# Panorama actual de la Ciberseguridad en España

Retos y oportunidades para el sector público y privado

Google

# La ciberseguridad en España

Una perspectiva desde las Pymes, sociedad civil y administración pública

Google

Nota: Este informe fue encargado por Google y preparado por The Cocktail Analysis. Google no proporcionó datos internos para generar estas estimaciones. Todos los datos del informe se basan en fuentes externas y en las propias encuestas realizadas por The Cocktail Analysis

the cocktail® analysis

C/ Salamanca, 17, 28020 Madrid
+34 91 567 06 05
info@tcanalysis.com

# Índice

# INTRODUCCIÓN

La ciberseguridad es ahora más importante que nunca. Gobiernos, empresas y particulares usan softwares y todo el universo está cada vez más conectado. También lo están los dispositivos, lo que abre oportunidades de crecer como sociedad, pero también propone nuevos retos... ¡y nuevas ventanas para los criminales online!

En VirusTotal analizamos más de dos millones de ficheros únicos y nuevos al día, de los cuales más de 350.000 son detectados por cinco o más motores antivirus e identificados como software malicioso. Hablamos de 350.000 nuevas variantes de *malware* al día.

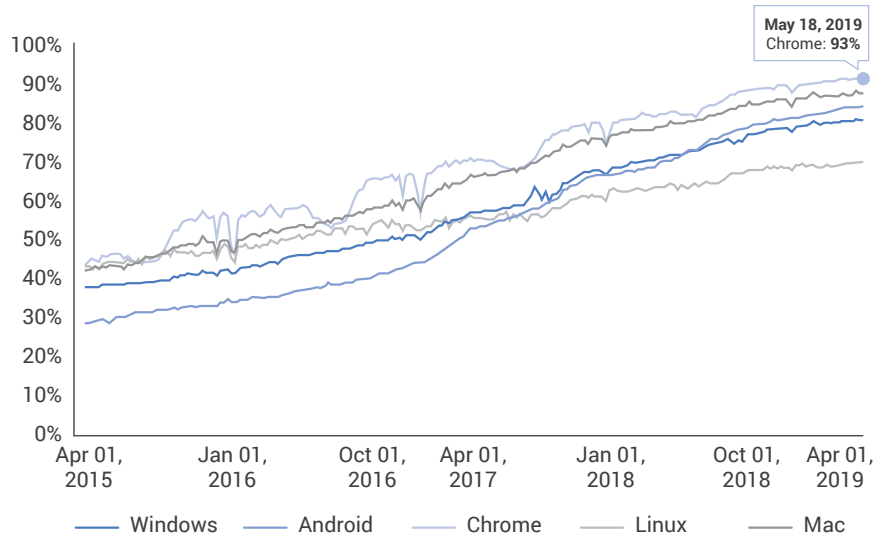
El término *malware* es un cajón desastre que engloba todo tipo de amenazas informáticas. Además de los famosos virus informáticos, tenemos los temidos *ransomware,* que cifran nuestros datos para pedir un rescate por ellos. También *troyanos* bancarios, que suplantan nuestra identidad para hacer transferencias desde nuestras cuentas en la banca online.

Luego están los *backdoors*, que son capaces de acceder a nuestros datos y grabarnos por la cámara, e incluso APTs, capaces de explotar vulnerabilidades en los sistemas y sabotear infraestructuras críticas. Hay decenas de *malware* diferentes dependiendo de sus características comunes. Y todas tienen un único objetivo: atacarnos.

Afortunadamente, no solo ha evolucionado el cibercrimen, sino que también hemos asistido a un considerable refuerzo de la seguridad en internet.

**Gráfico 1**

Porcentaje de páginas cargadas mediante HTTPS en Chrome, por plataformas



Han aumentado las conexiones web y nuestros datos viajan cifrados de extremo a extremo e impiden que terceros puedan espiarnos capturando el tráfico en tránsito. Por ejemplo, en marzo de 2015 solo el 45% de las páginas visitadas en Chrome utilizaba el protocolo https. Este porcentaje se elevó al 93% en mayo de 2019.

La implantación de 2FA (segundo factor de autenticación) sigue incrementando su adopción de forma constante (28%), aunque todavía está lejos de lo deseable. Fue ganando popularidad en la banca online española para prevenir estafas derivadas del *phishing* y troyanos que roban el usuario y contraseña de acceso. A día de hoy, ya existen múltiples opciones para prevenir el 96% de los ataques de *phishing* y el 76% de los ataques dirigidos.

El futuro tiene pocas certezas, pero sí sabemos que será más automático y dependiente de la tecnología. Atrás quedaron los días en los que nuestro trabajo era proteger ordenadores. Nuestra acción ahora es construir confianza ofreciendo seguridad a negocios, personas y gobiernos. Nuestro nuevo trabajo es proteger a la sociedad, algo en lo que todos podemos y debemos participar de forma activa.

**Bernardo Quintero**
*Founder* de VirusTotal

# RESUMEN EJECUTIVO

Si eres emprendedor autónomo o dueño de una pyme es probable que vendas tus artículos online o que tengas cámaras de seguridad conectadas a internet en tu local. Seguro que realizas videollamadas con tus clientes y por supuesto, recibes y envías correos electrónicos a diario, al igual que tus trabajadores. Esta velocidad de innovación, esta facilidad para comunicarnos, ofrecer nuestros servicios y acercarnos a los clientes es casi ilimitada y ya forma parte de nuestra vida y nuestros negocios, lo cual puede hacernos olvidar que toda revolución tiene sus retos.

En este estudio queremos profundizar en uno de los principales: **la ciberseguridad**. ¿Cómo nos protegemos ante las amenazas del ciberespacio? ¿Cómo hace frente el tejido empresarial español —compuesto en su mayoría por pymes— a los nuevos riesgos online? ¿Cuál es la percepción de los principales actores políticos y económicos ante el acelerado incremento del número de ciberataques a nivel mundial?

- **Pymes: el 99,8% del tejido empresarial español no se considera un objetivo atractivo para un ciberataque.** Esto se traduce en que casi 3 millones de empresas en España están poco o nada protegidas contra hackers. La cultura de la ciberseguridad en las pymes españolas es todavía reactiva. Tan solo un 36 % de las pymes encuestadas tienen establecidos protocolos básicos de seguridad, como la verificación de dos pasos para el correo de empresa, y el 30 % de las webs no disponen del protocolo https. La pyme es el eslabón más vulnerable de esta cadena, por falta de medios, tiempo, e incluso concienciación.

  **El 60% de las pymes europeas que son víctimas de ciberataques** desaparece en los seis meses siguientes al incidente, muchas veces lastradas por el coste medio del ataque, que suele rondar los 35.000 euros.

- **Grandes empresas y gobiernos: tienen cada vez más presente la ciberseguridad en sus planes de acción.** En España, el CNI-CERT, Centro Criptológico Nacional, detectó 38.000 incidentes de ciberseguridad —ataques al sector público— en 2018, lo que supone un incremento del 43% respecto al año anterior. En contrapartida, la ciberseguridad gana más relevancia en la agenda pública: por primera vez todos los partidos políticos incluyeron en sus programas electorales alguna medida relacionada con la necesidad de garantizar la seguridad en internet.

  El 84% de las empresas españolas incrementará su inversión en ciberseguridad en los próximos tres años, y destinará a ello un mínimo del 10% de su presupuesto informático.

- **Usuarios: existe un nivel elevado de concienciación, pero no se traduce en una implementación de protocolos de seguridad.** Un 62% manifiesta conocer protocolos https y un 75% conoce y utiliza la verificación en dos pasos en sus compras, transacciones bancarias, etc. Sin embargo, solamente:

  - El 14% actualiza sus contraseñas con regularidad.
  - El 21% hace regularmente copias de seguridad de sus archivos y actualiza los sistemas operativos de sus dispositivos

## ¿Cómo cuantificamos este estudio?

Para realizar esta radiografía de la ciberseguridad en España se han combinado varias metodologías de recogida de datos con el fin de ofrecer una visión lo más amplia y completa posible.

Fórmulas metodológicas:

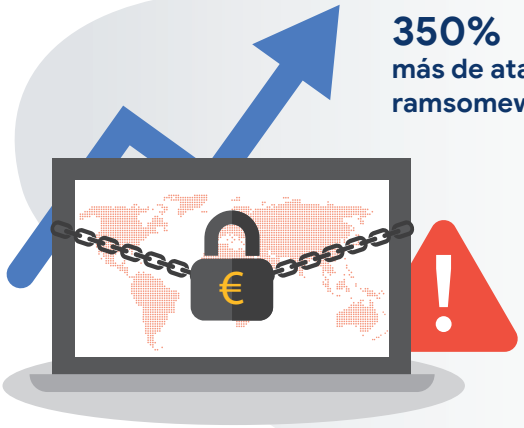
- **Desk Research:** análisis de fuentes secundarias sobre cifras e indicadores básicos del ámbito de la ciberseguridad.
- **Entrevistas a expertos:** investigación cualitativa a través de entrevistas a profesionales de la administración pública y responsables de las grandes corporaciones. Entrevistas realizadas: **12.**
- **Encuesta a pymes:** investigación cuantitativa que analiza la ciberseguridad en el ámbito de las pequeñas y medianas empresas. Tamaño muestral: **720 encuestas telefónicas**.
- **Encuesta a usuarios de Internet:** investigación cuantitativa que profundiza en la concienciación de los usuarios ante las amenazas de la ciberseguridad. Tamaño muestral: **817 encuestas online**.

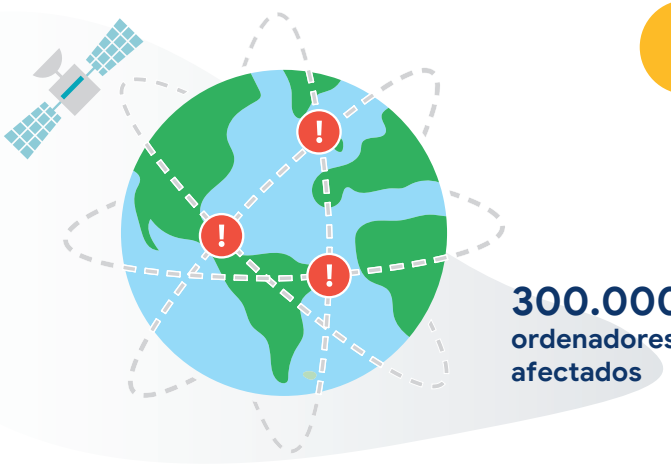
# PRINCIPALES CONCLUSIONES SOBRE LA CIBERSEGURIDAD EN ESPAÑA

1

**Incremento del número de ciberataques a nivel mundial:** en 2018 hubo un 350% más de ataques de *ransomware* (programa malicioso que restringe el acceso a determinadas partes o archivos del sistema operativo infectado, y pide un rescate a cambio de quitar esta restricción) que en el año anterior.

Las pérdidas generadas por los ciberataques ascienden al 0,8% del PIB Mundial, estimado en unos 74,15 billones de euros.




2

**La ciberseguridad es una disciplina que traspasa fronteras y requiere de una legislación transnacional.** Por ejemplo, en 2018 el *ransomware* WannaCry infectó a 300.000 ordenadores de 150 países, afectando a más de tres cuartas partes del planeta, y causó pérdidas de 3.500 millones de euros:

**1.000 millones más** que el presupuesto nacional de educación.

3

El 99,8% del tejido empresarial Español —compuesto por pymes— no se considera un objeto atractivo a los ciberataques.

**Casi 3 millones de empresas en España** están poco o nada protegidas contra hackers.

4

Actualmente dos tercios de las empresas españolas carecen de suficientes empleados para combatir las amenazas del ciberespacio.

**En Europa se necesitarán 350.000 profesionales del sector de la ciberseguridad en los próximos tres años.**



5

**Pymes y usuarios particulares fueron los principales objetivos de los ciberataques en 2018,** con un total de 102.414 incidentes registrados en España.

Actualmente estos ataques son más masivos, en forma de cientos de pequeños ataques contra objetivos poco protegidos y requieren la intervención del usuario.

6

**El coste medio de un ciberataque a una pyme es de 35.000 euros** y el 60% de las pymes cierra seis meses después de haber sufrido un ciberataque.


7

La cultura de la ciberseguridad en las pymes españolas es todavía reactiva.

**Tan solo un 36% de las pymes encuestadas tiene establecidos protocolos básicos de seguridad** como la verificación de dos pasos para el correo de empresa.

El 30% de las webs no dispone del protocolo https.

8

**Apenas un 14% de los usuarios encuestados actualiza sus contraseñas** y solo un 21% hace regularmente copias de seguridad de sus archivos.


9

**Solo 1 de cada 10 usuarios encuestados se manifiesta completamente seguro cuando accede a internet.**

El 75% considera la ciberseguridad como muy importante pero solo 1 de cada 4 tiene antivirus de pago en sus dispositivos, tanto en ordenadores como en tablets o teléfonos móviles.

# DE LOS CIBERATAQUES A LA PREVENCIÓN: COMPRENDIENDO EL FENÓMENO EN ESPAÑA

Un buen punto de partida para comprender la importancia de la ciberseguridad y su urgencia es conocer el comportamiento de los ciberataques —tanto en el sector público como en el privado—, examinando las cifras, tipologías, objetivos.

También resultan reveladoras las opiniones y declaraciones de los expertos consultados y las pymes encuestadas en este informe, que nos permiten conocer las principales necesidades y las medidas que se están tomando. Todo ello nos da una idea de en dónde estamos y hacia dónde vamos en materia de ciberseguridad en España.

# ¿Qué son los ciberataques?

## Definición

### Un gran reto: diferenciar entre los distintos tipos de delitos informáticos

Europol define así los ciberataques[1]: "Cualquier delito que solo se puede cometer utilizando ordenadores, redes informáticas y otras formas de tecnología de comunicación de la información (TIC)". Junto a esta conceptualización tan generalista aparecen otras más específicas, como la que ofrece el Manual de Tallin[2], más orientada a las consecuencias: "Aquella operación cibernética, ofensiva o defensiva, de la que se espera que pueda causar pérdidas de vidas humanas, lesiones a las personas o daños y destrucción de bienes".

Pero a pesar de la diferencia de enfoques, las definiciones siguen siendo demasiado generales y uno de los retos en el campo de la seguridad de la información es justamente conocer los distintos tipos de delitos informáticos y poder distinguirlos.

---

1 Europol *"IOCTA 2018"* https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

2 Manual de Tallin (Tallinn Manual on the International Law Applicable to Cyber Warfare): Este documento establece las bases para elaborar un protocolo de actuación en caso de guerra cibernética. Ha sido elaborado por el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN.

En ese sentido, ¿quién no ha sufrido un ciberataque o conoce a alguien que haya sido víctima de uno? Desde el hackeo de un perfil en las redes sociales a la sustracción de saldo de una cuenta bancaria, la denegación temporal de servicios de la web de una empresa o la destrucción de información o equipos irremplazables; es muy probable que conozca algún caso cercano.

Malware o software malicioso: Tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Su nombre se debe a la unión de los términos "malicious software". Esta definición general incluye: virus, gusanos, troyanos, backdoors, spyware, etc.

Virus: Malware diseñado para que al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo. Necesita de la acción humana.

Spyware o software espía: Malware que recopila información de un ordenador y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del ordenador.

Ransomware: El ciberdelincuente toma control del equipo infectado y «secuestra» la información del usuario cifrándola, para luego pedir un "rescate" por los datos.

Troyanos: Malwares que se caracterizan por carecer de capacidad de autorreplicación y generalmente, este tipo de malwares requieren del uso de la ingeniería social para su propagación.

Gusanos: Malwares que tienen como característica principal su rápida propagación, realizando copias de sí mismos e infectando a otros ordenadores, independientemente de la acción humanas.

Phishing: Estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir información confidencial (contraseñas, datos bancarios, etc.) de usuarios legítimos de forma fraudulenta.

Ddos: Mediante este tipo de ataques se busca sobrecargar un servidor y hacerlo colapsar, para que los usuarios legítimos no puedan utilizar los servicios prestados por él.

*Ver más en el Glosario*

## Objetivos de los ciberataques

### Ante una mayor protección de las grandes compañías, cada vez hay más ataques dirigidos a pequeñas empresas y ciudadanos

En este estudio se hace una distinción entre **los ataques entre Estados**, que suelen calificarse como "actos de guerra" u operaciones de ciberinteligencia y ciberespionaje, y **las actividades criminales**, dirigidas sobre todo a empresas y ciudadanos.

Las grandes compañías invierten cada vez más en protegerse de los cibercriminales, cosa que no ocurre entre pymes y usuarios, en parte por razones económicas y en buena medida también porque erróneamente no se consideran un blanco de las amenazas.

Actualmente, en las grandes empresas prima una estrategia: analizar los riesgos y **conocer a los atacantes** con el objetivo de prevenir sus acciones. "La pregunta no es: «¿Me van a atacar?». Damos por sentado que vamos a ser atacados, así que la pregunta es: «¿Cómo vamos a reaccionar?»", explica Alejandro Villar, director de Cybersecurity & Technology Risk en Repsol.

Los bancos españoles, por ejemplo, han dado una especial importancia a la seguridad informática desde los años 90 estando cada vez más protegidos. "No tienen nada que envidiar a los de Estados Unidos", asegura David Barroso, *Founder* de CounterCraft.

La realidad es que, contra lo que muchos creen, **cada vez hay más ataques dirigidos a pequeñas empresas y ciudadanos**, no solo por la debilidad tecnológica de estas sino también por el desconocimiento sobre las ciberamenazas.

La tendencia, según los expertos consultados, va en ese sentido: a mayor protección de las grandes compañías, los ciberdelincuentes centran sus esfuerzos cada vez más en **objetivos más pequeños**. Y muchos responsables de pymes que subestiman el riesgo lo pensarían dos veces si supieran que, de media, un ciberataque a una empresa de tamaño modesto suele costarle **unos 35.000 euros**[3].

> "Las pymes entienden de zapatos o mecánica, pero no entienden de ciberseguridad. Muchas veces la viabilidad económica de estas empresas depende de un ataque contra un equipo en el que han cifrado toda la base de datos de clientes, y de repente se quedan sin nada. Porque su negocio reside en ese ordenador, en esos datos. A sectores que eran analógicos se les ha vendido lo bueno de lo tecnológico, pero no se les ha advertido del lado negativo o de la necesidad de estar ciberpreparados"
>
> Elena Matilla, de Red Eléctrica

3 Karspersky Lab & Ponemon Institute: *"No hay víctimas pequeñas para los cibercriminales"*. https://www.kaspersky.es/about/press-releases/2017_no-small-victims-for-cybercriminals

## TIPOLOGÍA

*Los ataques a grandes empresas han disminuido para dejar paso a un mayor número de ataques a pymes y ciudadanos. Este cambio de objetivo define la naturaleza de los ciberataques actuales*

- **Ataques menos dirigidos y más masivos**: se lanzan a discreción sobre muchas víctimas potenciales y son poco complejos técnicamente. Un ejemplo: la distribución de correos con *spam* entre pymes para infectar cualquier dispositivo mal protegido o el llamado fraude del CEO, los atacantes se hacen pasar por el CEO de una empresas y escriben al departamento financiero solicitando una transferencia para realizar una compra. Son muy numerosas las pequeñas empresas que han perdido dinero con estos tipos de ataques.
- **Ataques profesionalizados**: tienen un componente muy especializado y con un objetivo muy definido. "Los ataques más casuales, simplemente movidos por la curiosidad técnica de los hackers ya no se dan, siempre te atacan para conseguir algo, ya sea con un objetivo económico, o simplemente porque pueden utilizar tu email para usarlo en nuevos ataques" como explica Hugo Teso, experto en ciberseguridad. "Debes tener una infraestructura, invertir cierto tiempo en conocer a esa empresa y tener todo un equipo de personas trabajando en el golpe. Son verdaderas organizaciones criminales", señala Eva Cañete, Chief Information Security Officer de Unicaja Banco.
- **Ataques que requieren de intervención humana:** se aprovechan de la falta de concienciación de usuarios y empleados (especialmente dañinos para pymes, que suelen contar con protocolos de protección menos avanzados y un bajo nivel de sensibilización entre su personal): "alguien que haga clic en un enlace malicioso, pinche un adjunto que no debe abrir, de una información por teléfono que no debe dar...", explica Elena Matilla, Chief Information Security Officer de Red Eléctrica.

> "Hay una profesionalización del atacante: no es lo mismo robo de propiedad intelectual que robo económico, y no es lo mismo ataque a empresas que ataque a cliente final. El atacante es especialista en el objetivo a atacar, y es una especialización, además, de años. Es ya una industria."
>
> Bruno Díaz, experto en ciberseguridad

**1.000 millones de personas suponen:**

- 3 veces la población de EEUU.
- 5 veces la población de Nigeria.
- 10 veces la población de Egipto.
- 21,7 veces la población de España.

## ¿Cómo afectan los ataques al sector privado?

### Ciberataques en aumento a nivel mundial: se triplican los ataques de *ransomware*

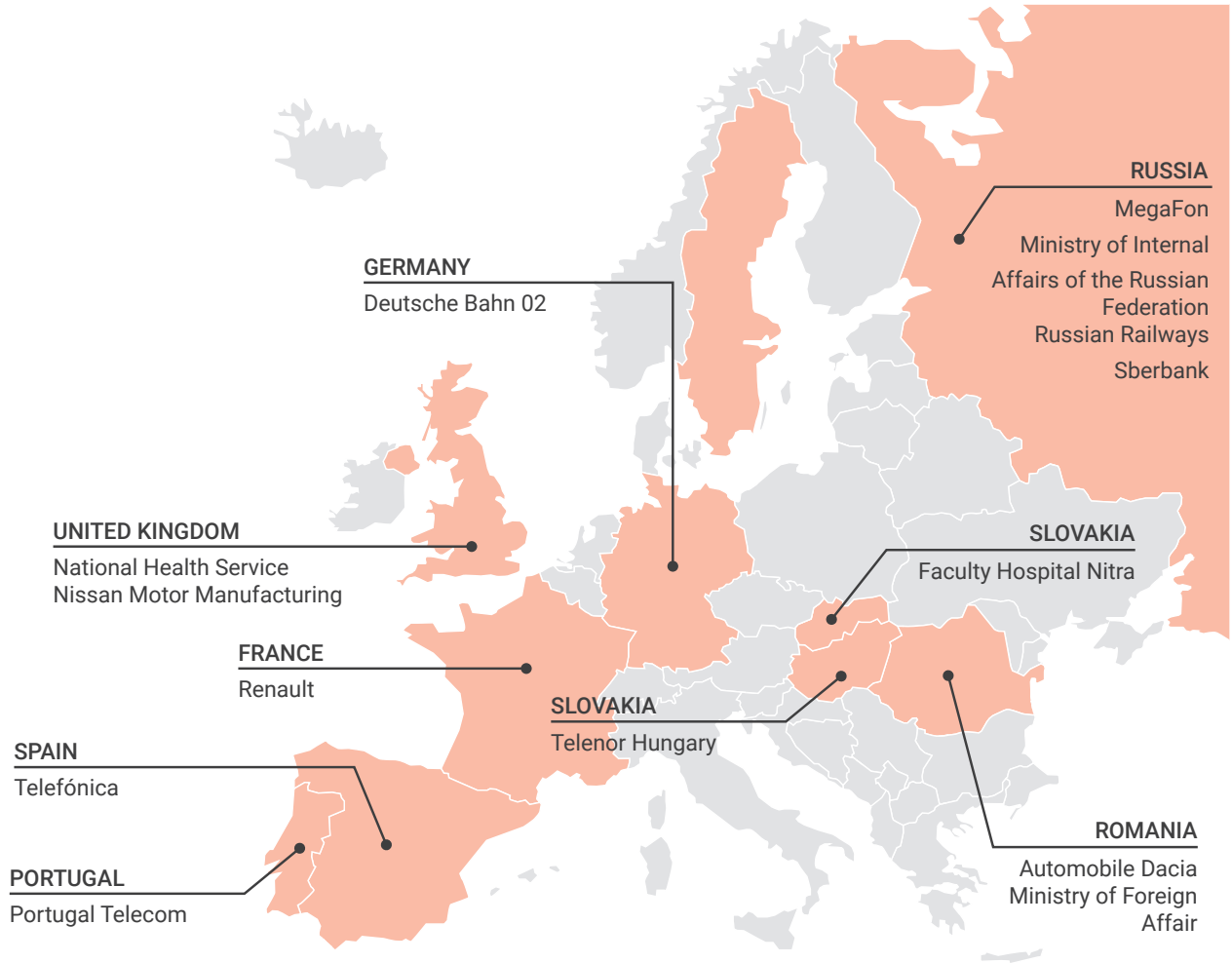
**El *ransomware* es de los ciberataques más extendidos y peligrosos.** Limita el acceso del usuario al equipo infectado mientras no se pague un rescate. Solo en 2018, el número de afectados por estos ataques fue de **más de 1.000 millones en todo el planeta**.

WannaCry es el *ransomware* más conocido y mediático hasta la fecha. Ocasionó pérdidas aproximadas de **4.000 millones de dólares** y los países más perjudicados fueron Rusia, Ucrania, India y Gran Bretaña, afectando a un centenar de empresas como Renault, Nissan y FedEx.

En España, la firma más afectada fue Telefónica, además de centrales energéticas, aeropuertos e importantes compañías relacionadas con el transporte público y las comunicaciones, cuyos nombres se mantienen en secreto para no propiciar nuevos ataques.

**Figura 1**

Estos son los países y principales blancos de Wannacry en Europa




Fuente: IOACTA 2018 Europol.

Según la Comisión de Valores e Intercambio de Estados Unidos[4], los ciberataques fueron en aumento durante 2018 y las pérdidas siguen creciendo de manera exponencial.

En 2018 el porcentaje de ataques a nivel mundial aumentó:

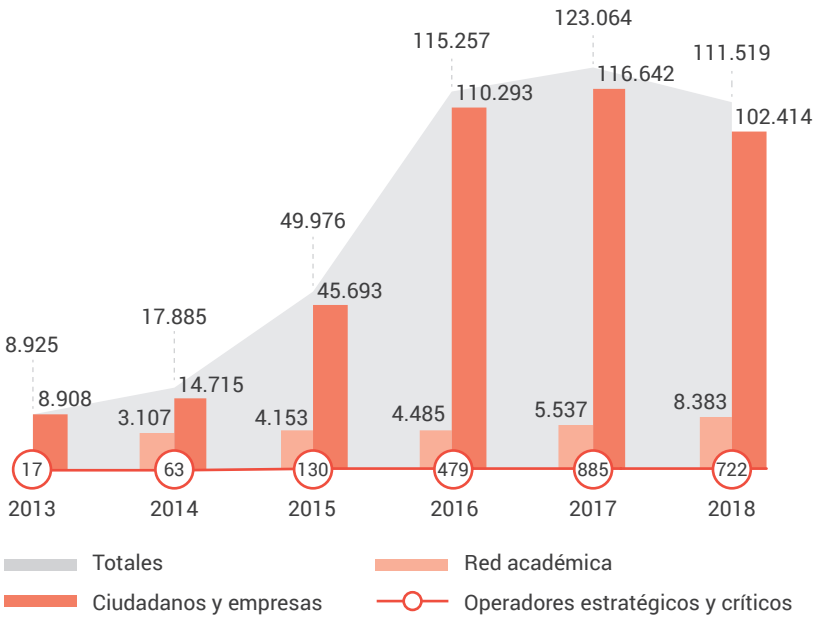
| | |
|---|---|
| 350% | en los ataques de *ransomware* |
| 250% | en los ataques de suplantación de identidad o de correo electrónico comercial |
| 70% | en los ataques de *phishing* |

## Cifras en España

### El caso español: 102.414 incidentes contra ciudadanos y empresas durante 2018

**Gráfico 2**

¿Cuántos incidentes ha gestionado el INCIBE en los últimos años?




Fuente: Instituto Nacional de Ciberseguridad (INCIBE).

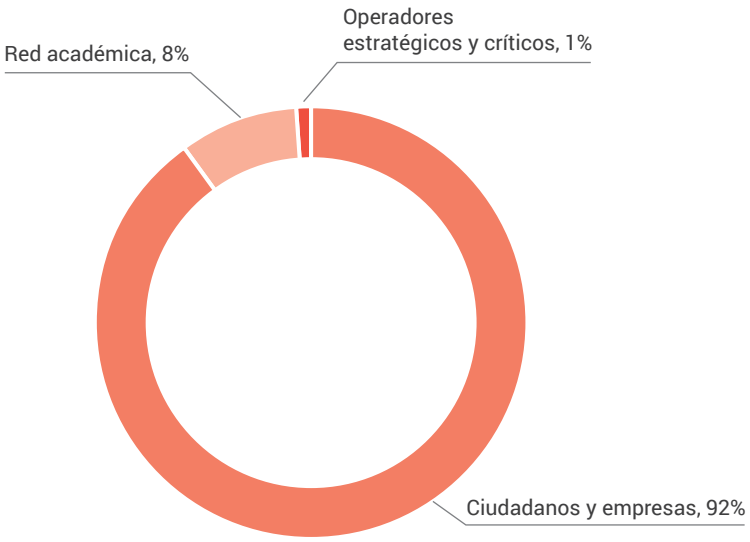
4 U.S. Securities and Exchange Commission https://www.sec.gov/spotlight/cybersecurity

Los datos del INCIBE[5] muestran que los principales objetivos de los ciberataques en 2018 fueron ciudadanos y empresas, con **un total de 102.414 incidentes reseñados**.

Entre las pymes, los ataques más comunes fueron de *ransomware*, secuestro de sistemas, fugas de información y ciberestafas; y en ciudadanos, técnicas de engaño como el *phishing* y los virus informáticos capaces de adentrarse en los dispositivos que no están actualizados o protegidos adecuadamente (*troyanos, gusanos, malware, phishing,* etc.)

**Gráfico 3**

¿Contra quién van dirigidos los ataques?




Fuente: Instituto Nacional de Ciberseguridad (INCIBE).

## Impacto económico

### Un golpe destructivo para las empresas más pequeñas

Conocer con exactitud las pérdidas del sector privado derivadas de este tipo de incidentes no es tarea fácil. Hasta 2016, las empresas no estaban obligadas a hacer públicos estos datos y la mayoría no lo hacía por una cuestión reputacional. Esto ha cambiado con la implantación de la directiva europea sobre Seguridad de Redes y de Información (NIS), que obliga a las empresas a comunicar cuándo son víctimas de un ciberataque.

5 INCIBE: Instituto Nacional de Ciberseguridad.

El último informe realizado por el Centro de Estudios Estratégicos e Internacionales (CSIS) y la compañía de software especializada en seguridad McAfee[6] cifra en **600.000 millones de dólares las pérdidas ocasionadas por los ciberataques** a las empresas (grandes, medianas y pequeñas) en los últimos cinco años, exactamente **el 0,8% del PIB global**. Son 155.000 millones de dólares más que en 2014, lo cual hace del cibercrimen un negocio muy lucrativo.

Según el Instituto Nacional de Ciberseguridad (INCIBE), en España en 2016 el coste medio de un ciberataque rondó los 75.000 euros, lo que supuso unos 14.000 millones de euros de pérdida para todo el tejido empresarial del país, desde las empresas más grandes hasta las más pequeñas.

**El 43%** de esos ciberataques va dirigido específicamente a pequeñas empresas y sus efectos son devastadores, pues un ciberataque suele costarle a una pyme unos 35.000 euros. Esto tiene como consecuencia que el 60% de ellas **desaparezca durante los seis meses siguientes,** en gran medida por no poder afrontar el alto coste que implica el ciberataque[7].

Otro aspecto que se ve muy afectado por este tipo de incidentes es la reputación de la empresa y la confianza que trasmite a sus clientes, ya que al ser víctima de un ciberataque proyecta una imagen de vulnerabilidad y baja solvencia tecnológica.

## ¿Cómo afectan a la administración pública?

### En España, el CNI-CERT, Centro Criptológico Nacional, detectó 38.000 incidentes de ciberseguridad

El incremento en el número de ciberataques registrados contra el Estado español no se debe solo a un aumento real de la cifra, sino también a la mayor capacidad para detectarlos. El Centro Nacional de Inteligencia (CNI) registró el año pasado **38.000 incidentes de ciberseguridad**, lo que representa un aumento del 43% respecto a 2017[8]. Aunque la mayoría fueron neutralizados, **102 se consideraron críticos**.

---

6 CSIS & Mcafee: *"Economic Impact of Cybercrime— No Slowing Down"* https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email

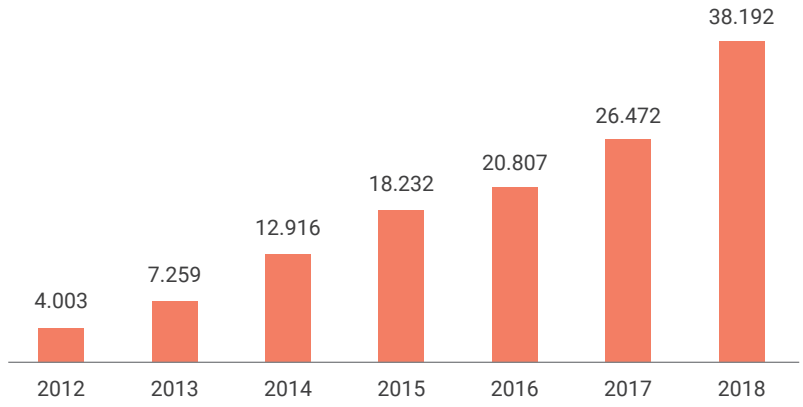
7 Karspersky Lab & Ponemon Institute: *"No hay víctimas pequeñas para los cibercriminales"*. https://www.kaspersky.es/about/press-releases/2017_no-small-victims-for-cybercriminals

8 Departamento de Seguridad Nacional: *"Informe de seguridad nacional 2018"* https://www.dsn.gob.es/es/file/2853/download?token=i8f5aG39

Solo en enero de 2019 se identificaron más de 4.000 incidentes contra objetivos estatales en España.

**Gráfico 4**

¿Cuánto ha aumentado el número de ataques gestionados por el Centro Criptológico Nacional (CCN-CERT) en los últimos siete años?



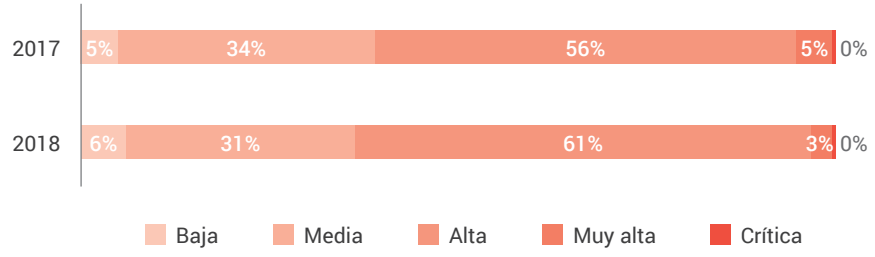

Fuente: Centro Nacional de Inteligencia.

De esos ataques, el 2,7% fue clasificado como de una peligrosidad "muy alta o crítica" según el tipo de amenaza, origen, perfil del usuario o sistemas afectados, entre otros.

El Gobierno español gestiona diariamente una media de **2,8 ciberincidentes con un alto nivel de impacto**.

**Gráfico 5**

¿Cómo se clasifica la peligrosidad de esos incidentes?

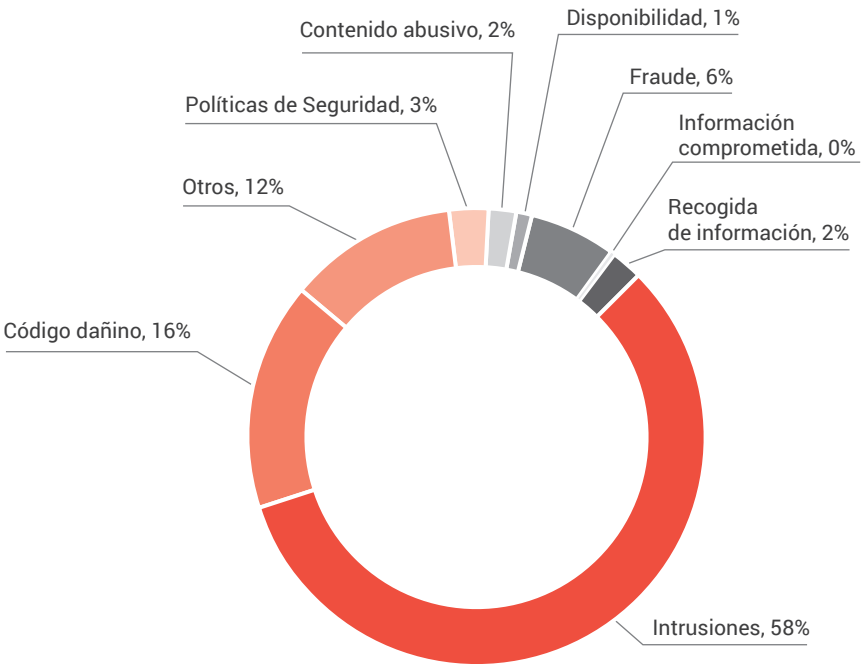



Fuente: Centro Criptológico Nacional.

El 58% de los ciberataques detectados estuvo dirigido a explotar vulnerabilidades e introducirse en los sistemas. También tuvieron una presencia importante las infecciones por código dañino (troyanos, *spyware* o *ransomware*) y las webs modificadas para minar criptomonedas[9].

**Gráfico 6**

¿A qué tipo de incidentes hizo frente el CCN-CERT en 2018?




Fuente: Centro Criptológico Nacional - Computer Emergency Response Team.

Los perfiles de los atacantes son diversos[10]:

- **Países extranjeros:** muchos Estados están invirtiendo en la creación de capacidades de ciberespionaje, ciberguerra o "guerra híbrida" destinadas al sabotaje de procesos críticos para el funcionamiento de un país o a desarrollar operaciones de información e influir en sus sociedades, como explica Marcos Gómez, subdirector de servicios de ciberseguridad del INCIBE.

9 Departamento de Seguridad Nacional: *"Informe de seguridad nacional 2018"* https://www.dsn.gob.es/es/file/2853/download?token=i8f5aG39

10 Centro Criptológico Nacional Computer Emergency Response Team: *"Ciberamenzas y tendencias 2018"* https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2856-ccn-cert-ia-09-18-ciberamenazas-y-tendencias-2018-resumen-ejecutivo-2018/file.html

- **"Ciberdelincuentes":** sus ataques se dirigen a objetivos concretos como escuelas, hospitales, instituciones, grandes empresas o bancos, entre muchos otros.
- **"Ciberterroristas" y "ciberyihadistas":** varias organizaciones terroristas han desarrollado sus propias divisiones informáticas, aunque todavía no parecen ser capaces de desarrollar ciberataques sofisticados.
- **"Hackivistas":** grupos reivindicativos que actúan por razones ideológicas.
- **"Cibervándalos":** simplemente responden al deseo de armar revuelo y suelen ser ciberdelincuentes amateurs y poco cualificados.

> "Las guerras futuras serán en el ciberespacio, ¿para que te vas a complicar en declarar una guerra (física) en el país vecino si le puedes cortar la luz a todo un país o lo puedes dejar incomunicado?"
>
> Eva Cañete, de Unicaja Banco

# ¿Qué es la ciberseguridad?

## Definición

### Una etiqueta que confiere unidad a ámbitos muy diversos

¿Dejarías tu coche con las llaves puestas en un barrio inseguro o la puerta de tu negocio abierta al terminar tu jornada? La respuesta, casi con certeza, es no. Todo el mundo comprende que hacerlo **le expone a ser víctima de un robo** o algo peor. Pero si bien esto está claro en la vida cotidiana, para muchas personas no lo está tanto en el mundo virtual.

Igual que en el campo de la seguridad convencional, la ciberseguridad comprende el manejo de herramientas, prácticas, conceptos y métodos aplicados a la protección de nuestro negocio, nuestras familias y nuestras sociedades en un medio concreto, en este caso **el ciberentorno**.

Los expertos coinciden en que el término "ciberseguridad" concede una entidad propia al sector. "Ha ayudado a darle notoriedad y mayor potencial a este área de trabajo", afirma Eva Cañete.

El auge de algunos fenómenos que incrementan la conectividad como **la nube**[11]**, IoT**[12] **o el 5G**[13] provocan una mayor exposición, multiplican

> "El ámbito de la ciberseguridad es muy amplio y comprende muchas cosas: de los sistemas técnicos que controlan los procesos físicos del mundo real a lo puramente «ciber», como el software que usamos o la nube. Son muchas tecnologías, muchísimos componentes a abarcar"
>
> Rubén Santamarta, Principal Security Consultant de IOActive

11 **Nube o Cloud**: Paradigma que permite a los usuarios ofrecer servicios almacenar información, ficheros y datos en servidores de terceros. Ver más en *Glosario*, al final del informe.

12 **IoT**: Internet of Things o Internet de las cosas: red de objetos físicos que cuentan con una dirección IP y se conectan a internet. También se denomina así a la comunicación que se produce entre estos objetos y otros dispositivos y sistemas habilitados para internet.

13 **5G**: Redes móviles de quinta generación con mayor velocidad de conexión a internet.

las posibilidades de ataques y hacen de la ciberseguridad una disciplina cada vez más necesaria:

- Los entornos industriales están cada vez más conectados y se vuelven más vulnerables. Hay ataques dirigidos, robos de información, pérdida de disponibilidad de los sistemas, sabotajes a los procesos...
- **Internet of Things** (IoT, por sus siglas en inglés): cada vez hay más dispositivos del hogar conectados a internet.
- "El **5G** permite obtener un ancho de banda mayor y con más capacidad. Esta digitalización del entorno (coches, ciudades, domótica[14], etc.) derivará en una mayor exposición... con el consiguiente aumento del riesgo". Juan Carlos Gómez, director global de Ciberinteligencia, Control y Respuesta a Ciberamenazas en Telefónica.

El ***blockchain***[15] y la nube proponen sin duda nuevos retos en ciberseguridad y aspectos tan cruciales como ***Big Data***[16], ***Machine Learning***[17] o la **Inteligencia Artificial**[18] pueden suponer un antes y un después en este campo por las posibilidades que ofrecen en detección y respuestas más automáticas.

## ¿Cómo lo afrontan grandes y pequeñas empresas?

### Las empresas españolas se sitúan por debajo de la media europea en niveles de ciberseguridad

Según la consultora tecnológica estadounidense BitSight[19], las empresas españolas **se sitúan por debajo de la media europea en el ran-**

---

14 **Domótica:** conjunto de tecnologías aplicadas al control y la automatización inteligente de la vivienda. *Asociación Española de Domótica e Imnótica:* http://www.cedom.es/sobre-domotica/que-es-domotica

15 **Blockchain:** Base de datos transaccional distribuida, formada por cadenas de bloques diseñadas para evitar su modificación una vez que un dato ha sido publicado. *Blockchain España*. https://blockchainespana.com/glosario/

16 **Big Data:** análisis de datos masivos. Un ejemplo podrían ser nuestra actividad en las redes sociales, tráfico web, transacciones en tiendas online, sensores en wearables y móviles, datos con geoposicionamiento, datos científicos, financieros, de salud o los de las *smartcities*, etc. Si usas Big Data que sea respetando la privacidad de tus clientes, INCIBE: https://www.incibe.es/protege-tu-empresa/blog/si-usas-bigdata-respeta-privacidad-clientes

17 **Machine Learning:** método de análisis de datos que automatiza la construcción de modelos analíticos. Es una rama de la inteligencia artificial.

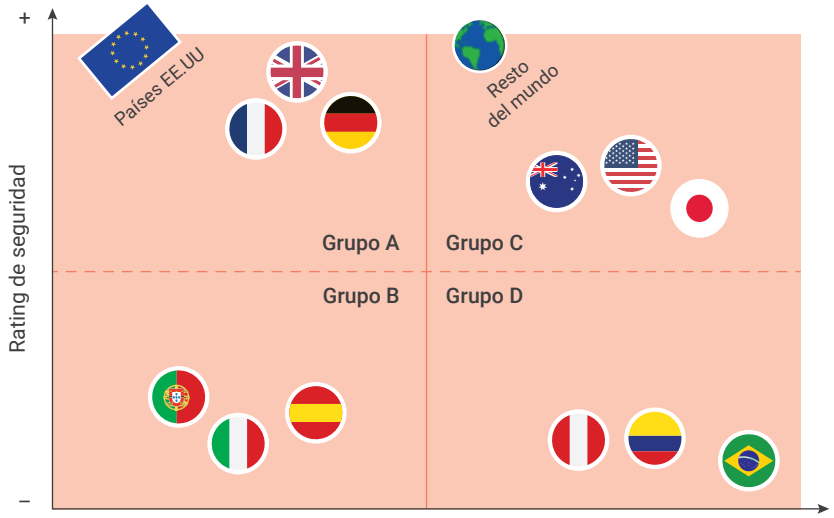
18 **Inteligencia Artificial (IA):** es una rama de la ciencia informática con fuertes raíces en otras áreas como la lógica y las ciencias cognitivas, en la que las máquinas realizan tareas de una mente humana, como aprender o razonar.

19 ElevenPaths en colaboración con Bitsight: *"Estado de la ciberseguridad de las empresas españolas"* https://www.elevenpaths.com/wp-content/uploads/2017/10/estado-de-la-ciberseguridad-de-las-empresas-espanolas.pdf

**king de ciberseguridad**. Países como Francia, Reino Unido y Alemania (grupo A) lideran Europa. De hecho, los países del viejo continente están a la cabeza del rating de seguridad, por encima incluso de Estados Unidos, Australia y Japón (Grupo C).

**Figura 2**

Comparación de rating de seguridad de las empresas españolas con el resto de países




Fuente: ElevenPaths (elaborado por Bitsight).

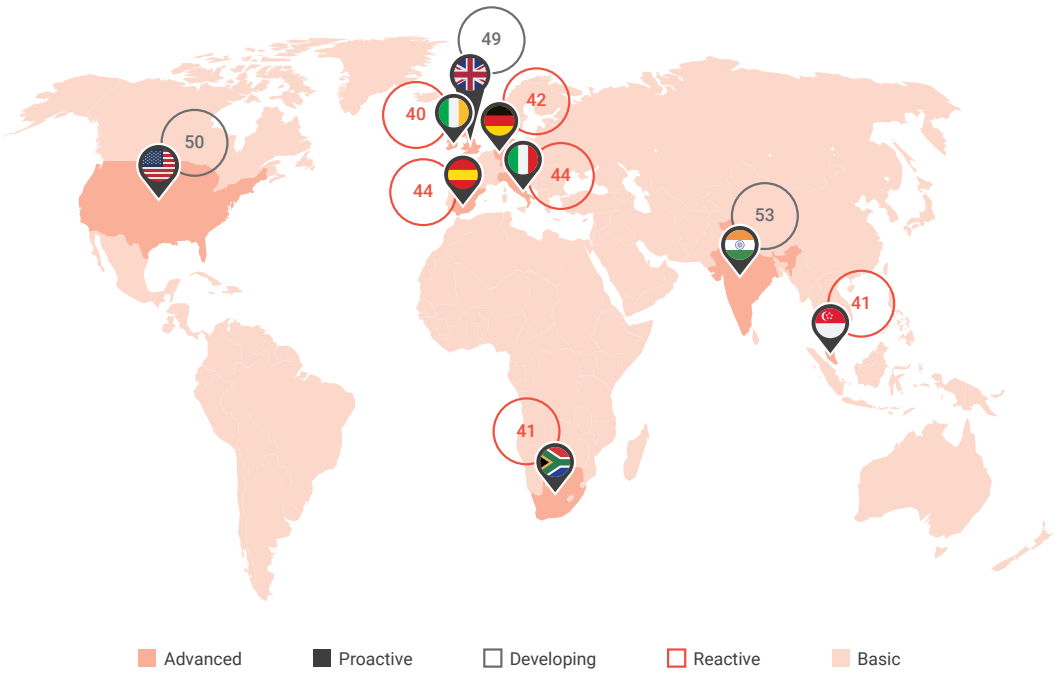
El informe "The Vodafone Cyber Ready Barometer 2018"[20] estimó que España mantiene **una posición "reactiva" en ciberseguridad**. Es decir, sus empresas ejercen "alguna acción" para asegurar su negocio, pero poseen un "margen significativo de mejora" en la materia.

En cuanto a las pymes, no existen estudios que esclarezcan su actuación en materia de ciberseguridad. Para ello hemos realizado una **encuesta a 720 pequeñas y medianas empresas**, que reveló que aunque las pymes ganan en presencia digital y en cierta concienciación en cuanto a la urgencia de la ciberseguridad, eso no se ha traducido necesariamente en un protocolo de actuación desarrollado e implementado a nivel de empresa.

20 Vodafone Group: *"The Vodafone Cyber Ready Barometer 2018"* https://img.en25.com/Web/VodafoneGroupPLC/%7b1dd2abd4-17b9-4e81-9b23-347f2b41f338%7d_Vodafone-Cyber-Ready-Barometer-research-report-2018.pdf

**Figura 3**

España tiene una puntuación de 44 en el *Cyber Ready Index*




Fuente: Vodafone Group.

Principales medidas y acciones por parte de las pymes en materia de ciberseguridad, según las empresas encuestadas:

- **Sistema de verificación en 2 pasos:** un 36% tiene establecida esta medida en su correo electrónico.
- **Protocolo https:** el 71% lo implementa en su web y más del 80% en e-commerce
- **Actualización de dispositivos:** el 85% de las empresas lleva un control de actualización de los sistemas operativos.
- **Cambio de contraseñas:** el 58% cambia sus contraseñas cada 3 meses o con mayor periodicidad.
- **Certificado SSL (e-commerce):** alrededor del 57% lo emplea.
- **Doble factor de autenticación en el pago (e-commerce):** casi el 53% lo implementa.

2 de cada 5 pymes atribuye **un elevado nivel de importancia** a la ciberseguridad.

*Los resultados generales de esta encuesta aparecen más desarrollados en el capítulo "Perspectiva de las pymes".*

El concepto de ciberseguridad entre las pymes se vincula mayoritariamente a **protección o reacción ante ataques** si bien la mayoría no es consciente de haberlos sufrido.

## Leyes e instituciones: así lo gestiona la administración

### La ciberseguridad: una prioridad relevante para las autoridades políticas

Los principales partidos políticos españoles dejaron constancia en los últimos comicios[21] de **su preocupación por la ciberseguridad.**

En su programa electoral, el Partido Socialista Obrero Español (PSOE) proponía campañas de concienciación para la ciudadanía, reforzar los mecanismos de protección de menores en la red e impulsar la creación de programas de formación, sensibilización y concienciación para menores, padres, madres y educadores. En concreto, el PSOE sugería la necesidad de desarrollar programas de ciberseguridad que incrementen la confiabilidad en las redes y plataformas, con especial incidencia en la prevención de cara a la ciudadanía y las empresas.

Por su parte, el Partido Popular (PP) incluía la ciberseguridad dentro de su Plan Nacional de Transformación Digital 2030, y añadía en su programa electoral la elaboración de planes, por parte de los centros educativos, para la formación de los escolares en ciberseguridad. Además, apostaba por la creación de una reserva estratégica de Talento en Ciberseguridad formada por reservistas voluntarios que actúen en apoyo de las necesidades dentro del ámbito específico de la ciberdefensa.

Entre las demás formaciones políticas, Ciudadanos proponía reforzar la ciberdefensa del sector público y las pymes, incrementando a la vez los recursos para consolidar los medios de ciberdefensa y ciberseguridad tanto en el sector público como en el privado y, en especial, en las pymes. Unidas Podemos insistió en la importancia de introducir programas de alfabetización mediática y de ciberseguridad en todas las fases del sistema educativo.

No obstante, las cifras de inversión en ciberseguridad en España están todavía lejos de las de otros países. El PSOE propuso **destinar 185**

21 En mayo de 2019.

**millones al INCIBE**[22] **y CNI** para reforzar la ciberseguridad. En contraste, el presupuesto de EEUU[23] en ciberseguridad es de 1.500 millones de dólares, mientras que el Gobierno británico dedicó 2.300 millones de euros en 2016 a programas de seguridad en internet.

El sistema público español de ciberseguridad descansa fundamentalmente sobre cuatro organismos:

- **CCN-CERT**, el Centro Criptológico Nacional del Centro Nacional de Inteligencia, que se encarga del Sector Público[24].
- **INCIBE-CERT**, el Instituto Nacional de Ciberseguridad de España con un enfoque en los ciudadanos, empresas y operadores de servicios esenciales. El INCIBE prevé aumentar su plantilla en más de un 70% durante los próximos tres años.
- **CNPIC,** el Centro Nacional de Protección de Infraestructuras y Ciberseguridad, que se ocupa de las infraestructuras y operadores críticos, como los proveedores de luz, agua, gas, etc.
- **ESPDEF-CERT,** el Mando Conjunto de Ciberdefensa, que trabaja con las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas.

La coordinación entre estos organismos compone el primer y principal escudo contra los problemas más graves de seguridad.

## Marco legal

### España se sitúa entre los países más avanzados en la materia

Existen varias dificultades al abordar la creación de un marco legal sobre ciberseguridad. En primer lugar, está el hecho de que los ataques son globales, **no vinculados a un país concreto**. Y luego está el anonimato inherente a internet y la **dificultad de identificar el origen del ciberataque**. "Internet es el salvaje oeste: es muy fácil de atacar y

22 Instituto Nacional De Ciberseguridad De España S.A. (INCIBE): *"Presupuestos Generales del Estado Año 2017"* http://www.sepg.pap.hacienda.gob.es/Presup/PGE2017Proyecto/MaestroDocumentos/PGE-ROM/doc/1/6/2/1/2/N_17_A_R_5_1_0N_0_0947_1_PECROOT1_19516.PDF

23 The White House https://www.whitehouse.gov/omb/budget/

24 Ministerio del Interior. *"Guía nacional de notificación y gestión de ciberincidentes"*. http://www.interior.gob.es/documents/10180/9814700/Gu%C3%ADa+Nacional+de+notificaci%C3%B3n+y+gesti%C3%B3n+de+ciberincidentes/f01d9ed6-2e14-4fb0-b585-9b0df20f2906

muy difícil de defender", argumenta David Barroso, *Founder* de CounterCraft.

Los recientes avances legales que buscan establecer una estrategia efectiva de ciberseguridad sitúan a España entre los países más adelantados en la materia:

- **El nuevo reglamento europeo de ciberseguridad** aprobado por el Consejo Europeo en marzo de 2019, consolida una agencia permanente de ciberseguridad así como una certificación común de ciberseguridad para toda la Unión Europea (UE)[25]. Los expertos señalaron este hito como una oportunidad para que España lidere las buenas prácticas en el continente ya que el ecosistema de certificación español se encuentra entre los mejor valorados de Europa.
- **El Real Decreto-ley 12/2018**[26], que transpone al ordenamiento español **la directiva NIS**[27] y busca reforzar la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios digitales, así como establecer un sistema de notificación de incidentes. El desarrollo reglamentario de esta norma está en fase de elaboración
- **La nueva Ley de Protección de Datos (LOPD)**[28], que consagra una serie de "derechos digitales" y garantiza un mínimo de protección frente a las ciberamenazas.
- **La Estrategia Nacional de Ciberseguridad 2019**[29], con la que se pretende garantizar la seguridad, las infraestructuras y la tecnología que integran el ciberespacio, puesto que su vulneración es una de las principales amenazas para la Seguridad Nacional.

> "La normativa NIS por primera vez nos beneficia porque se exige la notificación de los incidentes de ciberseguridad, y eso nos puede ayudar a tener una base de datos, a tipificar incidentes y al final contribuye a **tomar la temperatura del nivel de riesgo** que tienen las empresas"
>
> Eva Cañete, de Unicaja Banco

25 Consejo Europeo Consejo de la Unión Europea: *"Una Unión que resiste mejor ante los ciberataques: El Consejo confirma un acuerdo sobre la certificación común y sobre una agencia reforzada"* https://www.consilium.europa.eu/es/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

26 Agencia Estatal Boletín Oficial del Estado: *"Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información."* https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

27 Directiva NIS: es una normativa de la Unión Europea que busca mejorar la seguridad de las redes y los sistemas de información en su territorio. Entró en vigor en agosto de 2017. EUR-Lex: *"Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016"* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148

28 Boletín Oficial de las Cortes Generales. Senado: *"Proyecto de Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. (621/000012)"* http://www.senado.es/legis12/publicaciones/pdf/senado/bocg/BOCG_D_12_289_2209.PDF

29 Presidencia del Gobierno: *"Estrategia de Ciberseguridad Nacional 2019"* https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-6347

- **La Comisión Mixta de Seguridad Nacional Congreso-Senado** trabaja en un informe en el que propone modificar el Código Penal para imponer penas más duras a los delitos cometidos por ciberdelincuentes y aboga, además, por una regulación de carácter internacional.[30]

# Retos para las empresas en materia de ciberseguridad

## La concienciación es el reto principal en todos los ámbitos

Imagina la siguiente escena: llegas a tu empresa y encuentras una memoria USB en el suelo del aparcamiento o el ascensor. La recoges y al llegar a tu puesto de trabajo la pones en tu ordenador, para ver si contiene algo que te permita averiguar quién de tus compañeros la ha perdido. No obstante, la memoria contiene un software malicioso diseñado para penetrar equipos como el tuyo. La seguridad de tu lugar de trabajo ha quedado **irrevocablemente comprometida**.

Esta es, de hecho, una de las tácticas más comunes que compañías o actores poco escrupulosos utilizan para penetrar los sistemas de seguridad de competidores o rivales. Por ello, en el ámbito empresarial y de la administración, **la concienciación es sin duda el reto principal** en todos los ámbitos, seguido del necesario **incremento de la formación, la inversión y los recursos** dedicados a temas de ciberseguridad.

En España, tanto en las empresas como en la Administración Pública, existe una **sensibilización** creciente hacia la ciberseguridad, pero hay un amplio margen de mejora.

En las grandes empresas, la ciberseguridad es una cuestión que no ha de ser relegada al departamento de informática. Ha pasado de ser un tema tecnológico a un tema de gestión de riesgos. Tanto las grandes empresas como las más pequeñas deben **ser conscientes** de que estos ataques pueden paralizar una compañía o incluso hacerla desaparecer.

Entre las pymes, existe una **baja percepción del problema** y estas tienden a autoexcluirse como potencial objetivo de ciberataques. Esta es

30 Centro Criptológico Nacional Computer Emergency Response Team: "*Los partidos apuestan por reformar el Código Penal para reforzar la ciberseguridad*". https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/7701-los-partidos-apuestan-por-reformar-el-codigo-penal-para-reforzar-la-ciberseguridad.html

una cuestión preocupante, ya que suponen el grueso del tejido empresarial español. Un hipotético ataque masivo al tejido de las pymes generaría **un grave impacto económico** ya que su capacidad de resiliencia (de recuperación tras un ataque) es mucho menor que la de las grandes empresas, debido a una menor potencia económica en general y a una menor capacidad de respuesta en términos de ciberseguridad.

Para la administración pública el tema puede escalar a **asuntos críticos de seguridad nacional**.

Los expertos se muestran de acuerdo en que una mayor toma de conciencia sobre la importancia de la ciberseguridad no ha implicado hasta el momento una implementación rigurosa de acciones en pro de la seguridad ni una mayor defensa de los ciberderechos.

Aunque se ha avanzado de forma notable en muchos aspectos, todavía existen **indicadores susceptibles de mejoras**, que implican importantes transformaciones, diversificación y especialización en el mercado laboral.

## Mercado laboral

### Se necesitan más profesionales del sector: el 40% de las empresas tiene dificultades para encontrar a especialistas tecnológicos

Dos tercios de las empresas españolas a día de hoy **no cuentan con suficientes empleados** para combatir las ciberamenazas.

> "A las empresas les cuesta mucho **encontrar profesionales de ciberseguridad.** Y no es una cosa particular de España: pasa lo mismo en el resto de los países. En muchos se están aumentando las capacidades para dar formación en colegios y en universidades y formar talento"
>
> Juan Carlos Gómez, director global de Ciberinteligencia, Control y Respuesta a Ciberamenazas de Telefónica

## Oferta formativa

### Son imprescindibles una mayor especialización y una actualización constante

España posee una amplia oferta de másteres y cursos en el ámbito de la ciberseguridad[31], y el Gobierno está preparando un sistema integral de formación profesional (FP) que incluiría disciplinas como ciberseguridad, robótica, big data, análisis de datos, fabricación 3D, realidad virtual, realidad ampliada, etc.[32]

---

31 INICIBE https://www.incibe.es/catalogos-formacion-ciberseguridad

32 Ministerio de Educación y Formación Profesional: *"Isabel Celaá impulsa la modernización de los estudios de FP 4.0"*. http://www.educacionyfp.gob.es/prensa/actualidad/2019/02/20190228-firmaprotocolos.html

> “Existen másteres muy genéricos que **no dan respuesta a lo que las empresas necesitan,** que suelen ser conocimientos muy específicos. Falta aplicación práctica y realista, conectada con el mundo real... Les enseñan cosas muy teóricas, **falta experiencia práctica.**”
>
> Hugo Teso, experto en ciberseguridad

Los expertos del sector señalan las principales necesidad en este campo:

- **Especialización:** a día de hoy existe mucha más información y también más oferta formativa que hace una década, pero también existen campos mucho más específicos: *research*, respuesta a incidentes, seguridad corporativa o seguridad en móviles.
- **Actualización constante:** derivada de la rápida evolución de la disciplina y la aparición de nuevos tipos de ataques.
- **No solo perfiles técnicos:** es importante formar también a abogados, sociólogos, periodistas, etc.

## Presencia femenina

### El mercado laboral asociado a la ciberseguridad es tradicionalmente masculino: según un estudio solo el 7% de los profesionales europeos de ese campo son mujeres

Los principales obstáculos para el acceso de las mujeres a este sector son la **falta de referentes**, la **baja presencia de mujeres en carreras STEM** (Science, Technology, Engineering y Mathematics), el desconocimiento genérico de la existencia de la ciberseguridad o la creencia de que es un ámbito exclusivamente técnico[33].

Un informe de Kaspersky Lab[34], que analiza los motivos que impiden el acceso de las mujeres al campo de la ciberseguridad afirma que:

> El 69% de las jóvenes nunca ha conocido a alguien que trabaje en ciberseguridad y menos aún (11%) a otra mujer, lo que se traduce en falta de referentes femeninos.
>
> El 45% de las encuestadas desconoce la existencia de las carreras de ciberseguridad.

No obstante, y acorde al ritmo de los tiempos, algo va cambiando: según **ISC2**[35], en 2017 apenas el 11% de los profesionales dedicados

> “Cuando hablamos de los distintos perfiles de ciberseguridad queremos decir que necesitamos **perfiles de todo tipo:** no solo los más técnicos, que sean capaces de hacer análisis forenses, como explotar las vulnerabilidades técnicas, que sepan hacer un test de intrusión, que sepan parchear, etc., sino también licenciados en derecho, que sepan cual es el marco regulatorio, qué se puede hacer y qué no; sociólogos, perfiles que sepan cómo transmitir esos mensajes que ayuden a la concienciación; expertos en comunicación que sepan trasladar el mensaje a la alta dirección...”
>
> Elena Matilla, de Red Eléctrica

33 Kaspersky Lab: *“Estudio sobre los motivos que impiden el acceso de las mujeres al campo de la ciberseguridad”.* https://media.kasperskydaily.com/wp-content/uploads/sites/88/2017/12/01113427/KAS0162-Kaspersky-Following-whose-lead-report-ES.pdf

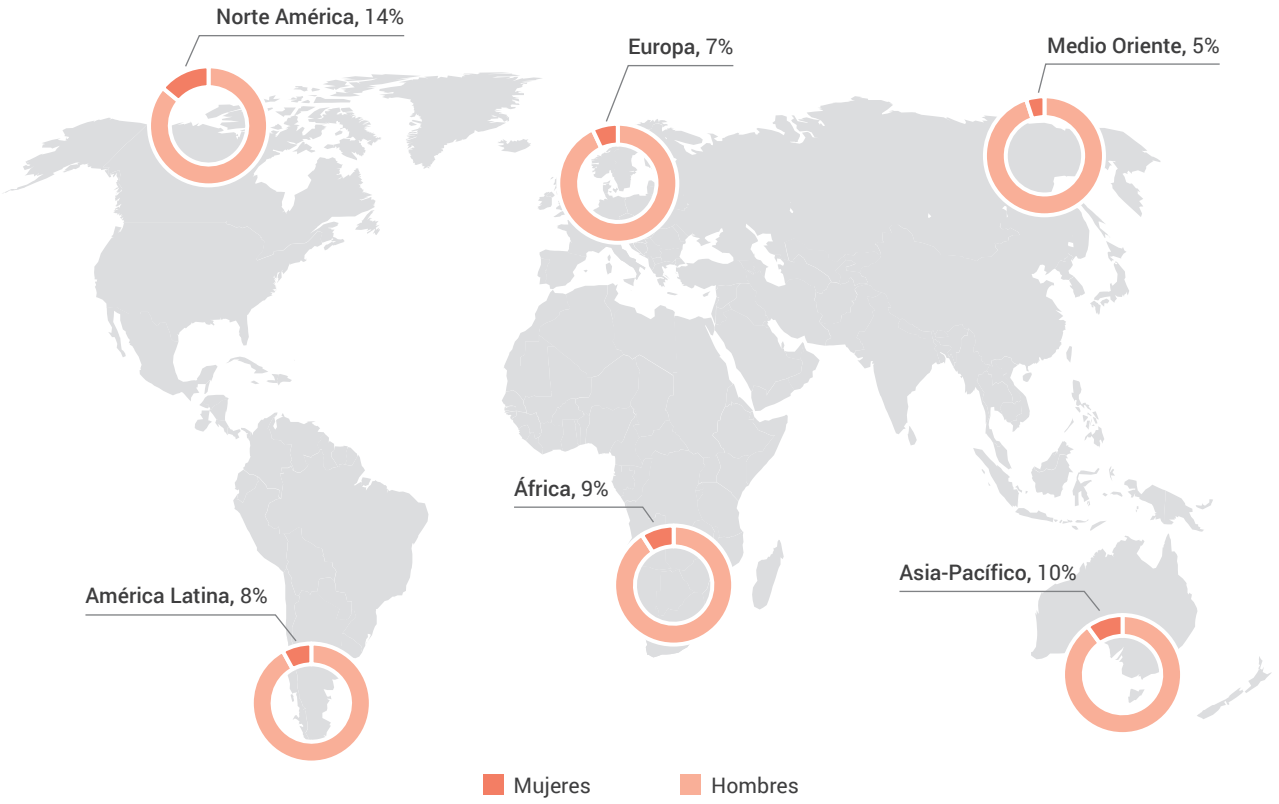
34 Ídem.

35 ISC2: El Consorcio Internacional de Certificación de Seguridad del Sistema de Información (ISC)², es una organización sin fines de lucro que se especializa en capacitación y certificaciones para profesionales de la ciberseguridad. An ISC2 Cybersecurity Workforce Report “Women in Cybersecurity” https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=270117229EA39FA1E7134CFB1C5BB1ACBDF8A88C

a la ciberseguridad en Europa eran mujeres, mientras que en 2019 ese número ha aumentado al 24%. Sin embargo, la consultora Frost & Sullivan da una cifra aún menor, del 7% en 2017[36]

**Figura 4**

Porcentaje de hombres y mujeres que trabajan en ciberseguridad, por regiones




Fuente: Frost & Sullivan.

En España ha habido **diferentes iniciativas** destinadas a promover la presencia de mujeres en materias científicas y tecnológicas *(Power to Code, Geek & Tech, WomenTeck, Girls in Tech*) y también algunas específicas sobre ciberseguridad, como *Mujeres Tech, Girls in ICT Day* o *Women4Cyber.*

36 Frost & Sullivan: *"The 2017 Global Information Security Workforce Study: Women in Cybersecurity"*. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2019/01/women-cybersecurity-11-percent.pdf

**Mujeres Tech:** es una iniciativa co-desarrollada por Cristina Aranda, que promueve la presencia femenina en el sector digital. Uno de los objetivos que persigue la asociación es impulsar la presencia de mujeres expertas en ciberseguridad y hacer que la tecnología tenga un impacto positivo en las empresas y en la sociedad.

**Women4Cyber:** es una iniciativa impulsada desde la Organización Europea de Ciberseguridad (ECSO), que nace con el objetivo de visibilizar las acciones y logros de las mujeres en materia de ciberseguridad, además de reforzar la participación femenina en este campo en el futuro.

# Un mundo de oportunidades

## Un campo con un enorme potencial

Aunque existen importantes retos y necesidades por cubrir, este sector en pleno desarrollo ya ofrece cuantiosas oportunidades, que no harán más que aumentar a medida que se vayan afianzando las políticas y normas de ciberseguridad en el ámbito empresarial y administrativo español.

Además de proteger nuestras operaciones comerciales, procesos, transacciones, datos, servicios y comunicaciones, el desarrollo de este sector tiene grandes potencialidades en el **mercado laboral y económico**.

## Auge del sector

### Oportunidades de la ciberseguridad: inversión y talento

Existe un aumento generalizado de la inversión en ciberseguridad en las empresas y la previsión es que se mantenga al alza. La consultora tecnológica Gartner estima que la facturación global del sector pasará de los 153.000 millones de dólares en 2018 a los **248.000 millones en 2023**. Un aumento nada menos que del 62%[37].

37 Gartner: *"Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019"* https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

## Gráfico 7

¿Cuánto se ha gastado en el mundo en ciberseguridad en los últimos tres años?

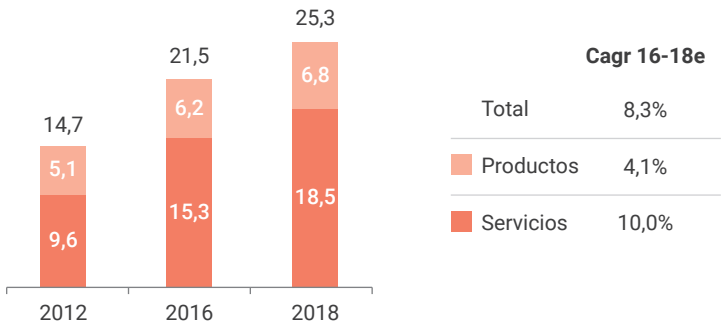
| Segmento de mercado | 2017 | 2018 | 2019 |
|---|---|---|---|
| Servicios de seguridad | 52,315 | 58,92 | 64,237 |
| Protección de la infraestructura | 12,583 | 14,106 | 15,337 |
| Equipo de seguridad de red | 10,911 | 12,427 | 13,321 |
| Gestion de acceso de la identidad | 8,823 | 9,768 | 10,578 |
| Software de seguridad para el consumidor | 5,948 | 6,395 | 6,661 |
| Gestión integrada de riesgos | 3,949 | 4,347 | 4,712 |
| Seguridad de datos | 2,563 | 3,063 | 3,524 |
| Seguridad de aplicaciones | 2,434 | 2,742 | 3,003 |
| Otro software de seguridad de la información | 1,832 | 2,079 | 2,285 |
| Seguridad en la nube | 185 | 304 | 459 |
| **Total** | **101,544** | **114,152** | **124,116** |

Fuente: Gartner.

En Europa, el gasto asociado a la inversión en el sector está en esa misma línea, como se puede ver en el siguiente gráfico del informe "Cyber security: European emerging market leaders" de la consultora Price Waterhouse Cooper (PWC).[38]

## Gráfico 8

Gasto estimado en ciberseguridad en Europa Oriental
(en miles de millones)




Fuente: PWC.

38 PWC: *"Cyber security: European emerging market leaders"* https://www.pwc.co.uk/deals/assets/cyber-security-european-emerging-market-leaders.pdf

Como subraya el estudio "The Vodafone Cyber Ready Barometer 2018"[39], el 84% de las empresas españolas (de más de 10 empleados) aumentará su inversión en ciberseguridad en los próximos tres años y dedicará a ello un mínimo del **10% de su presupuesto informático**.

## Mercado laboral

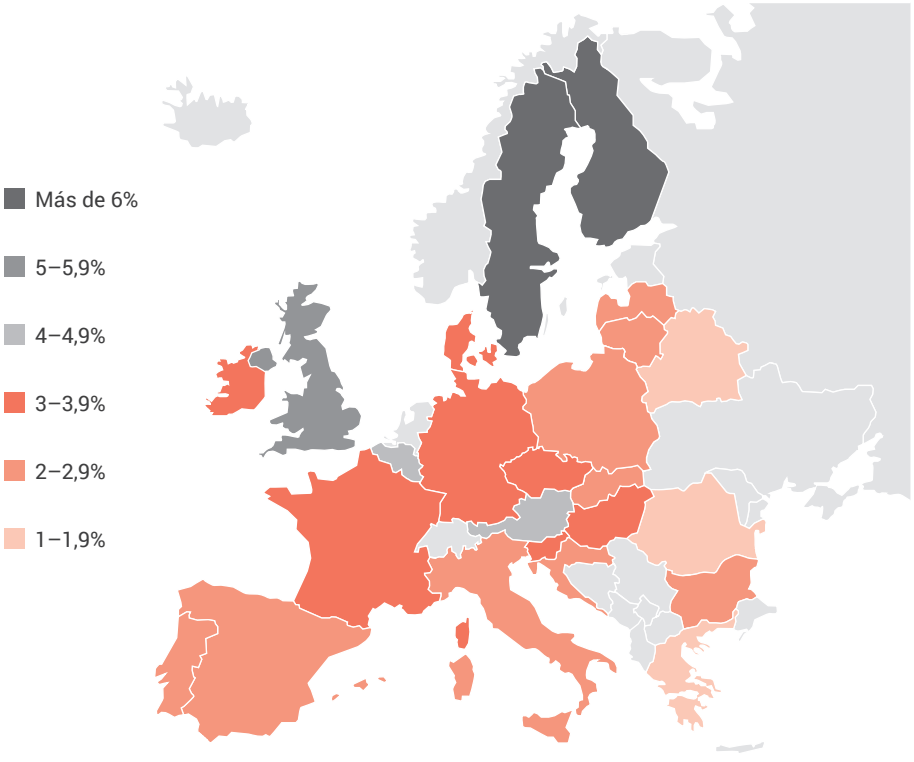
### Nuevas oportunidades de empleo: la ciberseguridad puede ser una esperanza laboral para muchos jóvenes

Este sector tiene la potencialidad de convertirse en un nuevo motor económico y en una amplia fuente de empleos para un gran número de profesionales recién formados.

> "La ciberseguridad en España puede ser un sector que nos saque del turismo y los servicios y también puede suponer **una esperanza para muchos jóvenes** que pueden tener una oportunidad laboral que en otro ámbito no va a aparecer"
>
> Rubén Santamarta, Principal Security Consultant en IOActive

**Figura 5**

¿Qué porcentaje de especialistas en tecnologías de información y comunicación hay en Europa?




Fuente: Elaboración del DSN con datos de la Comisión Europea (Digital Single Market).

39 Vodafone Group: *"The Vodafone Cyber Ready Barometer 2018"* https://img.en25.com/Web/VodafoneGroupPLC/%7b1dd2abd4-17b9-4e81-9b23-347f2b41f338%7d_Vodafone-Cyber-Ready-Barometer-research-report-2018.pdf

Según el estudio "2017 Global Information Security Workforce Study", elaborado por el Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC), el mercado europeo cuenta con una tasa de desempleo en ciberseguridad del 1%. Virtualmente, **«desempleo cero»**[40].

El informe anual del portal InfoJobs 2017 [41] constata que **el 47% de las empresas españolas con más de 50 empleados tiene previsto contratar profesionales del entorno TIC**, especialmente *ethical hackers*, expertos en ciberseguridad y *data scientists*.

Según este informe el sector de Informática y Telecomunicaciones ocupa, un año más, la primera posición en el ranking de empleabilidad, con un **salario bruto promedio de 32.640** euros anuales (aproximadamente 6.000 euros por encima del salario medio en España).

### Gráfico 9

¿Cómo aumentará la cifra de profesionales en los distintos roles del sector?[42]


Fuente: KPMG

40 Frost & Sullivan: *"2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk"* https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2019/01/women-cybersecurity-11-percent.pdf

41 Infojobs: *"Estado del Mercado Laboral en España"* https://nosotros.infojobs.net/wp-content/uploads/2018/05/Informe-Anual-InfoJobs-ESADE-2017-Completo.pdf

42 KPMG: "Disrupción y crecimiento" https://assets.kpmg/content/dam/kpmg/es/pdf/2017/06/ceo-outlook-2017-espana.pdf

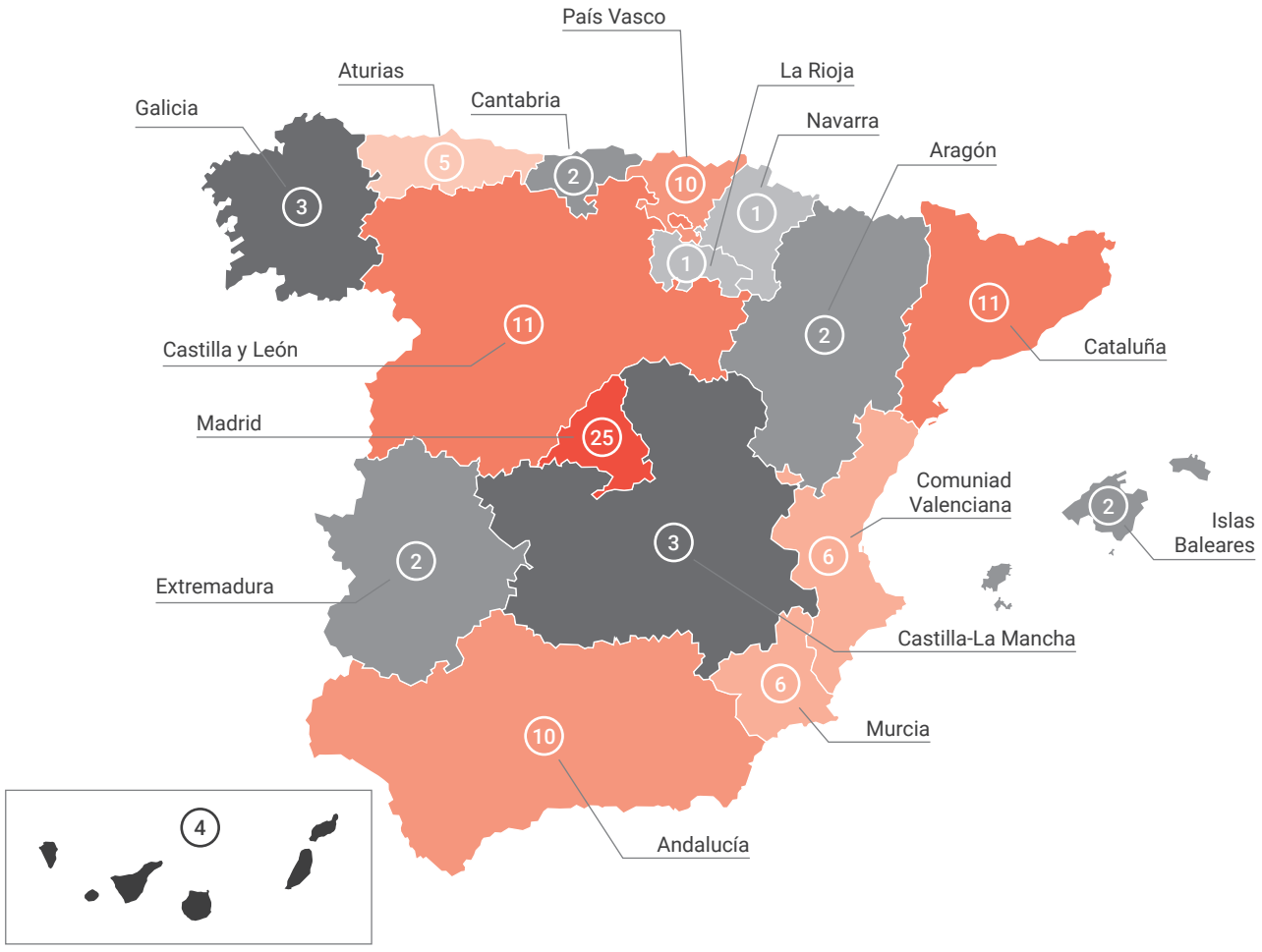
## Centros de investigación

### La investigación juega un papel crucial para el presente y el futuro

A partir de los retos que plantea la ciberseguridad, se ha incrementado el número de centros de investigación y profesionales que van adquiriendo mayor especialización. En España existen a día de hoy **104 equipos de investigación en ciberseguridad** distribuidos por todo el país. La Comunidad de Madrid aglutina el mayor número.[43]

**Figura 6**

¿Cuántos equipos de investigación en ciberseguridad hay en España?




Fuente: INCIBE.

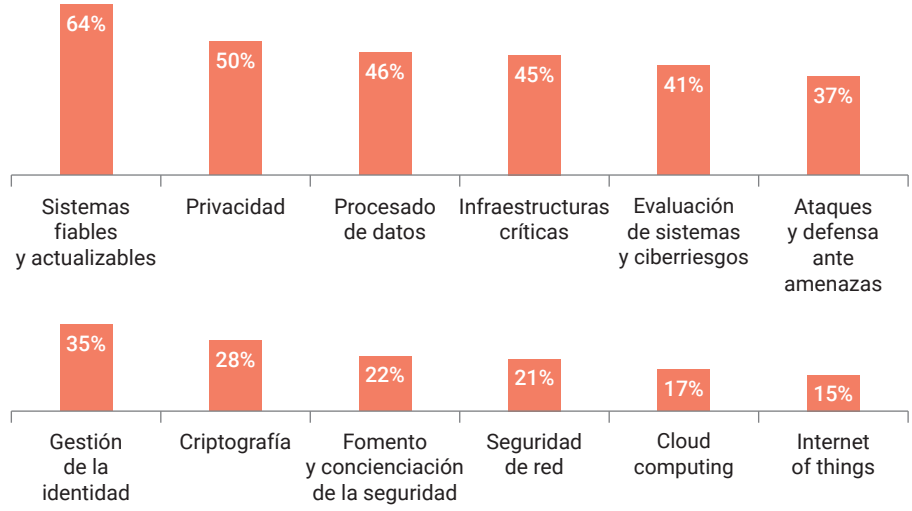
43 INCIBE: *"Catálogo y Mapa de Conocimiento de la I+D+i en ciberseguridad"* https://www.incibe.es/sites/default/files/paginas/red-excelencia/estudios-caracterizacion/201701_catalogo_infografia.pdf

Los principales agentes investigadores son las universidades (94), si bien existen también nueve centros tecnológicos centrados en la investigación de la ciberseguridad con 1.302 profesionales y un centro de investigación especializado.

Estos centros enfocan la investigación alrededor de temas como "Sistemas fiables y actualizables", "Privacidad", "Procesado de datos" e "Infraestructuras críticas".

**Gráfico 10**

¿Qué se investiga?




Fuente: INCIBE.

# PERSPECTIVA DE LAS PYMES

## Estar en internet, una necesidad empresarial

En pleno siglo XXI, prácticamente toda empresa posee **una dimensión digital**. El caso más evidente es el de aquellas firmas que solo operan en internet, mediante la venta online y las herramientas de comunicación virtual con el cliente, pero incluso en el otro extremo, el de los negocios más tradicionales, su gestión diaria depende de elementos como el correo electrónico y los programas de contabilidad. La mayoría de las pymes y grandes empresas se sitúa en un punto intermedio, con una página web con información comercial y datos de contacto y la oferta de **al menos una parte de sus servicios a través de internet.**

Para tener una aproximación representativa de la perspectiva de las pymes españolas en materia de ciberseguridad se realizaron una serie de entrevistas telefónicas que pueden dividirse en muestras de dimensionamiento y de profundización. En este apartado se recogen los resultados de dichas encuestas.

**Dimensionamiento:** 400 entrevistas telefónicas a pymes representativas teniendo en cuenta todos los tamaños de empresa —número de empleados— y el sector de actividad.

**Profundización:** centrado en pymes con más de 3 asalariados (ya que en empresas pequeñas es más complejo alcanzar cierto nivel de profundización) con una muestra 320 entrevistas telefónicas.

# Presencia digital

## Las pymes ganan presencia en el campo digital

Las formas más extendidas de presencia digital entre las pymes son:

- **Mail corporativo** (7 de cada 10 cuentan con una cuenta de correo específica para empleados de la empresa).
- **Página web corporativa** (62%).
- Presencia en **redes sociales** de algún tipo (53%).

Aspectos como programas de gestión de clientes, venta online (e-commerce) o apps para dispositivos móviles son todavía minoritarias.

**Gráfico 11**

¿Qué presencia digital tienen las empresas encuestadas?


Base total: 720

Fuente: The Cocktail Analysis.

# Nivel de seguridad

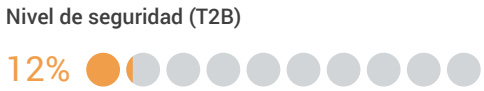
## Los responsables de informática atribuyen un nivel "bajo" de seguridad a sus empresas

Destaca el escaso nivel de seguridad atribuido por los responsables de informática a sus propias empresas. Solo un 12% valora este nivel como "muy seguro".

El concepto de ciberseguridad entre las pymes se vincula mayoritariamente a **protección o reacción ante ataques**. La mitad de las empresas lo asocia espontáneamente a "actuaciones de seguridad frente a terceros (como los virus, los hackers, etc.)".

## Gráfico 12

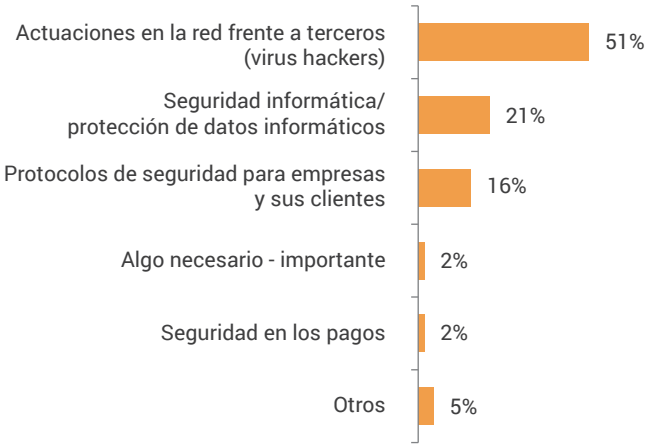
¿Cual es el nivel de ciberseguridad atribuida a la empresa por los responsables de informática?




Base dimensionamiento: 400
Fuente: The Cocktail Analysis.

## Gráfico 13

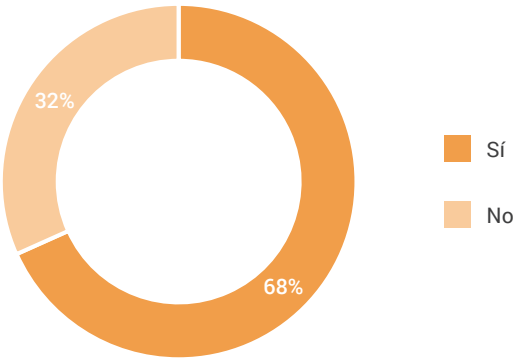
¿Cómo perciben las empresas el concepto de ciberseguridad?




Base dimensionamiento: 400
Fuente: The Cocktail Analysis.

## Gráfico 14

¿Conoce lo que significa ciberseguridad?



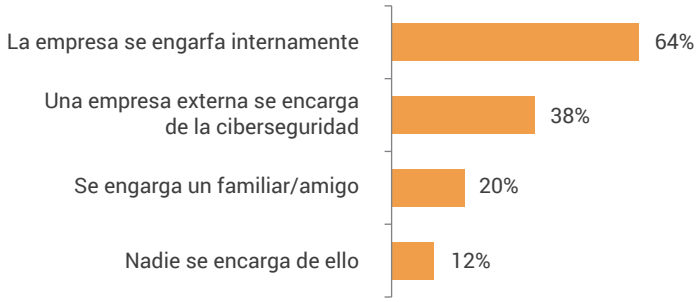

Base dimensionamiento: 400
Fuente: The Cocktail Analysis.

**3 de cada 10 responsables** de informática de las pymes confiesan no conocer el concepto de ciberseguridad.

No es común que las pymes externalicen su desempeño en ciberseguridad. El 64% de las pymes encuestadas **se encarga de su propia ciberseguridad**.

### Gráfico 15

¿Quién gestiona la ciberseguridad de la empresa?




Base dimensionamiento: 400
Fuente: The Cocktail Analysis.

En la mayoría de los casos no parece haber una persona con un rol específico de responsable de ciberseguridad de la empresa. En un 68% de las ocasiones el propio responsable de ciberseguridad es también **el responsable de la gestión de la empresa.**

### Gráfico 16

¿Quiénes responden por la ciberseguridad en las empresas encuestadas?


Base dimensionamiento: 400
Base la empresa se encarga internamente: 257
Fuente: The Cocktail Analysis

La mayor parte de las pymes encuestadas (67%) no dispone de un protocolo específico o normas sobre medidas de seguridad. De estas medidas, las más habituales son **el antivirus (91%) y las copias de seguridad (85%)**. Luego estarían el *firewall* o cortafuegos y la protección de las redes inalámbricas wifi.

Por otra parte, la contratación de un seguro contra riesgos cibernéticos es todavía muy minoritaria entre las pymes españolas, con solo un 12% de las empresas encuestadas que poseen una póliza contratada.

# Ciberataques en pymes

## El porcentaje de pymes que son conscientes de haber sufrido un ataque es residual

Solo un 17% de las pequeñas y medianas empresas declara haber sufrido alguna vez algún ciberataque. La inhabilitación de dispositivos a causa de un virus y el *malware* son **los ataques más comunes.**

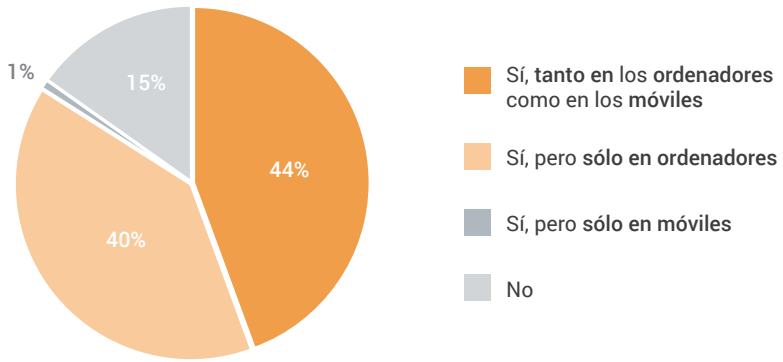
## Medidas adoptadas

### 1. Actualización de dispositivos

El 85% de las empresas lleva un control de actualización de los sistemas operativos de los dispositivos, aunque casi la mitad lo hace **solo en ordenadores**.

**Gráfico 17**

¿Controlan las empresas la actualización de los sistemas operativos?




Base empresas con más de 3 empleados: 396
Fuente: The Cocktail Analysis

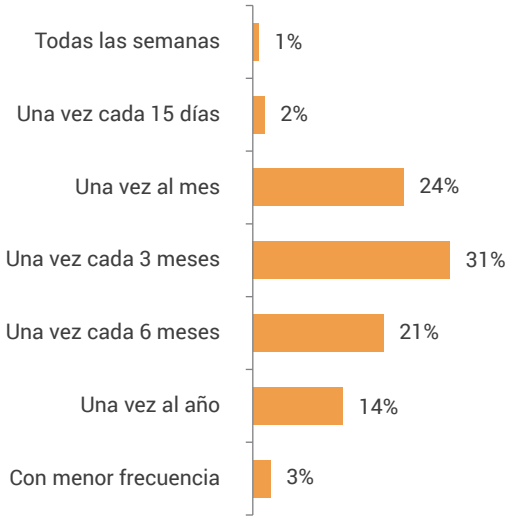
## 2. Cambio de contraseñas

Poco más de la mitad de las pymes (58%) **cambia sus contraseñas cada 3 meses** o con una periodicidad mayor

El 49% de las pymes encuestadas no dispone de normas que exigen la actualización de contraseñas cada cierto tiempo.

**Gráfico 18**

¿Con qué frecuencia actualizan sus contraseñas las empresas?

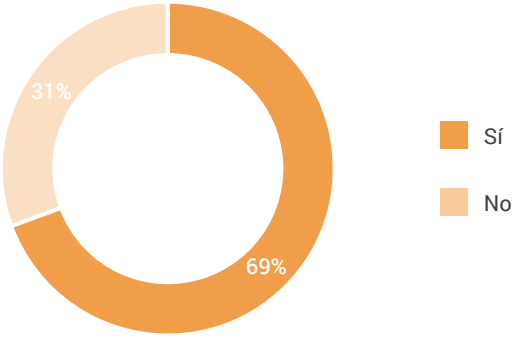



Base tienen un protocolo de actualización de contraseñas: 202
Fuente: The Cocktail Analysis

## 3. 2SV (Sistema de verificación en dos pasos)

**Gráfico 19**

¿Conoce el sistema de verificación en dos pasos?




Base empresas con más de 3 empleados: 396
Fuente: The Cocktail Analysis

El conocimiento del sistema de 2SV (verificación en 2 pasos) muestra **niveles muy positivos:** un 69% de los responsables de pymes con empresas de más de 3 empleados reconoce este sistema cuando se les presenta. Sin embargo, solo un 36% tiene establecida esta medida en su correo electrónico.

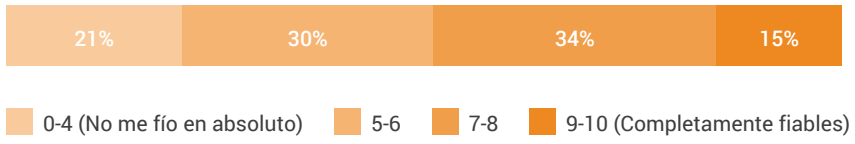
## 4. Almacenamiento en la nube

El almacenamiento en la nube muestra niveles de penetración cada vez más elevados entre las pymes españolas: la mitad afirma que almacena en cloud.

El nivel de fiabilidad atribuido a estos servicios de almacenamiento en la nube también es alto. Prácticamente la mitad de la muestra lo califica **con una puntuación de 7 o más**, en una escala de 0 a 10.

**Gráfico 20**

¿Confían los empleados en los servicios de almacenamiento en la nube/cloud?




Base empresas con más de 3 empleados: 396
Fuente: The Cocktail Analysis

## 5. Cultura de ciberseguridad entre empleados

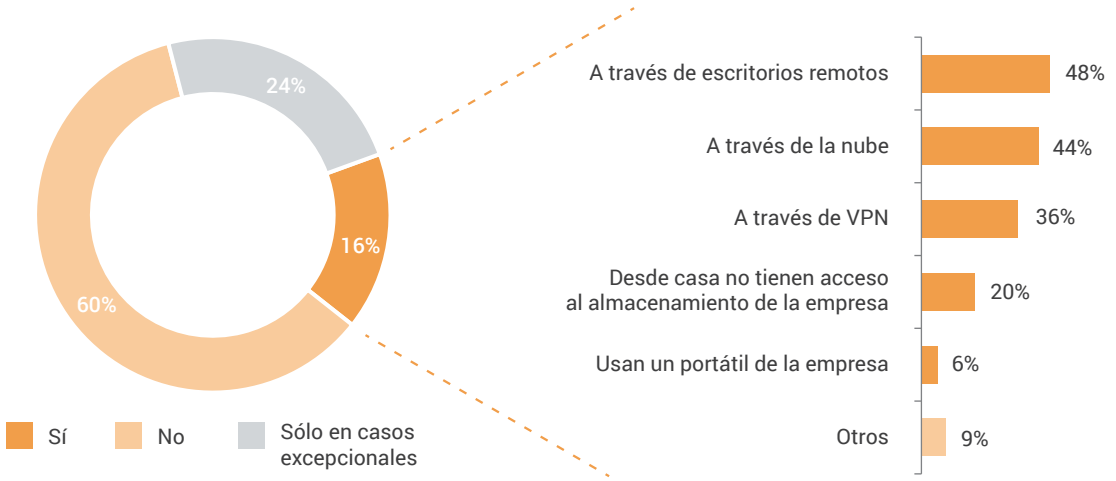
Solo un 30% de los responsables de informática encuestados considera que los empleados están concienciados sobre lo importante que es la ciberseguridad.

Además, **la formación en este campo aparece como minoritaria** en las pymes españolas y solo 6 de cada 10 pymes tienen restringido el acceso a determinada información sensible.

Otro elemento a considerar en materia de ciberseguridad en las empresas es el **teletrabajo**, si bien la posibilidad de trabajar desde otros lugares apenas se considera entre las pymes españolas. En aquellos casos en que existe esta opción, se trabaja principalmente a través de escritorios remotos (48%) y en la nube (44%).

## Gráfico 21

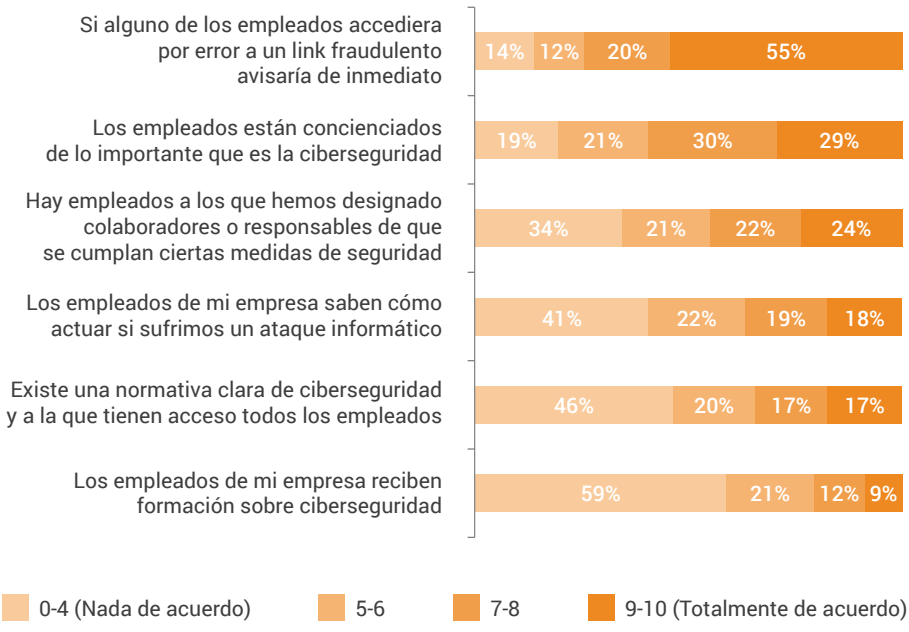
¿Cómo acceden los empleados a distancia a los sistemas de la empresa?




Base se les permite teletrabajar: 64
Fuente: The Cocktail Analysis.

## Gráfico 22

Cultura de ciberseguridad: ¿cómo lo ven los empleados?




Base empresas con más de 3 empleados: 396
Fuente: The Cocktail Analysis.

Sobre el nivel de concienciación y cultura de ciberseguridad en los empleados, se aprecia un amplio margen de mejora. Por ejemplo, según los representantes de las pymes encuestadas, solo el 17% de sus trabajadores sabría **cómo actuar ante un ciberataque**.

El 84% de las pymes no tiene configurado un acceso seguro para aquellos empleados que trabajan con sus dispositivos personales

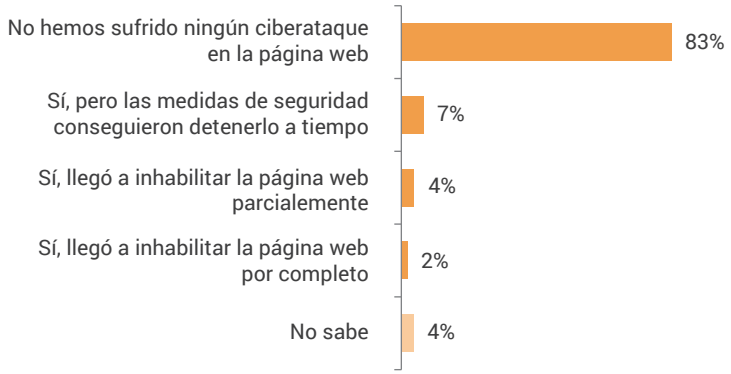
## 6. Medidas de seguridad implementadas en la web

Un 30% de pymes españolas **no tiene implementado el protocolo https** en sus webs y solo un 31% dispone de un programa específico para garantizar la seguridad de su página. De hecho, un tercio de las pymes desconoce si la empresa dispone o no de este programa específico.

Es muy bajo el porcentaje de pymes que es consciente de haber sufrido algún ataque en su página web. Entre las que manifiestan haberlo padecido, la gran mayoría reaccionó y **consiguió frenarlo a tiempo**.

**Gráfico 23**

Ciberataques contra la web de la empresa




Base empresas con más de 3 empleados y página web en la empresa: 302
Fuente: The Cocktail Analysis.

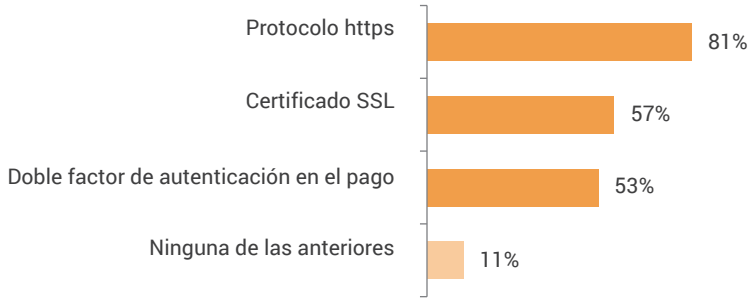
## 7. Medidas de seguridad implementadas en e-commerce

Sobre las medidas de seguridad adoptadas por las empresas en e-commerce, el protocolo https es el más extendido, seguido del certificado SSL y el doble factor de autenticación en el pago.

Al valorar la seguridad que brinda su e-commerce a los clientes, el 71,4% la percibe como "completamente seguro" y solo un 2,9% como "nada seguro", para una media de 8,9 en una escala de 0 a 10.

**Gráfico 24**

Medidas de seguridad en e-commerce



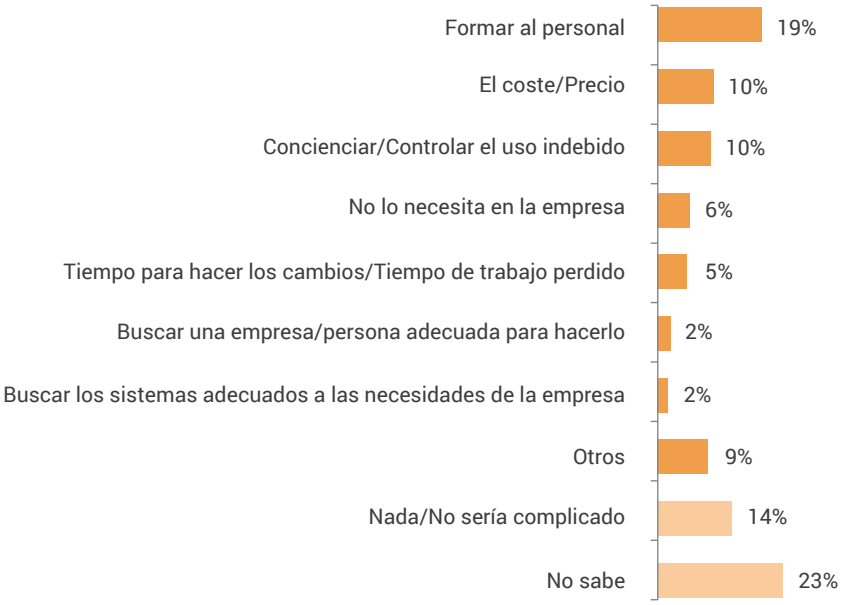

Base empresas con más de 3 empleados y dispone de e-commerce/venta online: 70
Fuente: The Cocktail Analysis

# Relevancia otorgada a la ciberseguridad

## Un 44% considera a la ciberseguridad como un aspecto muy relevante para una empresa, una tendencia al alza

**Gráfico 25**

Barreras a la implementación de medidas en ciberseguridad




Base empresas con más de 3 empleados: 396
Fuente: The Cocktail Analysis

2 de cada 5 pymes atribuye **un elevado nivel de importancia** a la ciberseguridad para una empresa y un 44% la considera “muy importante”.

Entre los elementos identificados como más complicados de implementar, destacan la formación de personal (19%), el coste (10%) y la concienciación / control del uso indebido (10%).

# LA VISIÓN DE LOS USUARIOS

## Conociendo el principal eslabón de la cadena

No es posible obtener una panorámica completa sobre la ciberseguridad en España sin prestar atención a los usuarios, que son quienes, en último término, conforman la fuerza de trabajo de las pymes, las grandes empresas y la administración pública. Y como dice un conocido lema del sector, **un sistema de seguridad es tan fuerte como su eslabón más débil**, en este caso los citados usuarios.

Para indagar en este aspecto, se ha realizado una encuesta a una muestra representativa por género, edad, zona y clase social de los internautas españoles, que nos ha permitido establecer una radiografía de cómo es percibida la ciberseguridad entre los usuarios de internet: su nivel de concienciación, nivel de relevancia atribuido a este campo, principales medidas implementadas y seguridad atribuida a las diferentes actividades online.

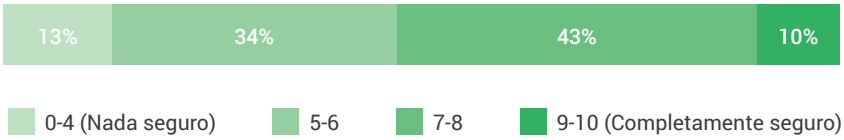
La metodología empleada para su elaboración ha sido cuantitativa, a través de **817 encuestas online** (para más detalles ver capítulo de Metodología).

## Concienciados, pero hasta cierto punto

- **3 de cada 4 participantes en el sondeo** atribuyen una gran importancia a la cuestión de la ciberseguridad. Es una percepción basada en la experiencia, ya que casi **6 de cada 10 usuarios han tenido algún tipo de incidente** relacionado con su correo electrónico, desde los más leves (un aviso del proveedor avisando de actividad sospechosa en su cuenta) hasta los más graves (suplantación de identidad, fraude).
- Solo **1 de cada 10** usuarios encuestados se manifiesta "completamente seguro" cuando accede a internet. **4 de cada 10** se sienten "bastante" seguros.
- Más de **8 de cada 10 encuestados tiene instalado algún antivirus**, aunque las tres cuartas partes de ellos se limita a utilizar **los servicios gratuitos de protección** para sus sistemas informáticos y dispositivos.
- **Menos de una quinta parte** de la muestra adopta medidas de precaución adicionales, como la actualización constante de contraseñas o realizar copias de seguridad de los archivos importantes con regularidad.

**Gráfico 26**

¿Se sienten seguros los usuarios en internet?




Base total: 817
Fuente: The Cocktail Analysis

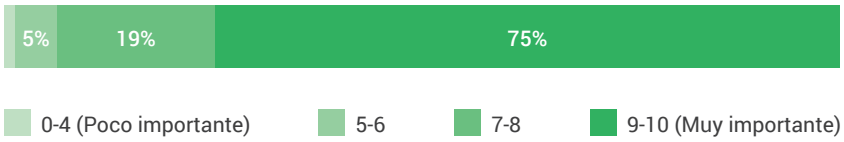
# Concienciación sobre ciberseguridad

## A pesar de la alta relevancia que tiene para los usuarios la ciberseguridad, muy pocos tienen instalado un antivirus de pago en alguno de sus dispositivos

La buena noticia: la relevancia otorgada a la cuestión de la ciberseguridad es elevada y parece existir una conciencia del riesgo pues **el 75% de los encuestados considera que es "muy importante"**

**Gráfico 27**

¿Cómo de importante es la ciberseguridad para los usuarios de internet?




Base total: 817
Fuente: The Cocktail Analysis

Y la mala noticia: **4 de cada 10 usuarios considera que tiene un nivel bajo de protección** a la hora de usar sus dispositivos conectados. Así, el 40% considera que sus dispositivos están **"poco o nada" protegidos.**

Cerca de un 60% de usuarios afirma haber tenido alguna incidencia relacionada con la seguridad:

- 46% ha recibido algún email con información sobre **actividades sospechosas** en su cuenta de email.
- 11% admite que han suplantado su contraseña en alguna de sus cuentas.

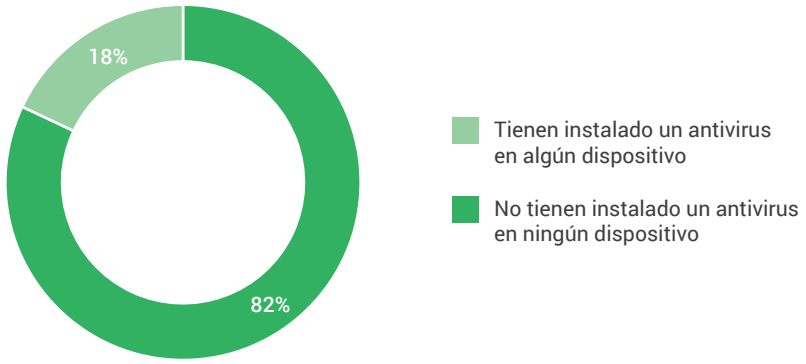
La amplia mayoría de los usuarios (82%) afirma tener instalado algún antivirus en al menos uno de sus dispositivos conectados a internet, aunque **el 74% se decanta por el antivirus gratuito** y solo 1 de cada 4 tiene un antivirus de pago en sus dispositivos (ordenadores, tablets, smartphones, etc).

Un **antivirus de pago** tiene un coste medio de **50 euros al año.** Con ese dinero se puede:

- Comprar dos entradas para el Zoo.
- Pagar un mes de abono de transporte público para una sola zona en Madrid y Barcelona.
- Tomar 35 cafés.

### Gráfico 28

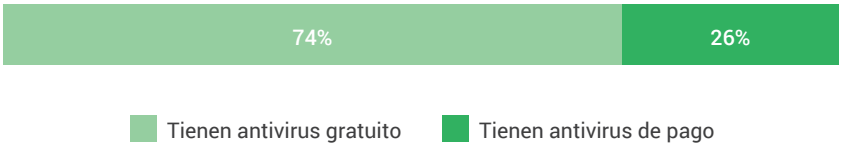
¿Tienes instalado un antivirus en alguno de tus dispositivos?




Base: Acceden a Internet desde alguno de sus dispositivos: 815
Fuente: The Cocktail Analysis.

### Gráfico 29

¿Este antivirus es de pago o gratuito?




Base tiene antivirus en algún dispositivo: 670
Fuente: The Cocktail Analysis.

# Medidas implementadas

## Apenas un 14% de usuarios actualiza sus contraseñas con regularidad y solo un 21% hace regularmente copias de seguridad de sus archivos

Cuando se pregunta a los usuarios sobre diferentes medidas adoptadas para navegar de manera segura en internet, aparecen algunas pautas ampliamente extendidas:

La reacción más común: Un 64% manifiesta que en caso de recibir un correo sospechoso **lo elimina sin abrirlo.**

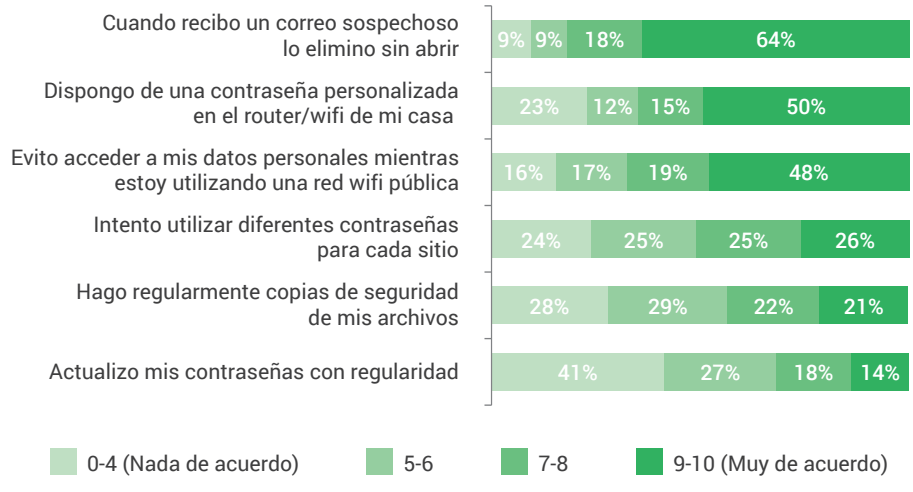
- La mitad de la muestra admite que dispone de una contraseña personalizada en el router /wifi de su casa.
- Casi la mitad está de acuerdo con la idea de evitar acceder a sus datos personales mientras usa una wifi pública.

Sin embargo, existen otras medidas básicas que necesitan mayor implementación:

- Solo un 26% utiliza diferentes contraseñas en cada sitio.
- Apenas 2 de cada 10 hacen regularmente copias de seguridad de sus archivos (21%).
- Un minoritario 14% actualiza sus contraseñas con regularidad.

**Gráfico 30**

¿Cómo reaccionan los usuarios ante las amenazas?




Base total: 817

Fuente: The Cocktail Analysis.

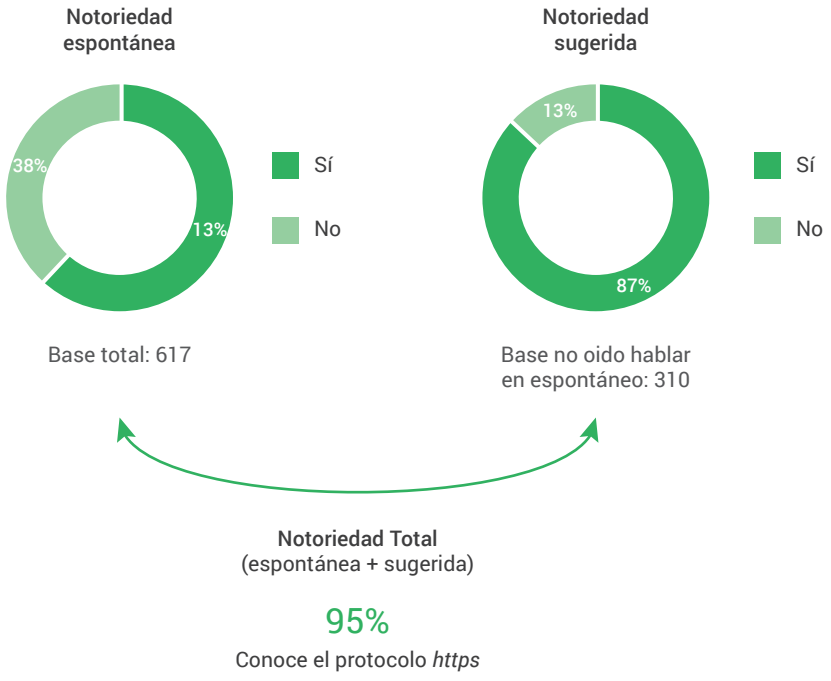
# Conocimiento y relevancia del protocolo https


## Cerca de un 70% afirma que “solo realiza compras o transacciones en páginas https”

Acerca del conocimiento espontáneo del protocolo https, un considerable 62% manifiesta que “ha oído hablar” de estas páginas. Cuando se puntualiza y explica a los usuarios de qué se trata —“las páginas con protocolo https son aquellas que se simbolizan con un candado y están destinadas a la transferencia segura de datos”—, los internautas que afirman conocer este protocolo **aumentan hasta un 87%.**

**Gráfico 31**

Notoriedad del protocolo https




Base total: 817
Fuente: The Cocktail Analysis.

La incorporación de este protocolo influye de manera positiva en la confianza hacia las páginas webs donde está implementado. Cuando se pregunta a los usuarios **si se sienten más seguros** si la página en la que están navegando tiene protocolo https, un 82% responde afirmativamente.

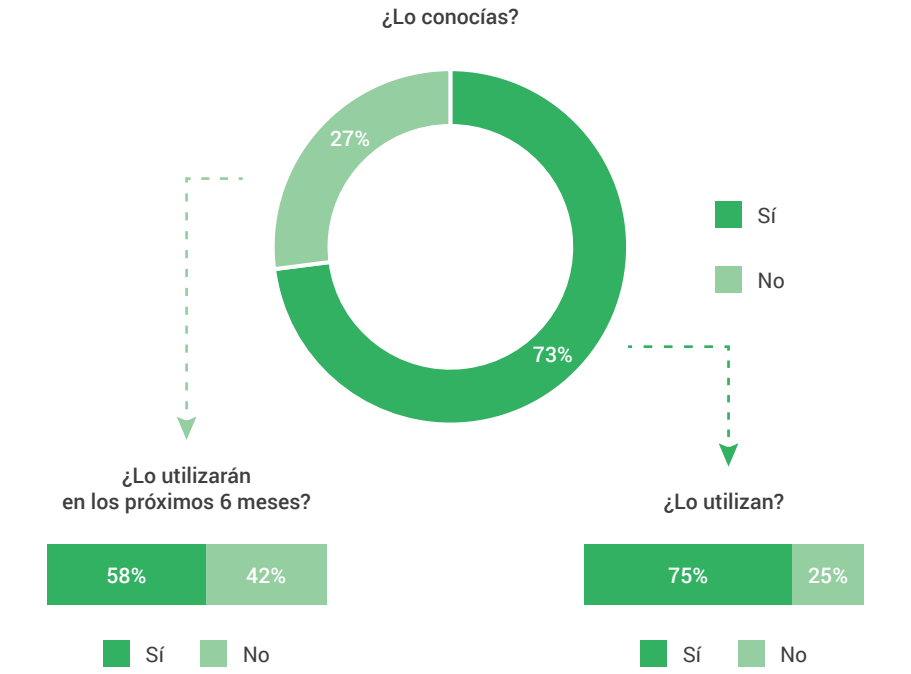
# Conocimiento y relevancia de 2 Step Verification (2SV)

## Uso masivo de la verificación segura

Casi 3 de cada 4 encuestados (73%) reconoce el **sistema de verificación en dos pasos**. Entre los que afirman no conocerlo tras la lectura de la descripción, un 56% manifiesta interés y predisposición a su uso en los próximos 6 meses. Y entre los que lo conocen, un 75% afirma que lo utiliza actualmente.

**Gráfico 33**

Conocimiento 2SV tras una descripción




Base no conocía el 2SV: 220
Base conoce el 2SV: 597
Fuente: The Cocktail Analysis

# Seguridad atribuida a diferentes actividades en internet

## Aquellas actividades más "sensibles" o con mayores riesgos potenciales, se perciben como más seguras

**Gráfico 34**

¿Es seguro lo que hacemos en internet?

| | Realizan... | Consideración de nivel de seguridad (valoraciones 9 y 10)* | Consideración de nivel de seguridad Media | Consideración de nivel de protección de datos personales (valoraciones 9 y 10)** | Consideración de nivel de protección de datos personales Media |
|---|---|---|---|---|---|
| Búsqueda de información | 88% | 13% | 6,3 | 10% | 5,7 |
| Consulta/operaciones bancarias | 82% | 40% | 8 | 34% | 7,7 |
| Redes sociales | 82% | 10% | 6 | 5% | 5,1 |
| Compras | 81% | 28% | 7,7 | 11% | 6,2 |
| Trámites con Administración Pública | 64% | 34% | 7,7 | 32% | 7,7 |
| Suscripción a plataformas de contenidos (Netflix, Spotofy, HBO, Amazon Prime...) | 51% | 17% | 6,9 | 15% | 6,5 |
| Seguro de hogar/coche | 23% | 18% | 7,2 | 17% | 6,7 |
| Seguro de salud | 14% | 27% | 7,6 | 26% | 7,3 |

* 0 "No me siento nada seguro/a" y 10 "Me siento completamente seguro/a"

** 0 "No están nada protegidos" y 10 "Están completamente protegios"

Base total: 817

Fuente: The Cocktail Analysis

Banca y administración pública son las operaciones online que el usuario percibe con un mayor nivel de seguridad y protección de datos.

Damos por sentado que las actividades más "sensibles" —o con mayor riesgo potencial en términos de seguridad— son más seguras. El usuario anticipa **un doble esfuerzo de seguridad** por parte de las plataformas que prestan estos servicios.

En el extremo opuesto, las redes sociales son percibidas como las plataformas online con menor nivel de seguridad y protección de los datos personales:

Solo **un 10%** valora con puntuación 9 o 10 el nivel de seguridad en redes sociales.

Destacan las plataformas de compra online como las terceras a las que se atribuye mayor seguridad. Pero en contraste, en estas plataformas el nivel de **protección de datos** no se considera muy elevado.

# METODOLOGÍA EMPLEADA

Este estudio abordó el panorama de la ciberseguridad en España desde diferentes perspectivas: pymes y grandes empresas, administración pública y un pequeño y siempre útil apartado dedicado a los usuarios. Se combinaron varias metodologías de recogida de datos para presentar las diversas visiones sobre la ciberseguridad.

Fórmulas metodológicas:

- **Desk Research**: análisis de fuentes secundarias sobre las cifras e indicadores básicos sobre el ámbito de la ciberseguridad.
- **Entrevistas a expertos:** investigación cualitativa a través de entrevistas a profesionales de la administración pública y responsables de las grandes corporaciones (Ver RECUADRO 1).
- **Encuesta a pymes:** investigación cuantitativa que analiza la ciberseguridad en el ámbito de las pequeñas y medianas empresas (Ver RECUADRO 2).
- **Encuesta a usuarios de internet:** investigación cuantitativa que profundiza en la concienciación de los usuarios ante las amenazas de la ciberseguridad (Ver RECUADRO 3).

**RECUADRO 1 – FICHA TÉCNICA**
ENTREVISTAS A EXPERTOS

Se ha realizado un estudio cualitativo mediante entrevistas en profundidad.

Muestra: 12 entrevistas.

Interlocutores:

- Tres entrevistas a expertos de las Administraciones Públicas:
  - Félix Barrio, *Gerente del área de Industria y apoyo a la I+D+i* en el INCIBE.
  - Raúl Riesco, *Subdirector de Ciberseguridad para Ciudadanos, Menores y Promoción del Talento* en el INCIBE.
  - Marcos Gómez, *Subdirector de servicios de ciberseguridad* en el INCIBE.
- Nueve entrevistas a responsables en grandes corporaciones y expertos en ciberseguridad:
  - Alejandro Villar, *Director Cybersecurity & Technology Risk* en Repsol.
  - Francisco Lázaro Anguís, *Chief Information Security Officer and Data Protection Officer* en Renfe.
  - Eva Cristina Cañete, *Chief Information Security Officer* en Unicaja Banco.
  - Juan Carlos Gómez, *Director Global de Ciberinteligencia, Control y Respuesta a Ciberamenazas* en Telefónica.
  - Elena Matilla, *Chief Information Security Officer* en Red Eléctrica.
  - Rubén Santamarta, *Principal Security Consultant* en IOActive.
  - David Barroso, *Founder* en CounterCraft.
  - Hugo Teso, experto en ciberseguridad.
  - Bruno Díaz Brière, experto en ciberseguridad.

Formato entrevistas: telefónicas / presenciales de 45-50 min.

**RECUADRO 2 – FICHA TÉCNICA**
ENCUESTA A PYMES

Se realizó un estudio cuantitativo a pymes mediante encuestas telefónicas (CATI).

Universo: pymes representativas españolas por número de empleados y sector de actividad.

Ámbito: España.

Duración del cuestionario: 10 min.

Tamaño muestral: 720 encuestas telefónicas (400 de dimensionamiento + 320 de profundización en pymes con más de 3 asalariados*). El acercamiento a las pymes ha sido a través de entrevistas telefónicas.

Error muestral: utilizando un p = q = 0,5 y nivel de confianza del 95,5%, es 3,7% para 720 encuestas telefónicas; 4,9% para 400 y 5,5% para 320.

Fecha: el trabajo de campo se realizó en abril de 2019.

* La decisión de ceñir la encuesta a pymes con más de 3 asalariados se debe a que en empresas pequeñas puede ser complicado alcanzar cierto nivel de profundización.

**RECUADRO 3 – FICHA TÉCNICA**
ENCUESTA A USUARIOS DE INTERNET

Se realizó un estudio cuantitativo a usuarios de internet mediante encuestas online (CAWI).

Universo: población internauta representativa española (género, edad, zona y clase social).

Ámbito: España.

Duración del cuestionario: 10 min.

Tamaño muestral: 817 encuestas online.

Error muestral: utilizando un p = q = 0,5 y nivel de confianza del 95,5%, es 3,4% para 817 encuestas online.

Fecha: el trabajo de campo se realizó en marzo de 2019.

# Glosario[1]

**2FA (segundo factor de autenticación):** La Autenticación de Dos Factores, también conocida como 2FA, verificación en dos pasos o TFA (Two Factor Authentication) es una capa adicional de seguridad, dentro de lo que se conoce como «Autenticación de Factores Múltiples», que requiere no solo una contraseña y nombre de usuario sino también algo único, una información que solo el usuario conoce, como por ejemplo, un token físico.

**2SV (sistema de verificación en dos pasos):** El sistema de autenticación envía, tras haber introducido usuario y contraseña, un código adicional, ya sea por correo electrónico, SMS, o llamada telefónica, y solicita que se ingrese dentro de un determinado lapso de tiempo para poder completar el login (después de ese tiempo, el código enviado expira).

**Antivirus:** Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como *malware*.

**Ataques DDoS** (Denegación de servicio): Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él. El ataque consiste en saturar al servidor con peticiones de servicio hasta que este no puede atenderlas, provocando su colapso.

**Backdoor**: Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema. Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito por los propios autores, pero al ser descubiertas por terceros pueden ser utilizadas con fines ilícitos.

**Firewall o cortafuegos:** Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen

1 https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios.

**Gusano:** Es un programa malicioso (o *malware*) que tiene como característica principal su alto grado de «dispersabilidad», es decir, lo rápidamente que se propaga. Mientras que los troyanos dependen de que un usuario acceda a una web maliciosa o ejecute un fichero infectado, los gusanos realizan copias de sí mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana.

**Malware:** Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

**Nube o Cloud:** El término cloud computing o computación en la nube se refiere a un paradigma que permite ofrecer servicios de computación a través de internet. Esta tendencia permite a los usuarios almacenar información, ficheros y datos en servidores de terceros, de forma que puedan ser accesibles desde cualquier terminal con acceso a la nube o a la red, resultando de esta manera innecesaria la instalación de software adicional en el equipo local del usuario, salvo el que facilita el acceso a la red. Importantes plataformas ofrecen herramientas y funcionalidades de este tipo y aunque conlleva una importante dinamización y libertad, se debe prestar especial atención a la seguridad de la información, particularmente desde el punto de vista de la protección de la intimidad y de los datos personales, ya que la información, documentos y datos se encuentran almacenados en servidores de terceros sobre los que generalmente no se tiene control.

**Phishing:** Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir información confidencial (contraseñas, datos bancarios, etc.) de usuarios legítimos de forma fraudulenta. El estafador o phisher suplanta la personalidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, SMS o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador.

**Protocolo https:** El Protocolo seguro de transferencia de hipertexto (en inglés: Hypertext Transfer Protocol Secure o HTTPS), es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

**Ransomware:** El ciberdelincuente toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.

**Spam:** Es correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva. Este tipo de mensajes pueden causar graves molestias y provocar pérdidas de tiempo y recursos.

**Spyware:** Es un malware que recopila información de un ordenador y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del ordenador.

**Suplantación de identidad:** Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude o acoso (*cyberbulling*).

**Troyano:** Se trata de un tipo de malware o software malicioso que se caracteriza por carecer de capacidad de autorreplicación. Generalmente, este tipo de malware requiere del uso de la ingeniería social para su propagación.

**Virus:** Programa diseñado para que al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo. De esta manera, cuando se ejecuta una aplicación infectada, puede infectar otros archivos. A diferencia de otro tipo de malware, como los gusanos, se necesita acción humana para que un virus se propague entre máquinas y sistemas. Los efectos que pueden provocar varían dependiendo de cada tipo de virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante correos electrónicos a terceros, etc. Los más comunes son los que infectan a ficheros ejecutables.

**Vulnerabilidad:** Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota.

the cocktail® analysis

C/ Salamanca, 17
28020 Madrid

+34 91 567 06 05

info@tcanalysis.com