Telefónica Tech

CYBER SECURITY

SIA Essentials

Informe sobre el escenario de amenazas

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 2023 Evolución servicio del 1º al 4º trimestre de 2023 8

06 Conclusiones 9

01 Introducción

El cambio al trabajo remoto ha acelerado la adopción de la nube, y el nuevo modelo de empleado, que adopta flexibilidad y movilidad, ha ampliado la posible superficie de ciberataque.

Además, en los últimos años, los ataques se han vuelto más sofisticados y más difíciles de detectar. Esto ha animado a las empresas a buscar soluciones de ciberseguridad más estrictas para proteger su información sensible.

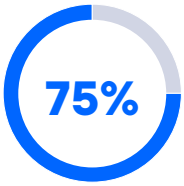
Según el informe Hiscox Cyber Readiness Report, el 49% de las empresas españolas admite haber sufrido un ciberataque en 2023.[1]

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] 22594 - Cyber Readiness Report 2023 - Spanish.pdf (hiscox.es)

02 Descripción general del escenario de amenazas

Vivimos en la era de la digitalización en la cual, todo se encuentra interconectado y se puede hackear. Los ciberdelincuentes cuentan con tecnología cada vez más avanzada, por lo que es fundamental, poner énfasis en el capital humano, que es donde principalmente se encuentran dirigidos los ataques.[2]



De los ciberataques dirigidos comienzan abriendo un correo electrónico con contenido malicioso.

El malware, ransomware, y phishing son algunas de las amenazas más frecuentes.

España, ocupa el tercer puesto a nivel global, como país que más ciberataques ha recibido, registrando hasta 40.000 ataques diarios.[3]

Los tres ciberataques más comunes registrados en 2023 fueron los ataques DDoS, el fraude financiero y los ataques de ransomware. Sus principales puntos de entrada han sido el email y mensajería instantánea, navegación web, dispositivos de almacenamiento externo, los teléfonos móviles personales y corporativos y redes sociales.[4] Los ataques también se han vuelto más sofisticados y los ciberdelincuentes siempre están explorando nuevos vectores de entrada, por ejemplo: los ataques DDoS son cada vez más grandes y complejos y han comenzado a dirigirse a las redes móviles.[5]

Ciberataques más comunes en España en 2023

- Ransomware
- DDoS
- Fraude Financiero

Principales vectores del ataque

- Email
- Servidores Corp & en la nube
- Teléfonos móviles

1 de cada 2
organizaciones ha sido víctima de un ciberataque en los últimos 3 años

4,35 M dólares
Coste medio de una vulneración de datos

[2] SoSafe Compromiso de Lucas Perez Sanchez (highspot.com)
[3] ciberataques-españa-crecen-30%-2023 (cybersecuritynews.es)
[4] Los tipos de ciberataques más comunes que reciben las empresas – Sosmatic
[5] Ataques DDoS: Qué son, evolución y cómo prevenirlos y mitigarlos (computing.es)

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.

Phising

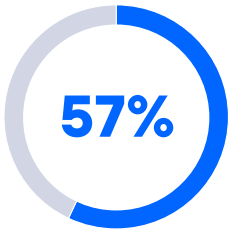
Enlaces web en correos electrónicos, SMS u otros lugares diseñados para fomentar los relojes que llevan a las personas a sitios web maliciosos donde se puede recopilar su valiosa información personal. Algunos ejemplos de phishing pueden ser: Business Email Compromise (CEO Fraud) o fraude financiero

Bots maliciosos*

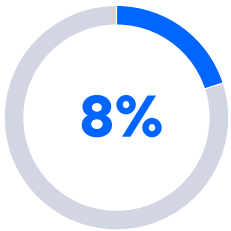
Software que se instala en secreto en los ordenadores y se controla de forma remota. Las redes de bots maliciosos encuentran y cargan información valiosa, lanzan ataques DDoS, brindan acceso a máquinas y mucho más.

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

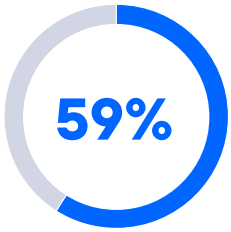
03 Impacto en el negocio



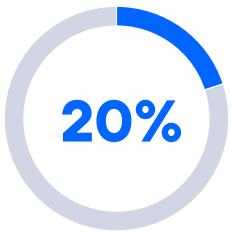
El 57% de **las pymes que cierran lo hacen por un ciberataque**, bien sea por el rescate pagado, por la sanción institucional o por que se haya perdido la confianza de los clientes.



Empresas españolas perdieron el 8% de sus ingresos durante el 2023 como consecuencia de los ciberataques. Un solo ciberataque, especialmente uno que resulta en una violación de datos de clientes, tendrá impactos a largo plazo en la empresa que lo sufre.[7]



Es la media del **incremento** que se ha pagado en el **2023, por un rescate ante un ciberataque**.[6]



En **2023,** el 20% de las organizaciones españolas experimentaron **un ataque de ransomware.**[8]

[6] El 57 % de las pymes que cesan su actividad en España es debido a un ciberataque – Atana
[7] España registró más de 220.000 ataques a dispositivos móviles en 2023 | Seguridad | IT Reseller
[8] El 20% de las empresas españolas ha sufrido un ataque de ransomware en 2023 | Seguridad | IT Reseller

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.

Información sobre el servicio

268.346.810
Total Amenazas Bloqueadas (TBT)

233.903.642 (87,16%)
Accesos a sitios web de malware bloqueados

21.340.097 (7,95%)
Bots bloqueados

13.103.071 (4,88%)
Sitios web de phishing bloqueados

719.022
Dispositivos Protegidos

+373
Promedio de amenazas bloqueadas por dispositivo

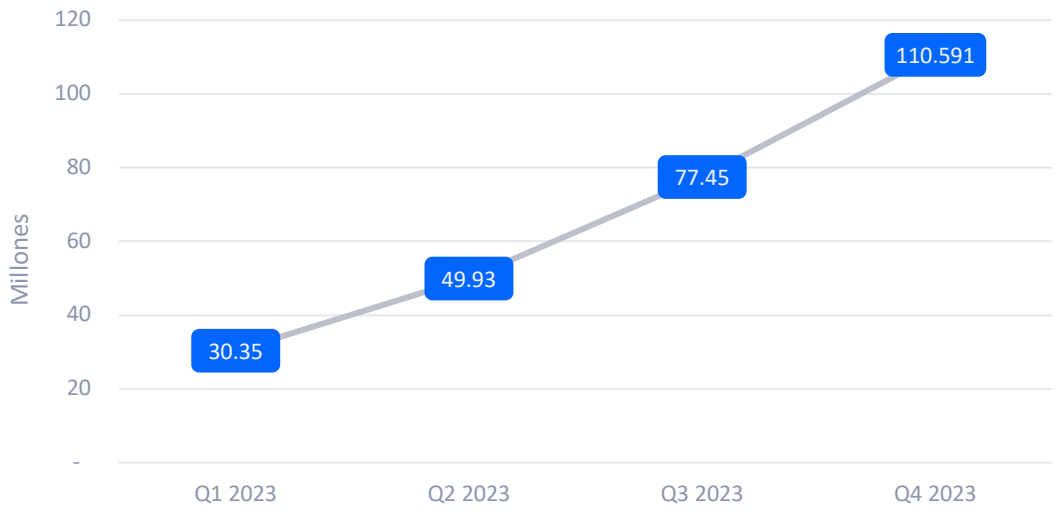
[9] Para saber qué tarifas son compatibles en España, pregunte por SRM (Seguridad en Red Móvil) - el servicio de SIA Essentials de Telefónica en España.)

05 Tendencias 2023

Evolución servicio del 1º al 4º trimestre de 2023

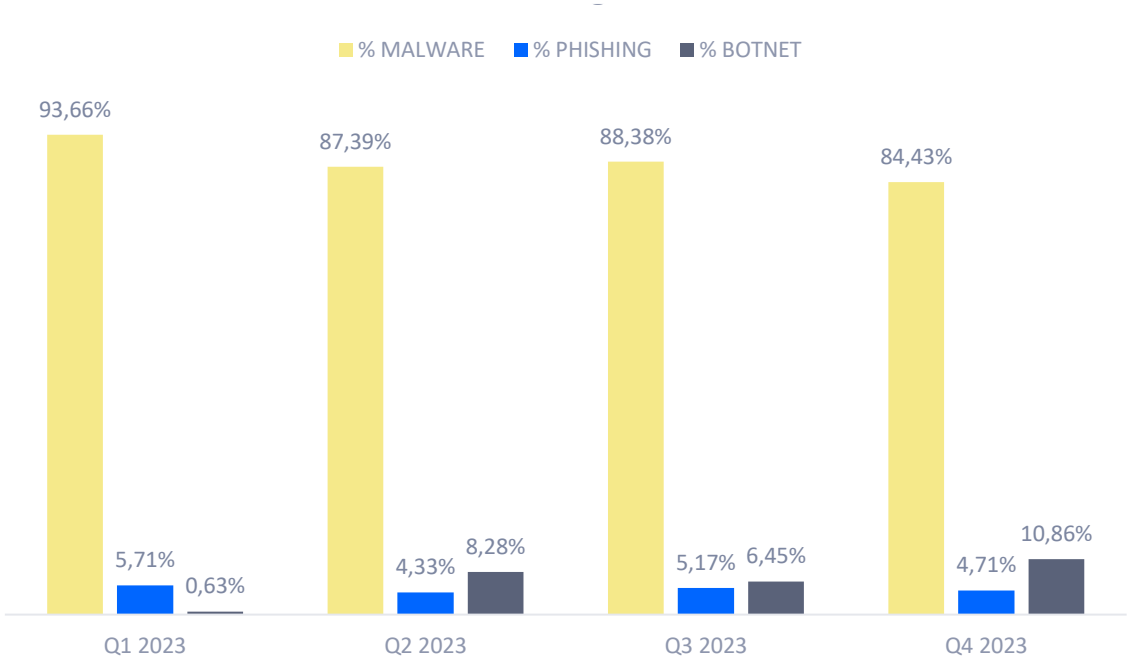
TOTAL DE AMENAZAS BLOQUEADAS EN EMPRESAS (millones por trimestre)

Fuente: TelefónicaTech/Akamai



TOTAL DE AMENAZAS BLOQUEADAS EN EMPRESAS

Fuente: TelefónicaTech/Akamai



06 Conclusiones

Según el último barómetro de riesgos de Allianz[10], el principal riesgo empresarial global para 2024 sigue siendo el de los incidentes cibernéticos y la interrupción del negocio. A medida que los ataques cibernéticos aumentan en número y sofisticación, las empresas deben establecer defensas de seguridad cibernética proactivas para proteger los activos y la continuidad del negocio.

Tanto para pequeñas, medianas y largas empresas, los ataques cibernéticos ocupan el primer puesto de riesgo como principal amenaza para 2024.

En concreto, ESET[11] ha publicado un informe, en el que indica que España fue el 3er país con más ciberataques corporativos en 2023.

SIA Essentials de Telefónica Tech ofrece a las empresas una ciberseguridad eficaz frente a las amenazas más comunes, protegiendo de forma transparente y no intrusiva a los usuarios corporativos en el acceso al correo y a Internet.

[10] https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf
[11] https://web-assets.esetstatic.com/wls/2023/02/eset_threat_report_t32022.pdf

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

Telefónica Tech