Telefónica Tech

Ciberseguridad en 2022 y más allá

2022

¿Dónde estás hoy?

"El panorama de los riesgos está cambiando, y la incertidumbre sobre el futuro de la postpandemia laboral está afectando a los planes empresariales del sector TI." [(1)]

80%

de los encuestados considera el riesgo relacionado con la ciberseguridad como un **riesgo empresarial**, no sólo como un riesgo tecnológico.

51%

de los encuestados ha experimentado un **incidente de riesgo de ciberseguridad** en los últimos dos años. [(2)]

El panorama

El perímetro se ha acabado - larga vida a los nuevos perímetros

El perímetro de seguridad está ahora en todas partes, especialmente con el aumento de la movilidad de los empleados, por lo que la seguridad afecta a todos los aspectos de una empresa y a todos sus integrantes, no sólo al departamento de TI.

Afrontar los retos de la nueva ola de digitalización

La transformación digital significa que el número de dispositivos conectados está creciendo exponencialmente y la superficie de ataque se está expandiendo, ya sea a través de IoT, OT o incluso la robótica.

Nuevos tipos de ataques

El *ransomware* sigue en auge, pero los nuevos ataques incluyen malware que infecta el servidor Dockers en las plataformas Cloud, ataques a APT y cadenas de suministro, o ataques que aprovechan y apuntan a la IA.

El paso de los ataques a las infraestructuras a los ataques a las personas

Mientras que los ataques a las vulnerabilidades de los sistemas siguen siendo un elemento básico de las actividades nefastas, se ha renovado el enfoque en los ataques contra los empleados individualmente a través de los dispositivos móviles. El auge del BYOD y de los dispositivos IoT creará más dolores de cabeza a los departamentos de TI en 2022. [(3)]

Phishing de credenciales de SaaS

Más del ***75%*** *de los ciberataques dirigidos comienzan con alguien de una organización que abre un correo electrónico con contenido malicioso....*
1/4 *de todos los empleados han notado un aumento de los correos electrónicos fraudulentos, el spam y los intentos de suplantación de identidad en su bandeja de entrada corporativa desde el comienzo de la COVID-19.* [(4)]

Zero Trust

Asumir que la red es hostil y sólo dar a las entidades el acceso menos privilegiado: los permisos mínimos que necesitan para cumplir su función. Se prevé que este marco se convierta en esencial para impedir que se explote la identidad a través de diversas vías en 2022. [(3)]

Para 2024
las organizaciones que adopten una arquitectura de ciberseguridad *mesh* reducirán el impacto financiero de los incidentes de seguridad en una media del
90% [(5)]

Para 2024 el
30%
de las empresas adoptará las capacidades de Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA) y Firewall As A Service (FWaaS) suministradas por el mismo proveedor. [(6)]

Para 2025 el
70%
de los consejeros delegados exigirá una cultura de resiliencia organizativa para sobrevivir a las amenazas coincidentes de la ciberdelincuencia, los fenómenos meteorológicos graves, los disturbios civiles y las inestabilidades políticas. [(5)]

Toma la iniciativa

Para 2024 el
60%
de las organizaciones de los sectores altamente regulados crearán una función dedicada a la **gestión de los ciber riesgos** -o una función equivalente- que proporcionará conocimientos especializados sobre los mismos, apoyo, supervisión y cuestionará las decisiones relacionadas con los riesgos por parte de los responsables de la seguridad y la gestión. [(2)]

Los responsables de la seguridad y la gestión de riesgos deben:

Desarrollar
una cultura de juicio cibernético y alinearla con la evolución de las necesidades de talento.

Priorizar
a los clientes y a los ejecutivos orientados al mercado (incluidos el director financiero, el director de marketing y el director general) en los planes de comunicación y relación con las partes interesadas.

Posicionar
la empresa hacia un futuro seguro eligiendo tecnologías de ciberseguridad que ofrezcan altos niveles de integración, automatización y capacidades de orquestación. [(6)]

Telefónica Tech

Desplegamos el poder de la **tecnología integrada**, combinando de forma única a las **mejores personas**, con la **mejor tecnología** y las **mejores plataformas**, con el apoyo de un dinámico ecosistema de socios, para marcar una verdadera diferencia para **nuestros clientes, cada día.**

Estamos aquí para **ayudar**.

Visita **telefonicatech.com**
para más información sobre Cloud Technology.

@TelefonicaTech | Telefónica Tech | Telefónica Tech | TelefonicaTech

Fuentes:
[(1)] https://www.forbes.com/sites/bernardmarr/2021/10/25/the-5-biggest-cloud-computing-trends-in-2022/?sh=7d2c7ceb2267
[(2)] https://www.accenture.com/gb-en/insights/strategy/green-behind-cloud
[(3)] Gartner Forecast Analysis: Public Cloud Services, Worldwide, 3Q21 Update October 2021
[(4)] https://www.apper.ph/2021/09/17/10-future-cloud-computing-trends-in-2022/
[(5)] Gartner, 2022 Planning Guide for Cloud and Edge Computing October 2021
[(6)] Gartner Forecast Analysis: Cloud Consulting and Implementation Services, Worldwide July 2021

Telefónica Tech