



CIBERSEGURIDAD

# SIA Essentials

Informe sobre el escenario de amenazas 2025

[telefonicatech.com](https://telefonicatech.com)



# Índice

01 Introducción.....	3
02 Descripción general del escenario de amenazas .....	4
03 Impacto en el negocio.....	6
04 SIA Essentials de Telefónica Tech.....	7
05 Tendencias 2025.....	8
06 Análisis .....	9
07 Conclusiones.....	10

# 01 Introducción

En la era de la transformación digital, la seguridad ya no es un complemento, sino un componente esencial de cualquier estrategia empresarial. La adopción masiva de soluciones en la nube, el auge del teletrabajo y la proliferación de dispositivos conectados han convergido para crear un entorno de amenazas sin precedentes.

Ante este panorama, las organizaciones se enfrentan a un desafío constante: cómo proteger sus activos digitales en un mundo donde los ciberataques son cada vez más sofisticados y las consecuencias, más devastadoras. La respuesta reside en una ciberseguridad proactiva, adaptable y centrada en la inteligencia de amenazas.

**Según el informe Hiscox Cyber Readiness Report, 6 de cada 10 pymes en España han sufrido ciberataques en 2025.<sup>1</sup>**

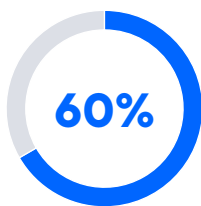
El propósito de este documento es **proporcionar a las empresas información sobre el panorama actual de amenazas para los lugares de trabajo digitales y modernos** y, a través del servicio SIA Essentials de Telefónica Tech, describir cómo una mejor postura de seguridad puede ayudar a proteger su negocio.



<sup>1</sup>[Hiscox Report 2025](#)

## 02 Descripción general del escenario de amenazas

En el contexto actual de transformación digital, la superficie de exposición a ciberamenazas se ha ampliado significativamente. La adopción acelerada de entornos cloud, el trabajo híbrido y la proliferación de dispositivos conectados han generado nuevos vectores de ataque que las organizaciones deben gestionar adecuadamente.



**De los ciberataques se originan a través del factor humano.<sup>2</sup>**

Las amenazas más relevantes continúan evolucionando en sofisticación y capacidad de impacto. Durante 2025 se consolida el ransomware y la extorsión múltiple, el phishing potenciado por IA y el fraude online como vectores de mayor frecuencia y efecto en las organizaciones.<sup>3</sup>

España mantiene una posición destacada en el mapa global de ciberataques, lo que exige una aproximación integral a la ciberseguridad. Los ciberdelincuentes continúan innovando en sus tácticas, técnicas y procedimientos, aprovechando las vulnerabilidades en sistemas cloud, APIs y entornos IoT. La formación y concienciación de los usuarios constituyen elementos críticos para mitigar estos riesgos.<sup>4</sup>

<sup>2</sup> [Verizon DBIR 2025](#)

<sup>3</sup> [INCIBE - Estado de la Ciberseguridad en España](#)

<sup>4</sup> [CCN-CERT - Informe de Amenazas](#)

<sup>5</sup> [Fuente: IBM - Cost of a Data Breach Report 2025](#)

### Ciberataques más comunes en España en 2025

**RANSOMWARE**

**DDOS**

**PHISHING**

### Principales vectores del ataque

 Email

 Servidores Corporativos & en la Nube

 Teléfonos móviles

**29%**

De las empresas han sido víctima de un ciberataque a través de un dispositivo móvil.<sup>5</sup>

**4,44 M \$**

Coste medio de un ciberataque para las empresas.

# Las amenazas más comunes de Internet en la actualidad



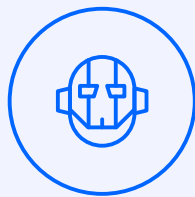
## Malware

Software malintencionado (como ransomware) desarrollado para dañar o interrumpir dispositivos o sus datos (encriptándolos con una clave secreta) o para obtener acceso no autorizado a una red.



## Phishing

Enlaces web en correos electrónicos, SMS u otros medios diseñados para fomentar los clics que llevan a las personas a sitios web maliciosos, donde se puede recopilar su valiosa información personal. Algunos ejemplos de phishing son el Business Email Compromise (CEO Fraud) o el fraude financiero.

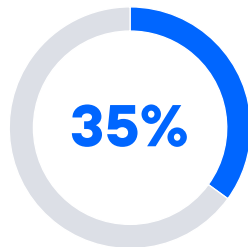


## Bots maliciosos\*

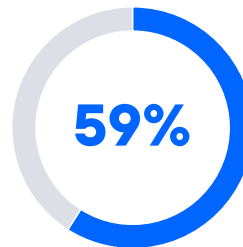
Software que se instala en secreto en los ordenadores y se controla de forma remota. Las redes de bots maliciosos encuentran y cargan información valiosa, lanzan ataques DDoS, brindan acceso a máquinas y mucho más.

\*También existen bots legítimos que realizan muchas tareas repetitivas en Internet

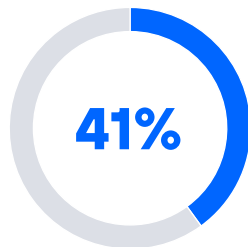
## 03 Impacto en el negocio



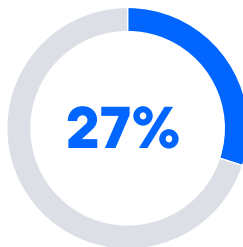
Los ciberataques en España crecieron un **35% en 2025**. Superando los **45.000 ataques diarios**, lo que refleja un aumento significativo de la exposición de las empresas.<sup>6</sup>



Un **59%** de las empresas que sufrieron ciberataques en el último año **reportaron impactos financieros significativos**.<sup>7</sup>



**4 de cada 10 empresas españolas** han sufrido incidentes de ciberseguridad en el último año, siendo el **ransomware una de las amenazas más preocupantes para las organizaciones**.<sup>8</sup>



El **27%** de las empresas experimentó un **ataque de ransomware** en el último año.<sup>9</sup>



<sup>6</sup> [OpenSecurity – Spain 2025](#)

<sup>7</sup> [Hiscoxgroup – Threat Landscape Report 2025](#)

<sup>8</sup> [S2Grupo – TLR2025](#)

<sup>9</sup> [Hiscoxgroup – Threat Landscape Report 2025](#)

# 04 SIA Essentials de Telefónica Tech



## ¿Qué hace?

El servicio de Telefónica Tech protege a los usuarios móviles cuando acceden a Internet, de amenazas de seguridad como el phishing o las descargas de software malicioso como el ransomware.



## ¿Cómo lo consigo?

Lo único que hace falta es contratar una tarifa móvil compatible con el servicio y Telefónica activará el servicio automáticamente.<sup>9</sup>



## ¿Cómo funciona?

**Funciona evaluando el tráfico de red utilizado para la navegación** (consultas del Sistema de nombres de dominio (DNS)) para **identificar y bloquear actividades maliciosas**.

Además de proteger a los clientes de actividades maliciosas, los administradores pueden administrar las políticas de acceso al contenido de internet para alinearlas con las políticas de la empresa.

Todo ello apoyado en las potentes funcionalidades de configuración y visualización del portal del cliente y sin necesidad de descarga o instalar nada en el dispositivo de los usuarios.

### Análisis del servicio:

Resultados hasta diciembre de 2025

# 2,78 mil millones

Total Amenazas Bloqueadas



## 2,52 mil millones

(90,48%)

Accesos a sitios web de malware bloqueados



## 168.411.587

(6,05%)

Bots bloqueados



## 96.768.602

(3,48%)

Sitios web de phishing bloqueados



## 1.965.578

Dispositivos protegidos



## +1.417

Promedio de amenazas bloqueadas por dispositivo

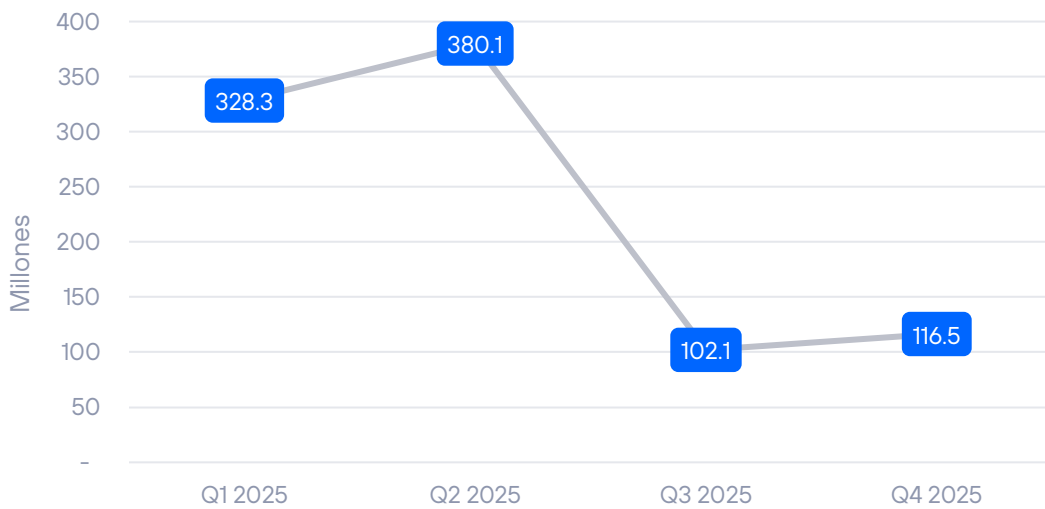
<sup>9</sup> Para saber qué tarifas son compatibles en España, pregunte por SRM (Seguridad en Red Móvil) – el servicio de SIA Essentials de Telefónica en España.

# 05 Tendencias 2025

Evolución servicio del 1º al 4º trimestre de 2025:

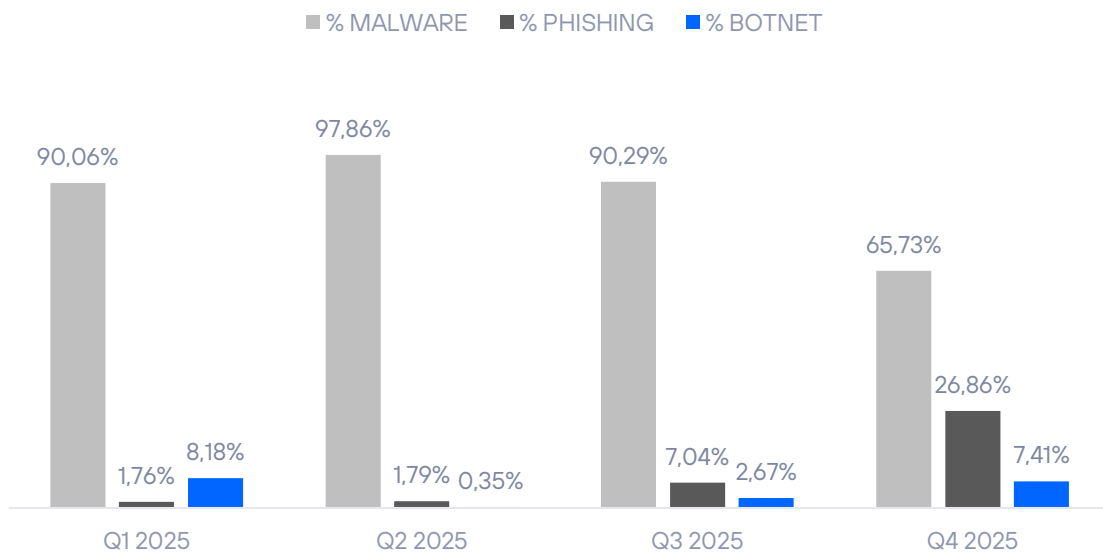
## TOTAL DE AMENAZAS BLOQUEADAS EN EMPRESAS

(Millones por trimestre) Fuente: Telefónica Tech / Akamai



## TOTAL DE AMENAZAS BLOQUEADAS EN EMPRESAS

Fuente: Telefónica Tech / Akamai



## 06 Análisis

La **evolución de las amenazas a lo largo de 2025** muestra un cambio relevante en su tipología. Aunque el volumen total de amenazas bloqueadas **disminuye en la segunda mitad del año**, especialmente en **Q4**, esta tendencia no implica una reducción del riesgo, sino una **transformación** en las **estrategias de ataque**.

Se observa una caída significativa del *malware* tradicional, mientras que aumentan el *phishing* y la actividad *botnet*. Este comportamiento indica un desplazamiento hacia modelos de ataque centrados en el acceso inicial, la **suplantación de identidad** y la **automatización**, donde el objetivo principal es comprometer al usuario o sus credenciales antes que al dispositivo.

Desde la perspectiva de **Telefónica Tech**, esta evolución refleja una mayor sofisticación del ecosistema atacante, que prioriza técnicas más silenciosas y efectivas en fases tempranas del ataque. En este contexto, la menor presencia de malware puede estar asociada tanto a un cambio táctico como a una mayor eficacia en la detección y bloqueo preventivo en capas iniciales.

Asimismo, el incremento de actividad *botnet* sugiere un mayor nivel de **automatización** en las fases de reconocimiento y **preparación de ataques**, en línea con entornos cada vez más expuestos debido a la adopción de *cloud* y servicios digitales.

En conjunto, los datos evidencian una **tendencia clara**: el **riesgo no disminuye**, sino que **evoluciona** hacia **amenazas** más orientadas al usuario y menos visibles. Esto refuerza la necesidad de adoptar un enfoque preventivo, capaz de anticipar y **bloquear la amenaza** antes de que se materialice en un **incidente**.

## 07 Conclusiones

La **ciberseguridad** se consolida como la **principal preocupación empresarial en 2025**, según el barómetro de riesgos de Allianz, destacando la necesidad de estrategias proactivas para **proteger los activos y asegurar la continuidad del negocio**. El incremento en la sofisticación y frecuencia de los **ciberataques** exige una respuesta integral y adaptada a cada organización, independientemente de su tamaño.

En este contexto, **Telefónica Tech**, a través de su servicio **SIA Essentials**, se posiciona como un aliado estratégico, ofreciendo una **ciberseguridad** eficaz y transparente que protege a los usuarios corporativos en todos sus accesos. Este compromiso se refleja en la constante **innovación** y **adaptación** de sus soluciones para hacer frente a las **amenazas emergentes** y garantizar un **entorno digital seguro para las empresas**.



## **Sobre Telefónica Tech**

Telefónica Tech es la compañía líder en transformación digital. La compañía cuenta con una amplia oferta de servicios y soluciones tecnológicas integradas de Ciberseguridad, Cloud, IoT, Big Data, Inteligencia Artificial y Blockchain.

[telefonicatech.com](https://telefonicatech.com)

La información contenida en el presente documento es propiedad de Telefonica Cyber Security & Cloud Tech S.A junto a Telefónica IoT & Big Data Tech S.A, (en adelante "Telefónica Tech") y/o de cualquier otra entidad dentro del Grupo Telefónica o sus licenciantes.

Telefónica Tech y/o cualquier compañía del Grupo Telefónica o los licenciantes de Telefónica Tech se reservan todos los derechos de propiedad industrial e intelectual (incluida cualquier patente o copyright) que se deriven o recaigan sobre este documento, incluidos los derechos de diseño, producción, reproducción, uso y venta del mismo, salvo en el supuesto de que dichos derechos sean expresamente conferidos a terceros por escrito. La información contenida en el presente documento podrá ser objeto de modificación en cualquier momento sin necesidad de previo aviso.

La información contenida en el presente documento no podrá ser ni parcial ni totalmente copiada, distribuida, adaptada o reproducida en ningún soporte sin que medie el previo consentimiento por escrito por parte de Telefónica Tech.

El presente documento tiene como único objetivo servir de soporte a su lector en el uso del producto o servicio descrito en el mismo. El lector se compromete y queda obligado a usar la información contenida en el mismo para su propio uso y no para ningún otro.

Telefónica Tech no será responsable de ninguna pérdida o daño que se derive del uso de la información contenida en el presente documento o de cualquier error u omisión del documento o por el uso incorrecto del servicio o producto. El uso del producto o servicio descrito en el presente documento se regulará de acuerdo con lo establecido en los términos y condiciones aceptados por el usuario de este para su uso.

Telefónica Tech y sus marcas (así como cualquier marca perteneciente al Grupo Telefónica) son marcas registradas. Telefónica Tech y sus filiales se reservan todos los derechos sobre las mismas.

