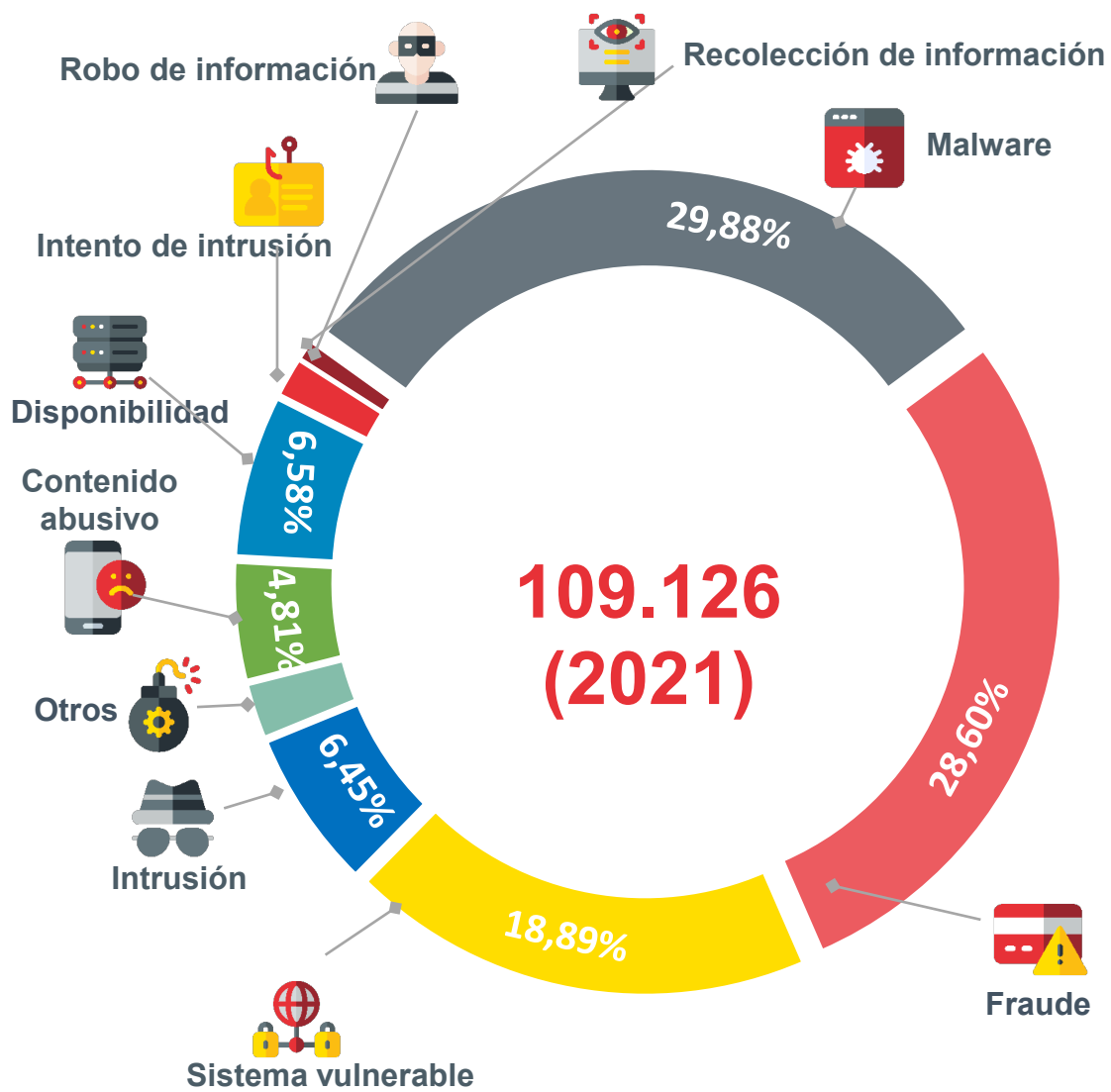


En los últimos 10 años se han producido más de **1.500 hechos relevantes**



Contexto

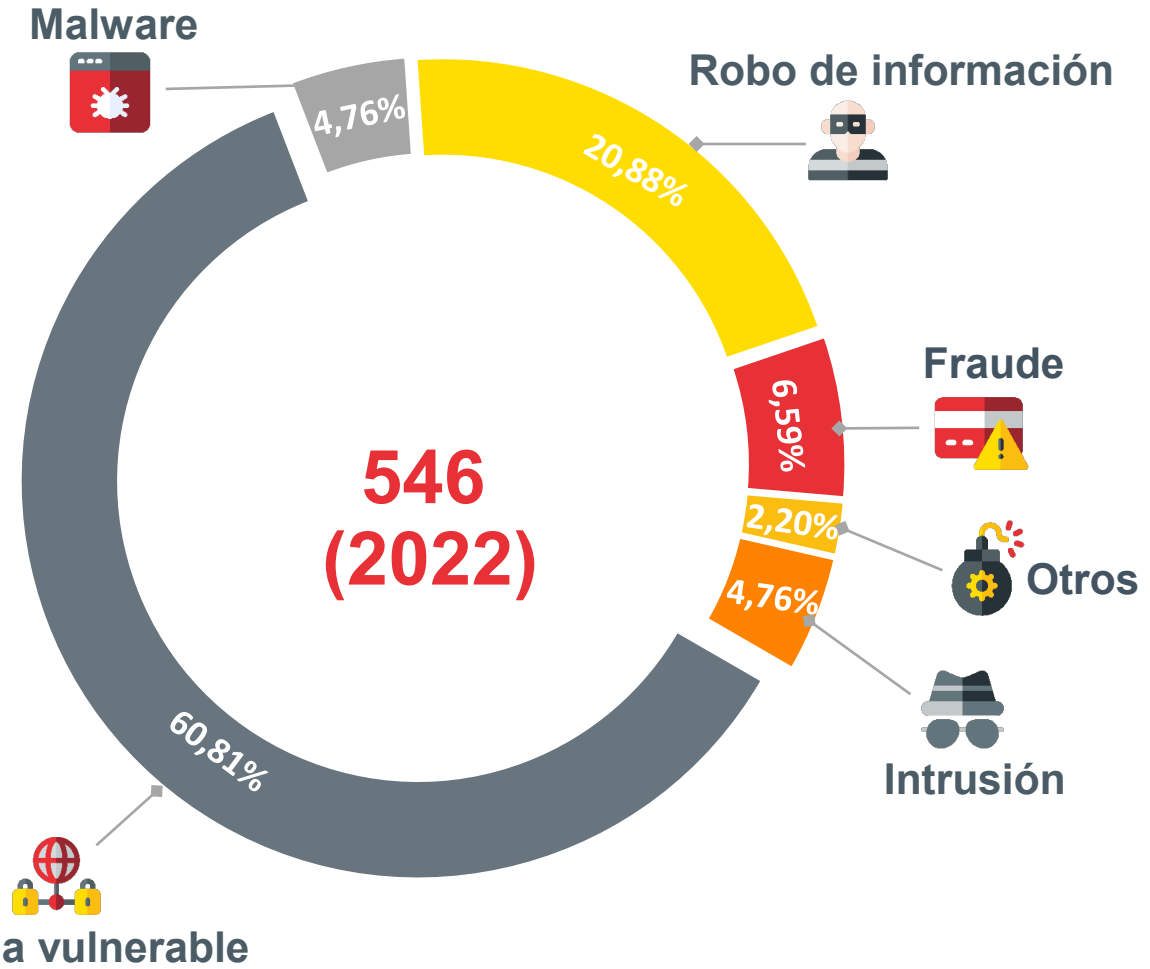
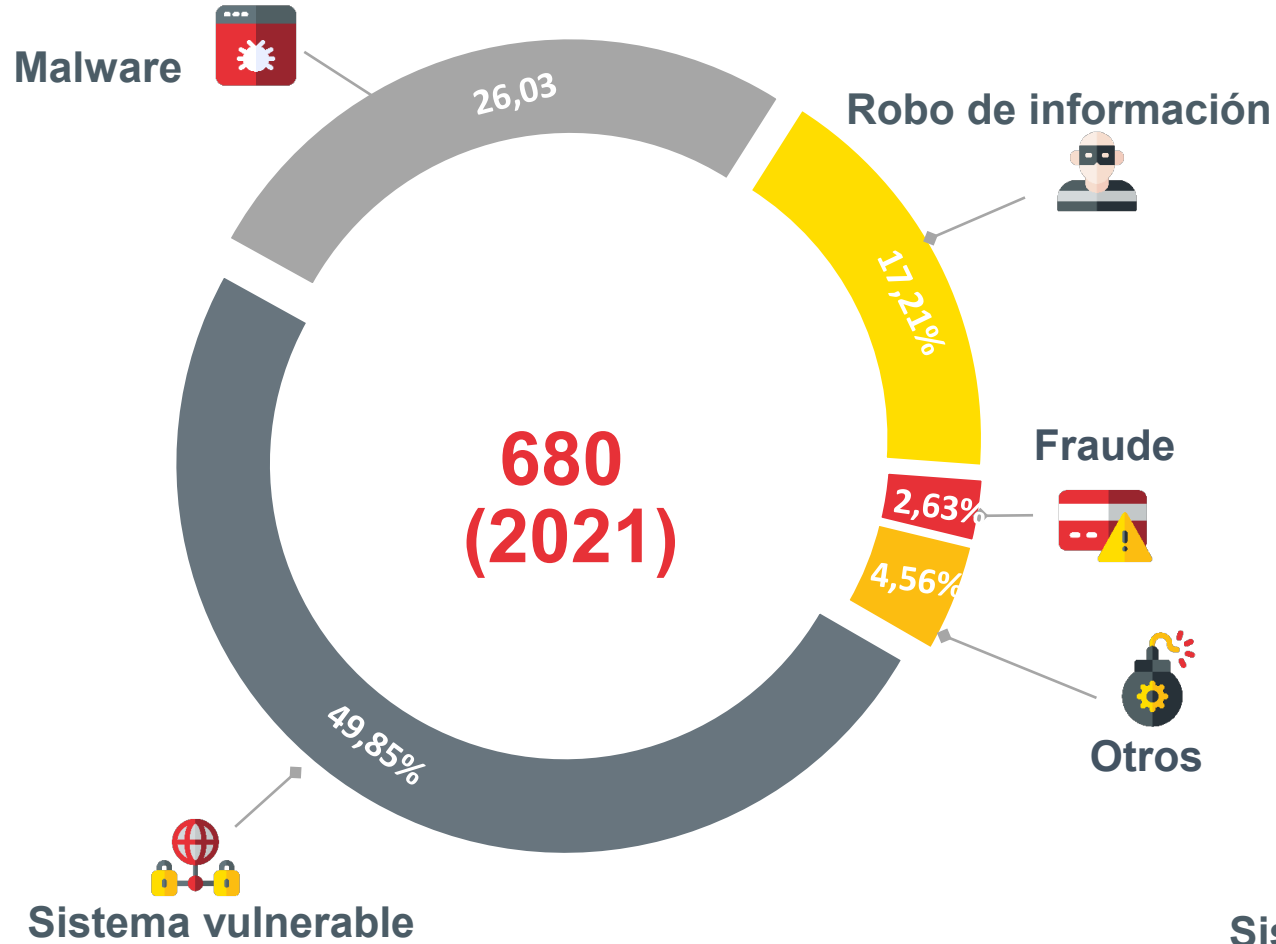
Incidentes de Ciberseguridad





Contexto

Incidentes de Ciberseguridad OOC





Contexto

Incidentes de Ciberseguridad OOC





INCIBE

(Contexto)

Spain: Land of Cybersecurity

Land of Cybersecurity



1st country in the EU with **58 CSIRTs**



2nd European Union country
4th in the world in **Cybersecurity maturity**



20+ years maturity of the Spanish cybersecurity ecosystem

Cybersecurity Industry

- 1,900 M euros**
- 14%+ of growth** expected in 2022
- Public-private partnership cooperation**
- 1,800 security companies and services.**
- 85% of companies offer cybersecurity services**
- 150,000 security workers**

Research ecosystem

- RENIC** (National Network of Excellence for Research in Cybersecurity):
 - 45** cybersecurity research teams in Spain
 - 452** researchers
 - 10** technology centers
 - 28** universities
 - 7** research centers
- RNLI** (National Network of Industrial Cyber Laboratories):
 - 25** laboratories

Talent in cybersecurity

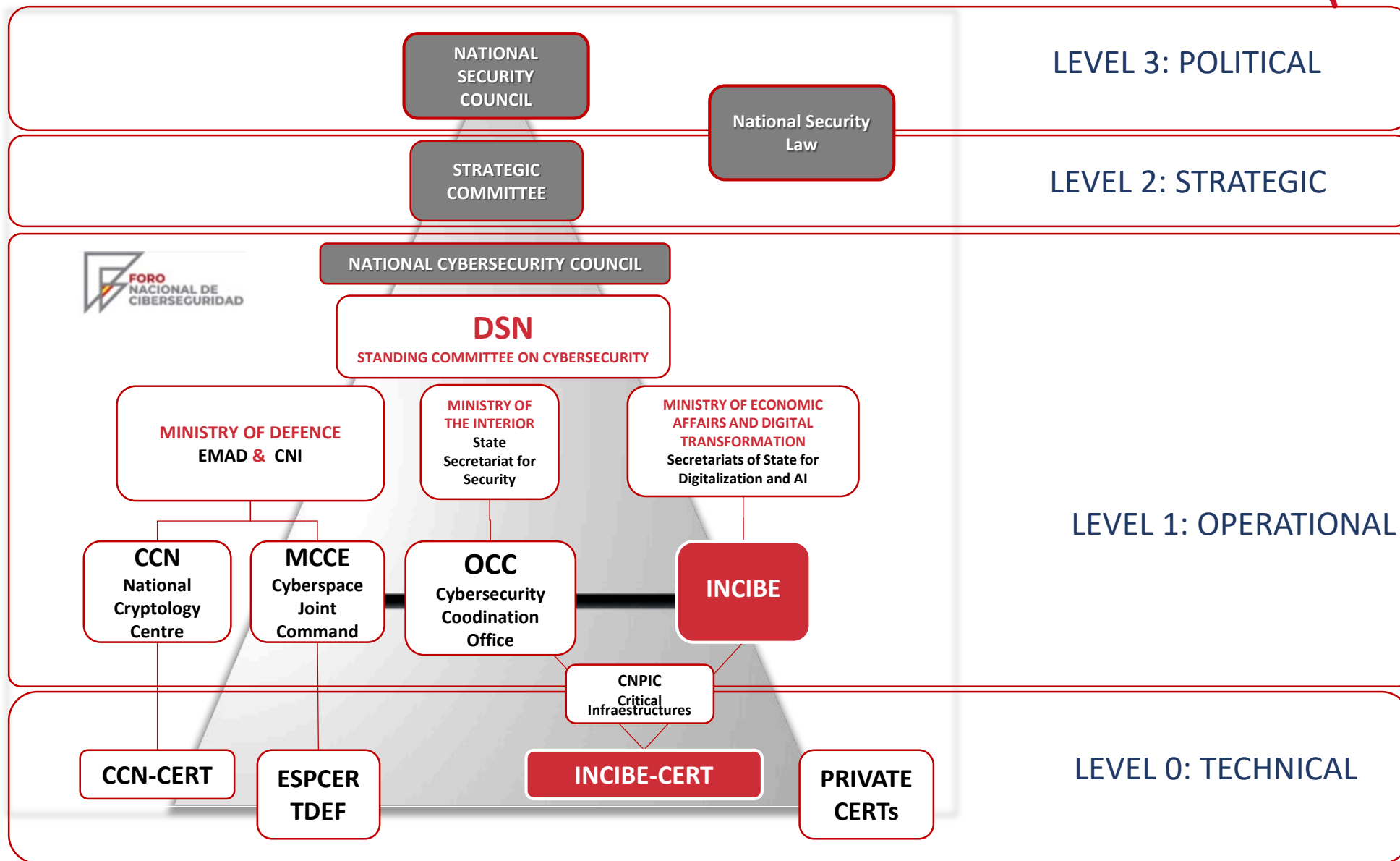
- 121** regulated training programs in cybersecurity:
 - 84** Master's degree programs
 - 3** university specializations
 - 4** bachelor's degrees
 - 30** Professional Training specializations
- 168 centers** offering training in cybersecurity

National Cybersecurity Plan (2022)

€+ €1 billion + 150 actions over the **next 3 years:**

- Platform for the exchange of information**, in real time, between public and private institutions.
- Cybersecurity infrastructures** in the autonomous communities and cities and local entities.
- Integrated** system of cybersecurity **indicators.**
- Cybersecurity Operations Centre** for the General State Administration and its Public Institutions.
- Promote **cybersecurity in SMEs, micro-SMEs** and the **self-employed.**
- Promote a **culture of cybersecurity**

Gobernanza nacional de ciberseguridad



INCIBE: Qué y Cómo lo hacemos



Fomentar la confianza digital



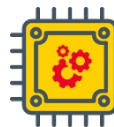
Dar soporte y respuesta a incidentes



Detectar y promocionar el talento en ciberseguridad



Impulsar la industria del sector de la ciberseguridad



Desarrollar nuevas tecnologías



Concienciación y difusión de la cultura de la ciberseguridad



Detección de incidentes



Detección de talento



Colaboración público / privada



Repositorio de ciberinteligencia



Capacitación en ciberseguridad



Respuesta a incidentes de seguridad



Promoción del talento en ciberseguridad



Iniciativas de emprendimiento



Herramientas para la ciberseguridad



Sinergias con entidades



Canales de soporte



Apoyo a la I+D+i



Ciberseguridad en sistemas industriales

INCIBE: Dónde encontrarnos



Ciudadanos



Usuarios de internet



Menores, padres y educadores



Centro de Respuesta a Incidentes



Empresas y profesionales



Concienciación a empresas



Emprendimiento en ciberseguridad

A través de nuestros canales:

A través de nuestros eventos:



Ciudadanos



Día de Internet Segura



Empresas y profesionales



#mujeresciber



INCIBE: Dónde encontrarnos



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

TU AYUDA EN CIBERSEGURIDAD



SÍGUENOS EN REDES



@incibe



in



www.incibe.es



contacto@incibe.es



INCIBE

(Con el talento)

INCIBE – con el talento



INCIBE – con el talento



¿De dónde partimos?



Análisis y diagnóstico del talento en ciberseguridad en España

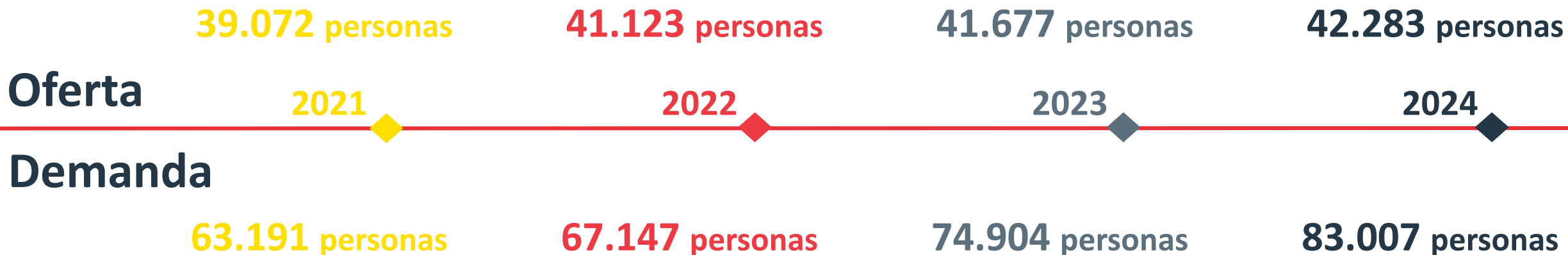
Objetivo: ofrecer una visión clara de la situación del talento en ciberseguridad en España en este momento así como recomendaciones y conclusiones para mejorar la situación.



¿De dónde partimos?



Talento en Ciberseguridad a nivel nacional



¿De dónde partimos?

PRESENCIA FEMENINA (Estudiantes)



Análisis del talento Femenino en CS en España

- ❖ **18%** de estudiantes de **especializaciones** en **ciberseguridad** son mujeres.
- ❖ La brecha se está cerrando de manera **progresiva** (aumento de 5 puntos en 5 años – matriculaciones en carreras técnicas, del 25% en 2016-2017 al **29%** en el curso **2019-20**).
- ❖ En **formaciones mixtas** esta cifra aumenta hasta, en algunos casos, el **50%**.

¿De dónde partimos?

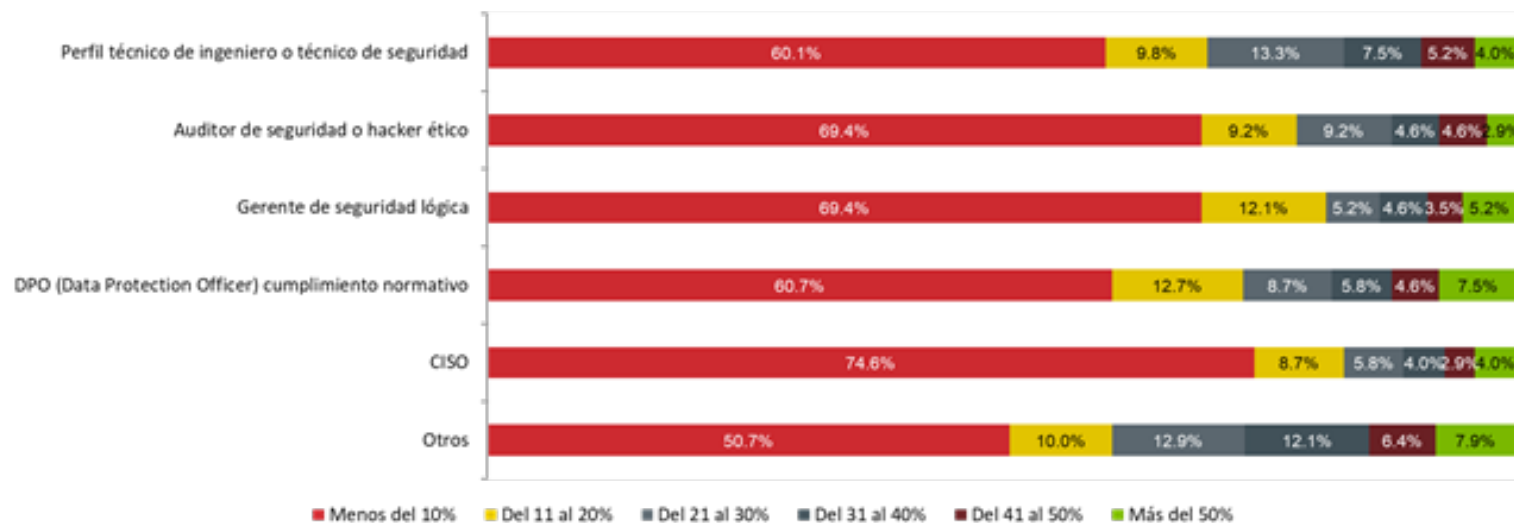
Análisis del talento Femenino en CS en España

PRESENCIA FEMENINA (Profesionales)

31% de presencia femenina en las organizaciones.

Porcentaje menor en **posiciones técnicas** y en **puestos de dirección** en ciberseguridad.

La brecha también se está cerrando de manera progresiva (aumento del 12% en el 2018 al **31%** en el 2020).



Oportunidad de futuro

LA CIBERSEGURIDAD

no es solo cosa del informático



La transformación digital de nuestras empresas necesita más que nunca “*digital workers*” ciberseguros

Expertos que sepan desenvolverse con soltura y ofrecer soluciones ciberseguras en un entorno virtual

Oportunidad de futuro



**Equipos
multidisciplinares y
heterogéneos**

¿Cómo crecer profesionalmente?

Incrementando el valor curricular y los conocimientos

Formación en Ciberseguridad:

- ◆ **Perfiles técnicos** → Formación especializada en nuevas tendencias de CS.
- ◆ **Perfiles no técnicos en disciplinas aplicables a la CS** (Legal, sanitario, educación, etc.) → Formación especializada en CS aplicada a estos perfiles.
- ◆ **Perfiles no técnicos en disciplinas no aplicables a la CS** → Formación especializada en CS para trabajar de manera ciberseguridad dentro de sus sectores de actuación.



Oportunidad de futuro



La importancia del talento en ciberseguridad



1 La ciberseguridad tiene un papel fundamental en el proceso de transformación digital

¿Por qué?

Aumento de las amenazas digitales



Necesidad de proteger los activos digitales



Reputación organizacional



Cumplimiento legal de protección de datos



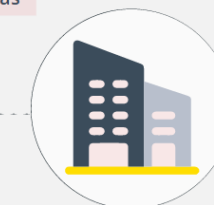
¿Cuáles son las partes interesadas?



Ciudadanía

Empresas

Administración



2 El talento representa un elemento clave en la estrategia de ciberseguridad

¿Cuál es la situación del talento en ciberseguridad en España?



Prioridad en la Administración

Reducir la brecha de talento

Identificar



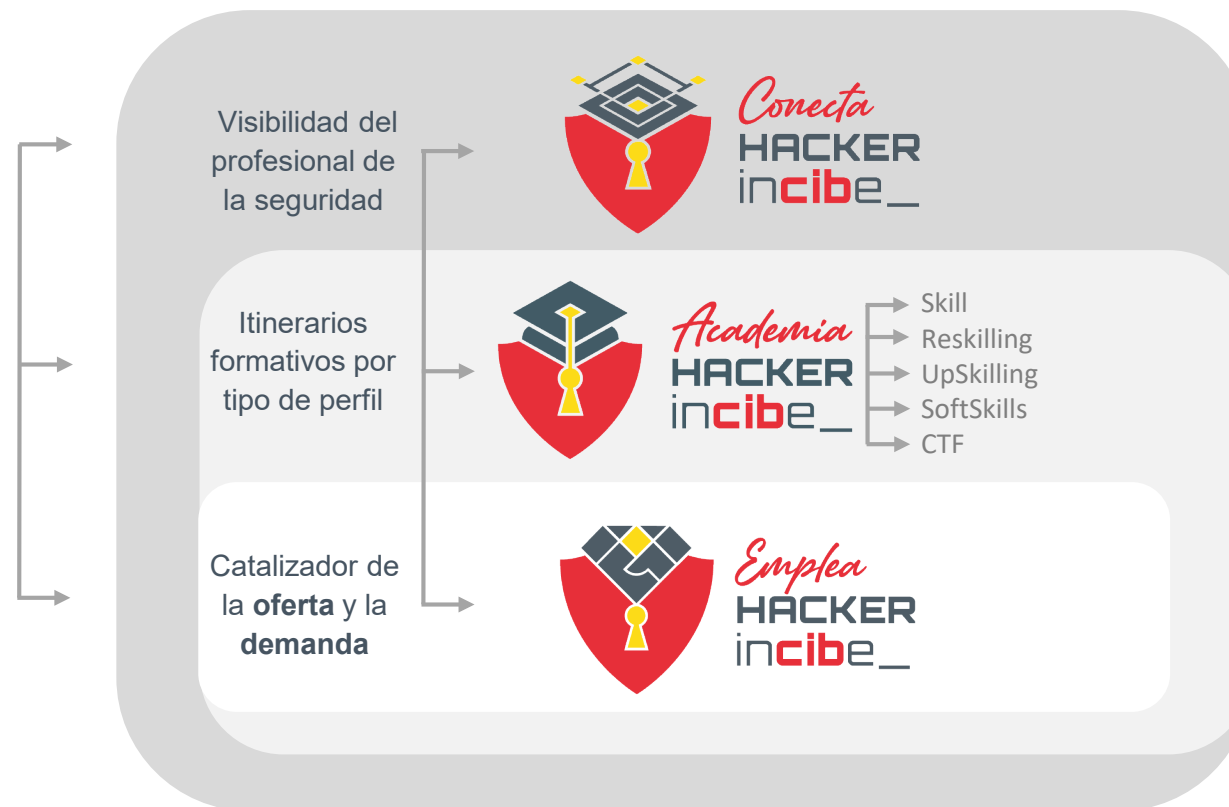
Atraer

Desarrollar



Retener

¿Y ahora qué?



- ◆ Incorporación de más talento femenino a la ciberseguridad
- ◆ Upskilling y reskilling en un contexto de profunda transformación digital
- ◆ Impulso a una industria de alto valor añadido

¿Y ahora qué?

España | digital 2026

INCIBE INCIBE-CERT CIUDADANÍA MENORES EMPRESAS EVENTOS ESPAÑA DIGITAL 2026

Confía INCIBE Emprende Ciberinnova **Talento Hacker** NCC-ES INCIBE Internacionalización RETECH

—

Descubre tu trayectoria Hacker

 **Conecta Hacker**

 **Academia Hacker**

 **Emplea Hacker**

 **Publicaciones**

 **Blog**

<https://www.incibe.es/ed2026/talento-hacker>

¿Y ahora qué?



Conecta
HACKER
incibe_



VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD



Hoy en día vivimos en un mundo digitalizado y conectado donde la mayor parte de los servicios, recursos y uso de datos se hace a través de Internet. Por ello, el uso seguro y responsable de los dispositivos es necesario, tanto para el día a día, como para el ámbito laboral.

talento HACKER

NIÑOS Y NIÑAS
La edad de inicio de uso de tecnología con acceso a Internet es cada vez más temprana. Tener formación en ciberseguridad es esencial para prevenir riesgos como la exposición no controlada de datos privados, y ciberamenazas como el robo y la suplantación de identidad, además de los delitos de odio, entre otros.

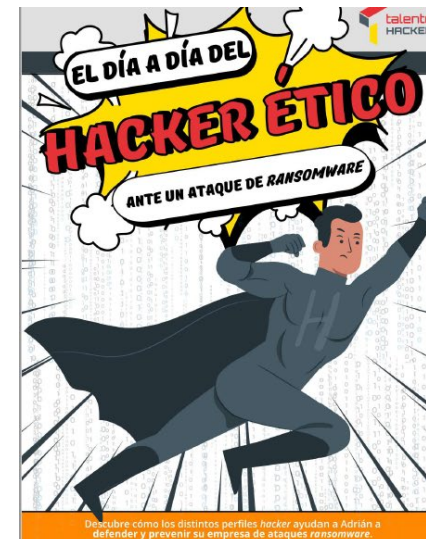
ADOLESCENTES, SECUNDARIA
Muchas personas descubren su interés por la ciberseguridad durante la educación secundaria, momento en el que empiezan a explorarla. De hecho, cada día es más fácil gracias a los contenidos y recursos que existen para empezar a aprender y poner en práctica sus conocimientos.

JÓVENES, ESTUDIOS SUPERIORES
Actualmente hay una amplia oferta de itinerarios formativos que permiten especializarse y dedicarse profesionalmente a la ciberseguridad. Formación profesional, Grados Universitarios y Másteres, son algunas de las opciones para iniciarse en el ámbito y adquirir un título oficial.

PERSONAS EN EDAD ADULTA
Tanto para aquellas personas que tienen formación tecnológica previa como las que no, en la ciberseguridad encontrarán un campo abierto a oportunidades. Los recursos y la oferta formativa existentes proporcionan el escenario ideal para dar un giro en la carrera profesional.

ADOLESCENTES, SECUNDARIA
Muchas personas descubren su interés por la ciberseguridad durante la educación secundaria, momento en el que empiezan a explorarla. De hecho, cada día es más fácil gracias a los contenidos y recursos que existen para empezar a aprender y poner en práctica sus conocimientos.

JÓVENES, ESTUDIOS SUPERIORES
Actualmente hay una amplia oferta de itinerarios formativos que permiten especializarse y dedicarse profesionalmente a la ciberseguridad. Formación profesional, Grados Universitarios y Másteres, son algunas de las opciones para iniciarse en el ámbito y adquirir un título oficial.



Descubre cómo los distintos perfiles hacker ayudan a Adrián a defender y prevenir su empresa de ataques ransomware.

EN UNA MAÑANA DE UN AMANECER CUALQUIERA...

DOCE PERSONAS RECIBEN UNA VIDEOLLAMADA.

MIENTRAS TANTO EN LA EMPRESA DE ADRIÁN...

CIBEREQUIPO

Esas personas, os he llamado porque necesito vuestra ayuda.

¿Nosotros, el ciberesquipo, te ayudaremos.

Óscar, Marta, Sandra, Andrés, Carmen

talento HACKER

Cómo la ciberseguridad se ha convertido en un objetivo estratégico

La digitalización está redefiniendo el futuro de economías, industrias y sociedades tal como las conocemos. La creciente demanda de mayor agilidad, velocidad y flexibilidad marca el inicio de una nueva generación de empresas más distribuidas y conectadas. Ello requiere transformarse en una organización ágil que utilice modelos de negocio rentables y adaptados de una manera rápida y continua a la dinámica del mercado.

En este escenario, la seguridad está siendo una palanca esencial debido a varios factores:

- Crecimiento de los datos digitales
- Crecimiento de las operaciones digitales
- Impulso del teletrabajo
- Incremento de las ciberamenazas

Estos factores impulsan el mercado de la ciberseguridad en España.

Debido a su transversalidad, el mercado de la ciberseguridad crecerá en todos los sectores de la economía, especialmente en el de distribución, servicios y el público.

- Distribución y servicios
- Sector Público
- Financiero
- Infraestructura
- Industria y recursos
- Consumidores

¿Y ahora qué?



Academia
HACKER
incibe_



Talleres temáticos



Hackeando



Retos descargables con solucionarios



Competiciones de ciberseguridad



Curso básico técnico de ciberseguridad

¿Y ahora qué?



Retos descargables con solucionarios

[English](#) [Contacto](#) [Tu Ayuda en Ciberseguridad](#) [Agenda](#) [Sala de prensa](#) [Encuestas](#) [Mapa web](#)



INSTITUTO NACIONAL DE CIBERSEGURIDAD

[Protege tu empresa](#) - [Eventos](#) - [Otras actividades](#) - [Conoce INCIBE](#) - [España Digital 2026](#) -

[Inicio](#) / [Academia Hacker INCIBE](#) / [Retos descargables](#)

Retos descargables

p> Los retos descargables de la **Academia Hacker de INCIBE** tienen la finalidad de formar en materia de ciberseguridad de manera práctica, amena y lúdica.

Consisten en una serie de retos técnicos, clasificados por categoría de reto y nivel de dificultad, que puedes descargar y tratar de resolver. Los retos tienen como objetivo fomentar el aprendizaje de las últimas técnicas de ciberseguridad, mediante una serie de desafíos técnicos que van aumentando su grado de dificultad.

Estos retos descargables, comprimidos con la contraseña "4c4d3m14H4ck3r1NC1B3", tienen una propuesta de solución que te ayudará a resolverlos y aprender de las técnicas y herramientas de ciberseguridad empleadas.

Nivel iniciación

Nivel intermedio

Nivel avanzado

IMPORTANTE

Los retos descargables están comprimidos en un fichero .7z con contraseña "4c4d3m14H4ck3r1NC1B3".

Los ficheros contienen: Enunciado, descargables y solucionario con contexto, descripción para participantes, pistas, solución y *flag*, en pdf y/o video.

Contacto

Si deseas más información, puedes ponerte en contacto con nosotros a través del correo talento.ciberseguridad@incibe.es



Retos descargables

p> Los retos descargables de la **Academia Hacker de INCIBE** tienen la finalidad de formar en materia de ciberseguridad de manera práctica, amena y lúdica.

Consisten en una serie de retos técnicos, clasificados por categoría de reto y nivel de dificultad, que puedes descargar y tratar de resolver. Los retos tienen como objetivo fomentar el aprendizaje de las últimas técnicas de ciberseguridad, mediante una serie de desafíos técnicos que van aumentando su grado de dificultad.

Estos retos descargables, comprimidos con la contraseña "4c4d3m14H4ck3r1NC1B3", tienen una propuesta de solución que te ayudará a resolverlos y aprender de las técnicas y herramientas de ciberseguridad empleadas.

Nivel iniciación



Magic crypto

Categoría: Criptografía

Dificultad: Iniciación

Fecha publicación: 07-06-2022

Descarga: [magiccrypto.7z](#)



Hash cracking

Categoría: Criptografía

Dificultad: Iniciación

Fecha publicación: 07-06-2022

Descarga: [hashcracking.7z](#)



Calculator

Categoría: Ingeniería inversa

Dificultad: Iniciación

Fecha publicación: 07-06-2022

Descarga: [calculator.7z](#)



Análisis de correos

Categoría: Forense

Dificultad: Iniciación

Fecha publicación: 07-06-2022

Descarga: [analisiscorreos.7z](#)



Ruta

Categoría: Criptografía

Dificultad: Iniciación

Fecha publicación: 07-06-2022

Descarga: [ruta.7z](#)



El libro del Quijote

Categoría: Criptografía

Dificultad: Iniciación

Fecha publicación: 07-06-2022

Descarga: [ellibrodelquijote.7z](#)



Nota cifrada

Categoría: Criptografía

Dificultad: Iniciación

Fecha publicación: 07-06-2022

Descarga: [notacifrada.7z](#)



Enigma

Categoría: Criptografía

Dificultad: Iniciación

Fecha publicación: 07-06-2022

Descarga: [enigma.7z](#)



Web ofuscate

Categoría: Web

Dificultad: Iniciación

Fecha publicación: 07-06-2022

Descarga: [webofuscate.7z](#)



Excursión

Categoría: Misceláneo

Dificultad: Iniciación

Fecha publicación: 07-06-2022

Descarga: [excursion.7z](#)



Programa exclusivo

Categoría: Ingeniería inversa

Dificultad: Iniciación

Fecha publicación: 13-06-2022

Descarga: [programa.7z](#)



Exfiltración

Categoría: Forense

Dificultad: Iniciación

Fecha publicación: 13-06-2022

Descarga: [exfiltracion.7z](#)

¿Y ahora qué?



Entrenamientos

Los entrenamientos de la Academia Hacker de INCIBE han contado con dos ediciones en 2021 y estuvieron formadas por:



55
RETOS



7.727
PARTICIPANTES



16
SEMANAS



ONLINE



Junior femenino



Junior masculino



Senior femenino



Senior masculino



Competiciones de ciberseguridad



Competiciones

Las competiciones en ciberseguridad (entre las que se encuentran los *Capture the Flags* o *CTFs*) tienen como objetivo resolver una serie de *tasks* (tareas) que van aumentando su grado de dificultad conforme a los puntos especificados en cada una (Ej. Stego100, Forensics500, etc.).

Dentro de la Academia Hacker INCIBE, se desarrollarán diversas competiciones, en las que los/las participantes podrán poner a prueba sus conocimientos y habilidades.

¿Estáis preparados/as?



Nivel iniciación
(Próximamente)



Nivel intermedio
(Próximamente)



Nivel avanzado
(Próximamente)

¿Y ahora qué?

MOOC “ Introducción técnica a la ciberseguridad”

2 convocatorias



250 horas
17 unidades



Laboratorios
Máquinas virtuales



Certificado posterior

¿Y ahora qué?



ECSC 2023 [See all scores >](#)

COUNTRY	SCORE
1 Germany	18296
2 Switzerland	17783
3 Denmark	17577
4 Netherlands	17545
5 France	17366
6 Italy	17184
7 Sweden	16534
8 Romania	16395
9 Poland	15103
10 Spain	14556

<https://www.youtube.com/watch?v=E49c1q68nyl>
<https://www.incibe.es/eventos/ecsc/seleccion-nacional>

<https://ecsc.eu/>



¿Y ahora qué?



Emplea
HACKER
incibe_



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



Alineados con el *European Cybersecurity Skills Framework* (ECSF) de ENISA

¿Y ahora qué?



Empieza
HACKER
incibe_



SoyHacker

Perfiles ENISA



Apartado dedicado a cada uno de los **perfiles** definidos por la *European Agency for Cybersecurity* (ENISA).

¿Y ahora qué?



Emplea
HACKER
incibe_



Cyber Incident Responder



¿Cuál es su papel en las organizaciones?

¿Qué hace?



Se ocupa de monitorizar el estado de la ciberseguridad de las organizaciones y de gestionar los incidentes cibernéticos, a fin de preservar la protección y el funcionamiento de los sistemas de información.

Misión



El *Cyber Incident Responder* tiene como objetivo monitorizar los sistemas de defensa de las organizaciones en aras de detectar, analizar y evaluar los incidentes de ciberseguridad y así, mitigar su impacto. Además, es el responsable de restablecer el funcionamiento de los sistemas y procesos, además de registrar todas las acciones aplicadas para ello. También, se encarga de recopilar las evidencias de lo sucedido, fase necesaria para identificar el origen de los incidentes, y a las personas implicadas.

Entregables



Plan de respuesta a incidentes.
Reporte de incidentes de ciberseguridad.

¿Qué necesita?

Habilidades

- Conoce y pone en práctica todos los aspectos relacionados con la gestión y respuesta a incidentes de ciberseguridad.
- Recopila y analiza los datos de los incidentes, identificando patrones y tendencias.
- Conoce en profundidad los diferentes tipos de incidentes de ciberseguridad y las amenazas que ponen en riesgo a las organizaciones.
- Trabaja con servidores, servicios nube, sistemas operativos y otras infraestructuras.
- Trabaja en la resolución de problemas y en la toma de decisiones bajo presión.
- Gestiona y analiza los *log files* o archivos de registro.
- Comunica e informa a las partes interesadas sobre los resultados de los análisis.

Su papel en las organizaciones

- ¿Qué hace?
- Misión
- Entregables
- Habilidades

¿Y ahora qué?



Emplea
HACKER
incibe_



Claves para elaborar tu CV en ciberseguridad

Recomendaciones generales:

01

Toda oferta de trabajo tiene su particularidad. Por ello, **el CV ha de adaptarse a la vacante que nos presentamos**, modificando la formación o la experiencia para destacar los elementos más relevantes en cada caso, y siempre con sinceridad.

02

Claridad y concisión. Es preferible que no ocupe más de 1 página, y que el nivel de detalle sea adecuado y ordenado, ya que nos ayudará a superar las primeras cribas.

PRESENTACIÓN

Describe brevemente tus motivaciones profesionales, qué aportarás a la empresa, y/o tus valores.

DATOS DE CONTACTO

Añade el número de teléfono, el correo electrónico y un enlace a tus perfiles en redes profesionales.

EXPERIENCIA

Ordénala cronológicamente, empezando por la más reciente e indicando:

- Inicio y el final de cada periodo.
- Empresa.
- Puesto desempeñado.
- Breve descripción de las funciones y logros alcanzados si son pertinentes.

FORMACIÓN

Incluye las que sean relevantes para el puesto. Si todavía no cuentas con experiencia en el ámbito, destaca el contenido formativo más importante.



PERFIL PROFESIONAL

Añade tu perfil profesional. Puede tratarse de un perfil generalista u orientado a algún campo particular.

FOTO PERSONAL

Es opcional, si bien dará un toque personal y más visual al documento. Asegúrate de que es reciente y que tanto tu aspecto como el fondo de la imagen son adecuados.

OTRAS ACTIVIDADES

Menciona la asistencia a congresos y webinars, o la participación en foros de discusión u otros eventos de ciberseguridad.

OTROS DATOS IMPORTANTES

- Certificaciones en ciberseguridad.
- Habilidades técnicas en ciberseguridad.
- Softskills. Habilidades en comunicación, trabajo en equipo...
- Conocimientos en idiomas, en particular el inglés.

INICIO / España Digital 2026 / Talento Hacker / Emplea Hacker / Hack CV / Herramientas y recomendaciones para buscar trabajo

Herramientas y recomendaciones para buscar trabajo



En ciberseguridad, como en otros sectores, hay numerosos medios o canales para buscar **ofertas de empleo**. Esto, unido a la gran demanda actual de perfiles, ofrece un escenario perfecto para **desarrollar nuestra carrera profesional**. No obstante, conocer las distintas herramientas que tenemos a nuestra disposición, y tener en cuenta algunas recomendaciones, nos ayudarán a encontrar la vacante que más se ajuste a nuestras aspiraciones profesionales con mayor éxito.

A continuación, te mostramos una serie de **herramientas y recomendaciones para la búsqueda de empleo en el ámbito de la ciberseguridad**.

Fuentes y herramientas de búsqueda

Portales de empleo

Los portales de empleo son plataformas que ponen en contacto a empresas con candidatos. Suelen ser bidireccionales, es decir:

- Los **candidatos** pueden inscribirse en las ofertas de empleo que publican las empresas.
- A su vez, permite a las **empresas** realizar búsquedas de los perfiles profesionales registrados en la base de datos, gracias a una serie de filtros.

Existen numerosos **portales de empleo**, algunos de ellos especializados en el ámbito tecnológico. Todos cuentan con un funcionamiento similar: permiten realizar búsquedas de empleo con **palabras clave** y **otros filtros**, como la ubicación, la modalidad (presencial, teletrabajo, mixto, etc.), el tipo de jornada o el contrato laboral y retribución.



INICIO / España Digital 2026 / Talento Hacker / Emplea Hacker / Hack CV / Claves para preparar una entrevista laboral

Claves para preparar una entrevista laboral



La entrevista laboral es una de las fases más importantes de los procesos de selección. Normalmente, antes de alcanzar esta habremos hecho llegar nuestra candidatura junto con nuestro CV, que sirve como una primera criba, y en alguna ocasión incluso superado una primera entrevista telefónica.

Algunas empresas incluyen varias entrevistas en sus procesos, en las que pueden llegar a tomar parte consultoras de selección, el Departamento de RRHH, y el responsable del área o proyecto. Estas permiten conocer al candidato, sus conocimientos y experiencia en torno al campo relativo a la vacante, su valor diferencial respecto a otros candidatos o sus motivaciones profesionales con vistas a largo plazo.

En definitiva, la entrevista supone una oportunidad para mostrar nuestro potencial, y, por tanto, su preparación será determinante para alcanzar nuestra meta.

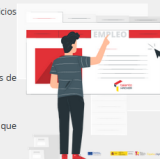
CLAVES PARA PREPARARTE UNA ENTREVISTA LABORAL EN EL ÁMBITO DE LA CIBERSEGURIDAD

1. Conoce la empresa

Busca información de la empresa en su web y/o en otras fuentes: su historia, actividad, situación actual, productos y servicios que ofrece. Además, puedes profundizar sobre el puesto concreto al que va dirigida la vacante:

- Obtén toda la información posible del área o departamento al que te presentas.
- Revisa su apartado de empleo. Algunas empresas cuentan en su web con un área dedicada a la publicación de ofertas de trabajo, donde aparece una descripción de sus valores y perfiles que buscan.

Esta información te servirá para responder adecuadamente a las preguntas sobre la empresa, y, a su vez, a identificar lo que esta espera de ti.

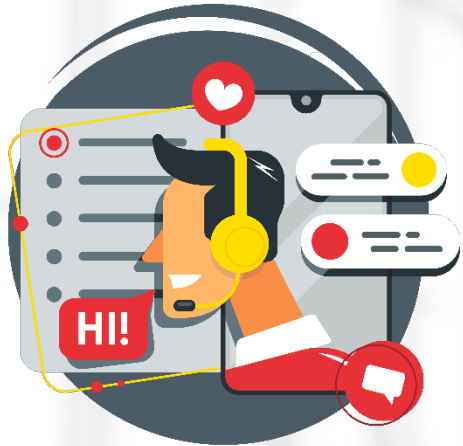


2. Revisa tu experiencia, formación y habilidades a partir de tu CV

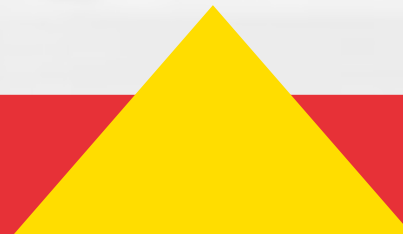
Conocer tu CV te permitirá resaltar la información de interés para la vacante, y responder a las preguntas de manera clara y concisa. En este sentido, evita respuestas monosilábicas (sí o no). En su lugar, ofrece una explicación sin extenderse en detalles irrelevantes y siempre con sinceridad.

Tanto si es presencial como en remoto, recuerda contar con una copia de tu CV, ya que te servirá como apoyo durante la entrevista.





¿Preguntas?





INSTITUTO NACIONAL DE CIBERSEGURIDAD

Gracias



SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

