

# BALANCE DE CIBERSEGURIDAD

**+24%** INCREMENTO SOBRE 2022

**83.517** Incidentes de ciberseguridad

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

**183.077** Sistemas vulnerables

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

DEL TOTAL DE INCIDENTES DE CIBERSEGURIDAD

**+22.000** empresas españolas se ven afectadas

**+58.000** ciudadanos son víctimas de incidentes

**INCIDENTES REFERENTES A CIUDADANÍA Y EMPRESAS**

- +8.800 accesos e intentos de acceso** no autorizados a información de una red o sistema informático de empresas, ciudadanía o familias españolas (por ejemplo, un extraño entra a una casa, sin permiso).
- +9.000 ataques** que han inutilizado los dispositivos de organizaciones o ciudadanos.
- +28.000 casos de fraude** reportados por las víctimas.
- +26.000 dispositivos dañados** por software malicioso.
- +7.000 sitios detectados** que albergaban contenido abusivo y la correspondiente retirada de los mismos.
- +1.400 accesos no autorizados** a datos importantes, como contraseñas, números de tarjetas de crédito o información personal (por ejemplo, alguien entra en un espacio digital y se lleva cosas valiosas sin permiso).

**237** Operadores esenciales y críticos

Empresas o servicios que son muy importantes para el funcionamiento diario de la sociedad. Incluye sectores, como la energía, el agua o las comunicaciones.

- 25,42%** Sistema financiero y tributario
- 25,00%** Transporte
- 22,08%** Energía
- 18,33%** Tecnologías de la Información y Comunicación (TIC)
- 4,58%** Agua

## INCIDENTES MÁS FRECUENTES

**+7.400** incidentes son contenido abusivo\* (Pornografía infantil, delitos de odio, ciberacoso, etc.)

**28.258** En concreto, **3 de cada 10** incidentes son fraude online

**INCIBE clausura 310 tiendas online** por fraude en 2023

**14.261** 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.

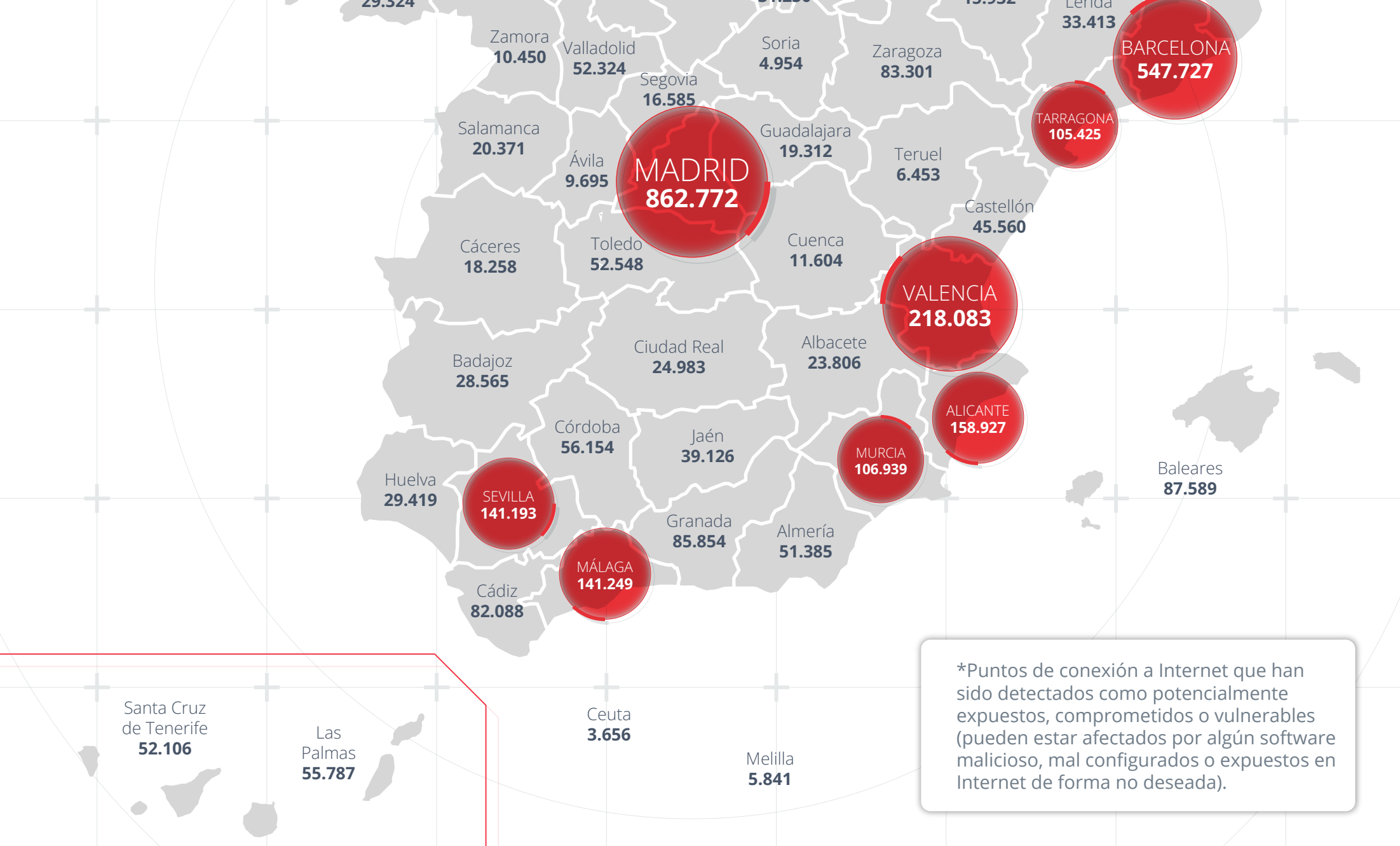
**+26.200** incidentes, en concreto, **3 de cada 10** están afectados por virus informáticos u otros software maliciosos que infectan los dispositivos, como equipos o teléfonos móviles, causando daños o robando información personal.

Del total de esta categoría, **621** son secuestros digitales donde los ciberdelincuentes bloquean el acceso a los archivos o sistemas, pidiendo dinero para devolvérselos a las víctimas.

**1 de cada 10** incidentes afectan a la **disponibilidad de la información**

Las víctimas no han podido acceder a los datos o sistemas afectados cuando lo necesitaban. Por ejemplo, no poder acceder a una web porque está siendo atacada.

## 59% DE LOS INCIDENTES SON DE PELIGROSIDAD "MUY ALTA" Y "ALTA"



## VULNERABILIDADES DETECTADAS



## BALANCE DE LA LÍNEA DE AYUDA

Incremento del **16,8%**

**80.920** Consultas y problemas de la Línea de Ayuda de INCIBE

- +61.000** personas atendidas por vía telefónica
- +16.400** usuarios atendidos por canales de chat
- +3.300** personas atendidas por correo electrónico

- 12%** de los usuarios que consultan a la línea de ayuda es en relación a algún tipo de suplantación de identidad digital.
- 11%** de las consultas de menores han solicitado ayuda y asesoramiento sobre casos de ciberacoso.
- 3 de cada 10** usuarios han recibido algún intento de phishing, llamada de vishing o mensaje de smishing.
- +5.300** personas han necesitado asesoramiento debido a compras fraudulentas en Internet.
- +4.100** usuarios que han trasladado sus dudas sobre fraudes de mensajería instantánea.
- 19%** de las empresas han contactado para reportar correos electrónicos que llegan mediante phishing.
- 645** se registran reportes de contenidos inadecuados relacionados con abuso sexual infantil a través de nuestra hotline.

**CONSULTAS DE EMPRESAS**

- Phishing: 18,5%
- Fraude Business Email Compromise: 11,4%
- Suplantación de identidad: 14,3%

Completan el ranking: denegación de acceso, ransomware y concienciación de los empleados y buenas prácticas en ciberseguridad, entre otras.

**CONSULTAS DE LA CIUDADANÍA**

- Vishing: 12%
- Smishing: 11,5%
- Suplantación de identidad: 11,7%

Completan el ranking: compras fraudulentas, fraudes en mensajería instantánea y phishing, entre otras.

**CONSULTAS DE MENORES Y SU ENTORNO**

- Privacidad y reputación: 21,4%
- Ciberacoso: 11,4%
- Suplantación de identidad: 10,6%

Completan el ranking: sextorsión, mediación parental, configuración y protección de dispositivos, entre otras.

Un **4,1%** de las consultas recibidas en el 017 se refieren a los peligros del acceso de menores a contenidos inadecuados en Internet (comunidades peligrosas o contenidos abusivos, como contenidos que fomentan el odio y la violencia o acciones perjudiciales para la salud).

**1.673** incidentes referentes a universidades, instituciones sanitarias y otras entidades.

Distribución de entidades de RedIRIS:

- 37,14%** de entidades privadas
- 62,86%** de entidades públicas

Incidentes de entidades públicas de RedIRIS	114
Incidentes de entidades privadas de RedIRIS	14
<b>Total de incidentes en entidades públicas de RedIRIS</b>	<b>1.633</b>
<b>Total de incidentes en entidades privadas de RedIRIS</b>	<b>40</b>

## FORMACIÓN Y CONCIENCIACIÓN

**+117.000** PERSONAS FORMADAS en ciberseguridad con INCIBE durante 2023

**40,7 mill.** PERSONAS ALCANZADAS con campañas publicitarias de concienciación de INCIBE (medios digitales, TV, prensa escrita, radio y elementos exteriores).

- +108.000** personas se han formado en ciberseguridad durante el **Día de Internet Segura 2023**, como en otras acciones formativas dedicadas a menores y ciudadanía, con especial atención al público sénior, y a los docentes. Se han impartido más de **177.000 horas** de capacitación.
- #ExperienciaINCIBE** que está compuesta por un camión desplegable y un stand itinerante, ha contando con más de **10.000** participantes, desde su puesta en marcha.
- +470** personas, de **24** países diferentes, han participado en acciones de capacitación durante el **Cybersecurity Summer Bootcamp**. El programa va dirigido a Fuerzas y Cuerpos de Seguridad, jueces, magistrados y especialistas de CERT, entre otros.
- 11.483** personas han participado en los eventos coorganizados por las **11** universidades, que componen el programa **CyberCamp**, e INCIBE, en las diferentes comunidades autónomas españolas.
- 3.705** personas formadas durante 2023 por **404** cibercooperantes. Los **cibercooperantes** totales son **1.143**.

## RETOS 2026

El crecimiento en la inversión en el **017** multiplicará **x4** la capacidad del mismo hasta 2026.

**EMPRENDIMIENTO**

**35** entidades colaboradoras desarrollarán con INCIBE acciones para impulsar el emprendimiento en ciberseguridad: acciones de captación (datos reflejados en el mapa), **84** ediciones de incubación y **62** de aceleración.

Distribución hasta 2026 en las CCAA incluidas Ceuta y Melilla

	CHARLAS	TALLERES	EVENTOS
Andalucía	228	74	29
Aragón	165	59	19
Asturias	24	16	8
Baleares	92	20	4
Cataluña	48	32	8
Cataluña	60	38	4
Canarias	84	30	0
Castilla La Mancha	268	86	48
Castilla y León	314	1	54
Comunidad Valenciana	249	57	34
La Rioja	40	24	12
Murcia	23	16	12
Navarra	28	20	0
País Vasco	68	16	4
Ceuta	16	8	0
Melilla	16	8	0

1.840 empresas de ciberseguridad registradas en el catálogo de INCIBE.

\*Datos relativos al catálogo de ciberseguridad del mes de diciembre de 2022.