

CYBER SECURITY

SIA Essentials

Informe sobre el escenario de amenazas 2024



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 2024 Evolución servicio del 1º al 4º trimestre de 2024	8
06 Conclusiones.....	9

01 Introducción

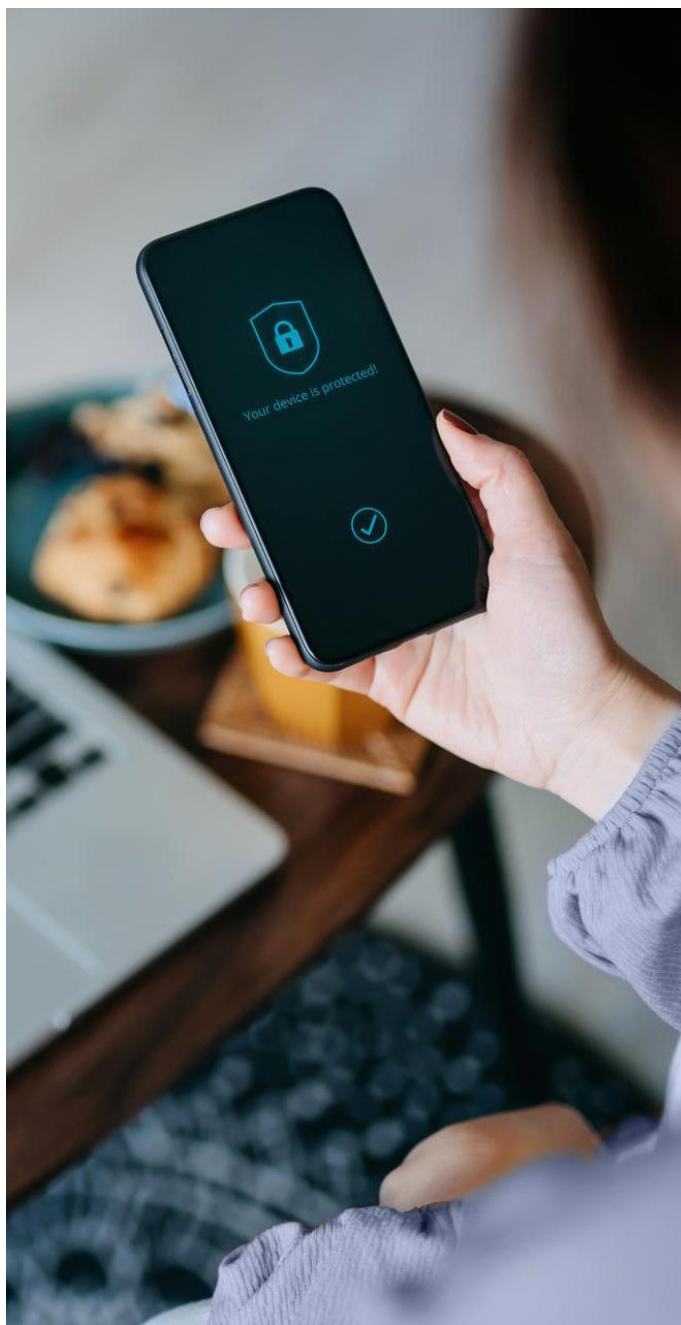
En la era de la transformación digital, la seguridad ya no es un complemento, sino un componente esencial de cualquier estrategia empresarial. La adopción masiva de soluciones en la nube, el auge del teletrabajo y la proliferación de dispositivos conectados han convergido para crear un entorno de amenazas 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, el 96% de las empresas españolas ha sufrido un ciberataque en 2024.¹

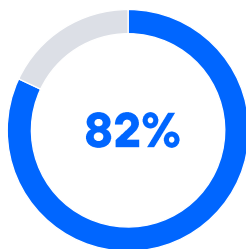
El propósito de este documento es **proporcionar a las empresas información sobre el panorama actual de amenazas para los lugares de trabajo digitales y modernos** y, a través del servicio SIA Essentials de Telefónica Tech, describir cómo una mejor postura de seguridad puede ayudar a proteger su negocio.

¹ [Hiscox Report 2024.](#)



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.²

Las amenazas más relevantes continúan evolucionando en sofisticación y capacidad de impacto. El ransomware, el phishing avanzado y las campañas de malware se han consolidado como los principales riesgos para las organizaciones españolas durante 2024.³

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.⁴

² Verizon DBIR 2024

³ INCIBE - Estado de la Ciberseguridad en España

⁴ CCN-CERT - Informe de Amenazas

⁵ Fuente: IBM - Cost of a Data Breach Report 2024

Ciberataques más comunes en España en 2024

RANSOMWARE

DDOS

PHISHING

Principales vectores del ataque



Email



Servidores Corp & en la nube



Teléfonos móviles

34%

de las empresas han sido víctima de un ciberataque a través de un dispositivo móvil.²

4,88 M dólares

Coste medio de una vulneración de datos.⁵

Las amenazas 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 lugares 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 pueden ser: Business Email Compromise (CEO Fraud) o fraude financiero

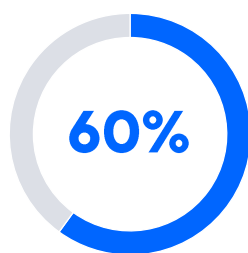


Bots maliciosos*

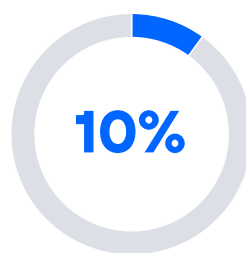
Software que se instala en secreto en los ordenadores y se controla de forma remota. Las redes de bots maliciosos encuentran y cargan información valiosa, lanzan ataques DDoS, brindan acceso a máquinas y mucho más.

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

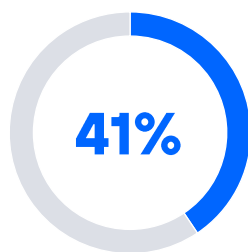
03 Impacto en el negocio



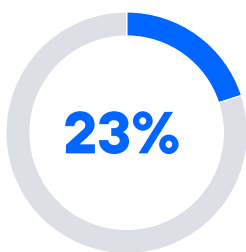
El **60% de las PYMES españolas** que sufrieron un ciberataque en 2024 reportaron pérdidas significativas que **comprometieron la continuidad del negocio**.⁶



Las empresas españolas perdieron el **10%** de sus ingresos durante 2024 **debido a ciberataques**, especialmente por ransomware y violaciones de datos.⁷



El **41% de las empresas españolas** reconocieron que sus empleados utilizan dispositivos móviles personales (BYOD) sin las medidas de seguridad adecuadas, **lo que aumenta el riesgo de vulnerabilidades de seguridad**.⁸



En 2024, el **23% de las organizaciones españolas** fueron víctimas de **ransomware**, posicionando a España como el quinto país más afectado a nivel mundial.⁹



⁶ ReportLinker - Spain Cybersecurity Market Report Q4 2024

⁷ S21sec - Threat Landscape Report 2024

⁸ ESET - Estudio sobre BYOD y seguridad móvil en España 2024

⁹ S21sec - Threat Landscape Report 2024

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. ⁹

—→ ¿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.

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

Análisis del servicio: resultados hasta diciembre de 2024.

1.857.746.735

Total Amenazas Bloqueadas (TBT)



1.683.149.783

(90,60%)

Accesos a sitios web de malware bloqueados



128.884.123

(6,94%)

Bots bloqueados



45.712.829

(2,46%)

Sitios web de phishing bloqueados

1.444.238

Dispositivos Protegidos

+1286

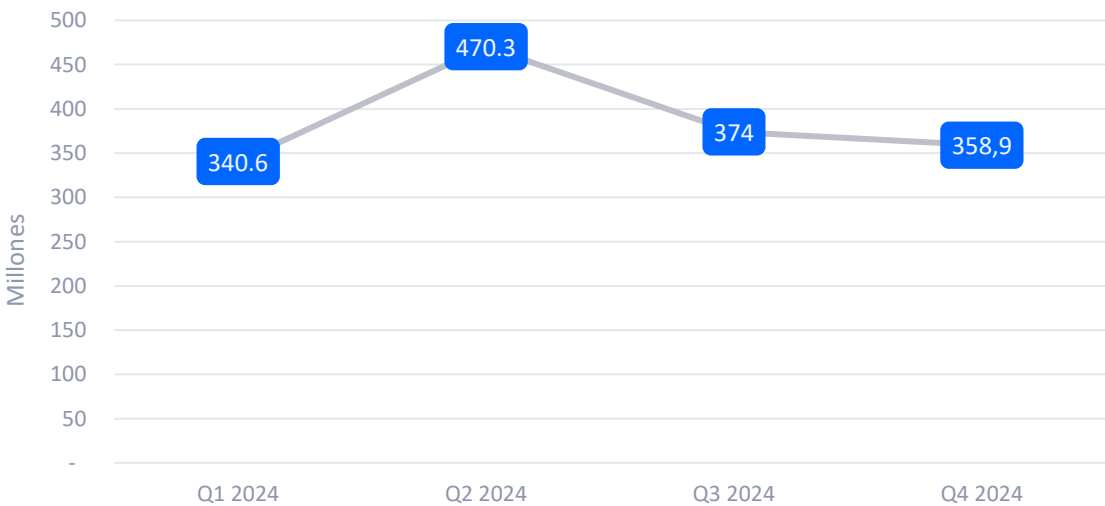
Promedio de amenazas bloqueadas por dispositivo

05 Tendencias 2024

Evolución servicio del 1º al 4º trimestre de 2024

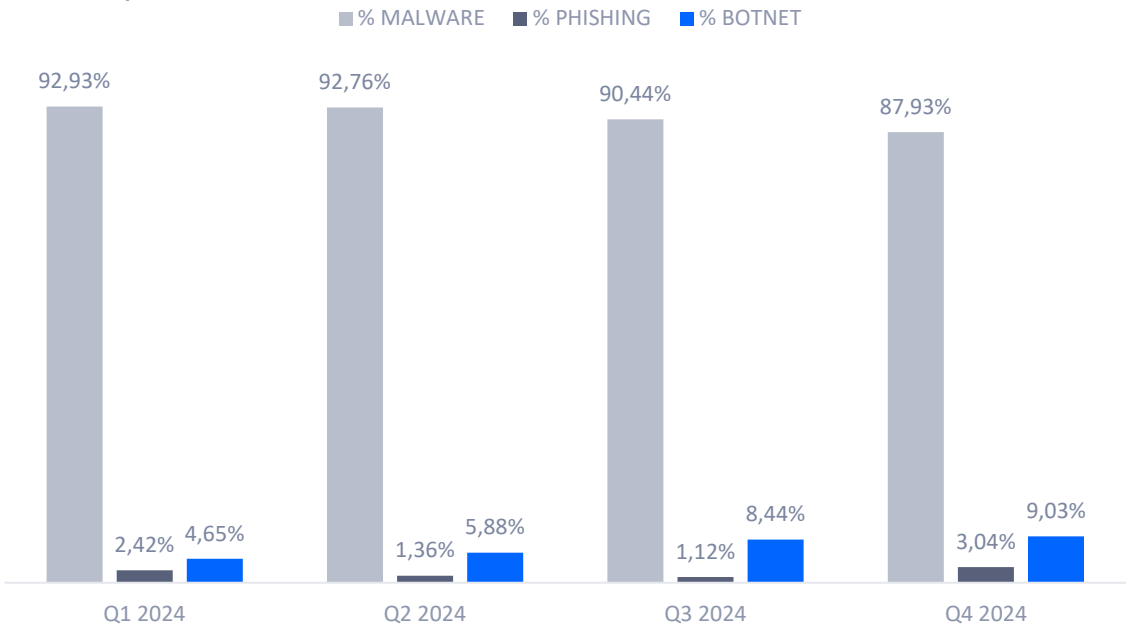
TOTAL DE AMENAZAS BLOQUEADAS EN EMPRESAS

(millones por trimestre) Fuente: TelefónicaTech/Akamai



TOTAL DE AMENAZAS BLOQUEADAS EN EMPRESAS

Fuente: TelefónicaTech/Akamai



06 Conclusiones

La ciberseguridad se consolida como la principal preocupación empresarial en 2024, 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

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.