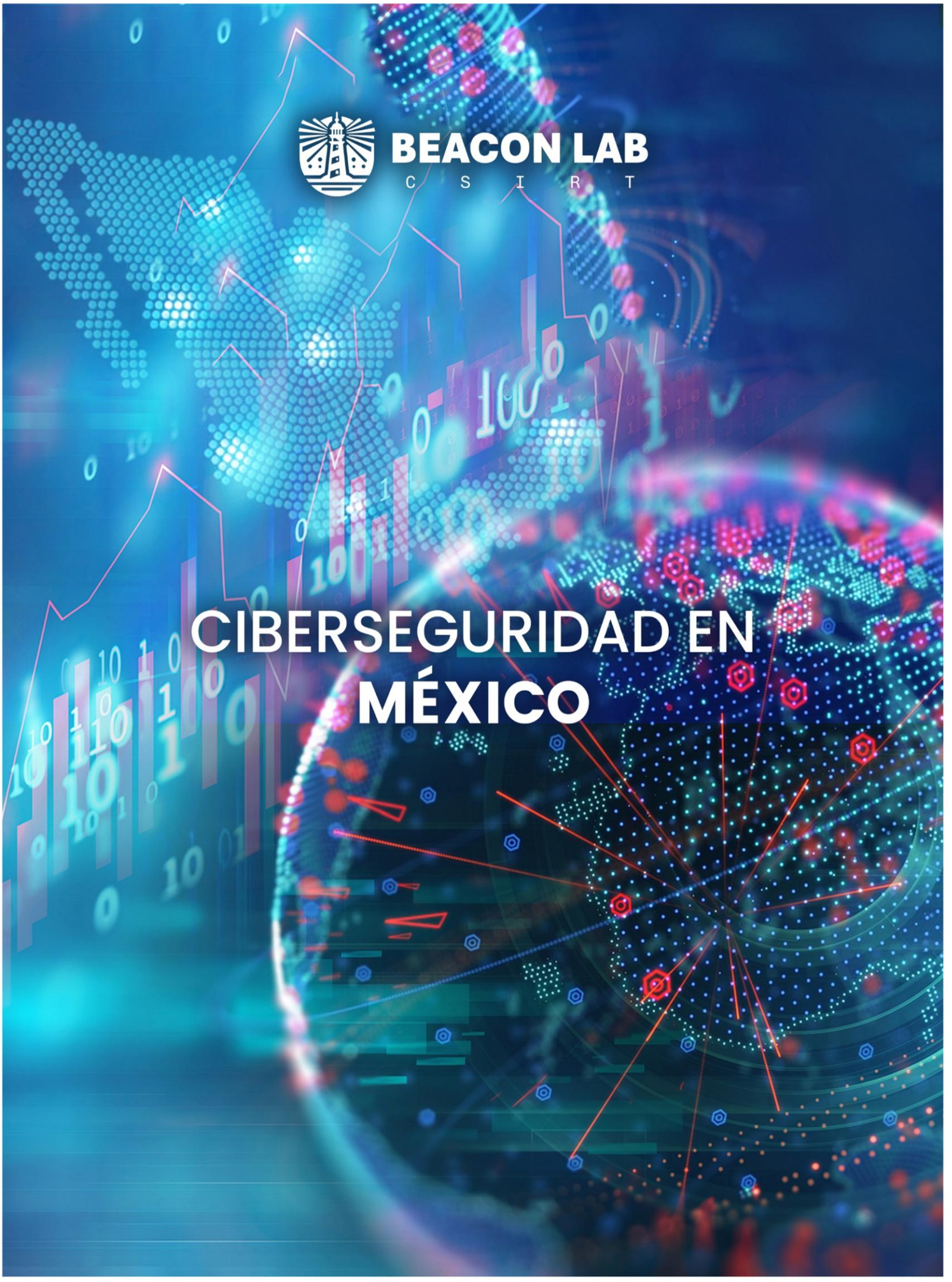

BEACON LAB
C S I R T
CIBERSEGURIDAD EN
MÉXICO

CIBERSEGURIDAD EN MÉXICO: ¿DÓNDE ESTAMOS Y HACIA DÓNDE VAMOS?

Actualmente, México enfrenta una situación complicada en cuanto a ciberseguridad. Por un lado, el país se ha convertido en un atractivo para los ciberdelincuentes, debido a su intensa actividad digital, un sector financiero en crecimiento y una relativamente baja madurez en la cultura de seguridad cibernética. Además, las leyes en este campo están desactualizadas, lo que dificulta la respuesta efectiva ante las nuevas amenazas. Muchas empresas adoptan un enfoque reactivo, enfocándose en la seguridad solo después de haber experimentado un incidente, como un ataque de ransomware.

A pesar de ello, se observan avances y oportunidades. La concientización en la ciberseguridad ha ido incrementando tanto en el sector público como en el privado, lo que ha llevado a la implementación de varias iniciativas gubernamentales, como la creación de una ley de ciberseguridad y la de un Centro Nacional de Respuesta a Incidentes Cibernéticos.

Una buena cultura de seguridad cibernética a través de la educación sobre riesgos y mejores prácticas, modernizar la legislación para adaptarse a las nuevas amenazas, invertir en tecnología y fomentar la colaboración entre los sectores público, privado y académico, puede ayudar a mejorar la ciberseguridad en el país, y aunque esta no puede ser garantizada al 100%, es crucial reducir los riesgos y desarrollar la resiliencia necesaria para seguir operando tras un ataque.

En general, la ciberseguridad es un tema de vital importancia para las empresas en México. Mientras las grandes corporaciones han hecho avances significativos, las pequeñas y medianas empresas (PyMEs) todavía enfrentan grandes desafíos. En promedio, las empresas destinan entre el 5% y el 10% de sus presupuestos de tecnología de la información a ciberseguridad.

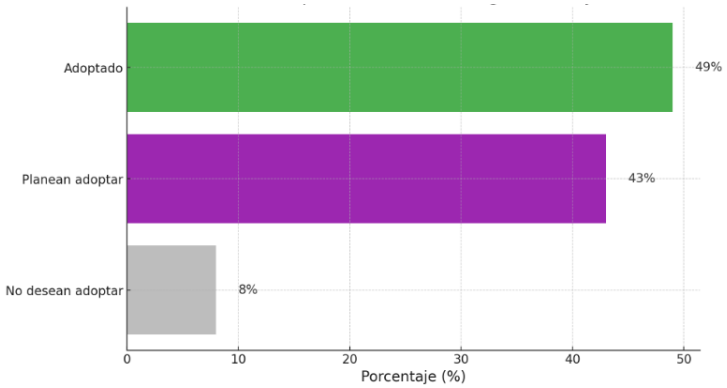
LA CIBERSEGURIDAD EN PEQUEÑAS, MEDIANAS Y GRANDES EMPRESAS

En México, las grandes empresas suelen tener mayor penetración en cuanto a medidas de ciberseguridad. Estas organizaciones, especialmente en sectores como banca, telecomunicaciones y retail, invierten considerablemente en tecnologías de protección, como firewalls, soluciones de antivirus, cifrado de datos y capacitación a sus empleados para reducir los riesgos. Esto se debe a que manejan una enorme cantidad de información sensible y, por lo tanto, son objetivos atractivos para los ciberdelincuentes.

Por otro lado, las medianas y pequeñas empresas aún tienen un largo camino por recorrer. Muchas de estas empresas no cuentan con recursos suficientes para invertir en herramientas avanzadas de ciberseguridad, lo que las deja más vulnerables ante ataques como ransomware o phishing. Sin embargo, la tendencia ha sido positiva. En 2022, el 71.9% de las MiPymes encuestadas consideraban que la ciberseguridad es "muy importante" o "importante", un aumento respecto al 61% en 2019. Específicamente, las micro y pequeñas empresas mostraron un gran avance, con un 84.3% que considera la ciberseguridad muy

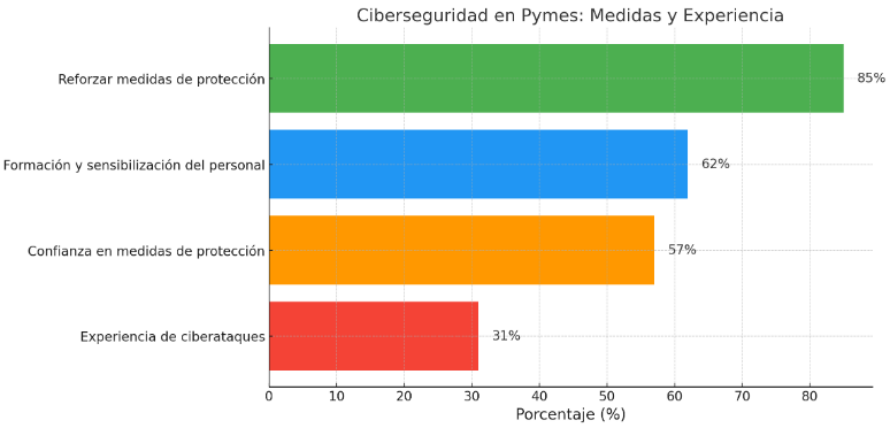
importante en 2022, comparado con el 60% en 2019. Para las medianas empresas, el aumento también ha sido positivo, aunque menos pronunciado.

La ciberseguridad se ha vuelto un aspecto esencial para empresas de todos los tamaños, ya que son vulnerables a ciberataques. Las empresas en Latinoamérica enfrentan un promedio de dos ataques de ransomware por minuto, con México en el tercer lugar de los países más atacados. Las pequeñas y medianas empresas (Pymes) están reconociendo la importancia de invertir en ciberseguridad, con un estudio que muestra que el 43% planeó implementar soluciones este 2024 y seguir con la misma tendencia para el 2025.



Nivel de adopción de soluciones de ciberseguridad en Pymes

Es de destacar la necesidad de que las Pymes adopten medidas de ciberseguridad, dado que solo el 49% ha implementado soluciones digitales en este ámbito. Se sugieren tres pasos clave para mejorar la ciberseguridad: usar contraseñas seguras y antivirus, capacitar a los empleados para detectar y prevenir ataques, y tener planes de respuesta ante incidentes. Además, el 85 % de estas empresas considera que deben reforzar sus medidas de **protección frente a vulnerabilidades y amenazas**. En un contexto donde las Pymes son fundamentales para la economía de México, es crucial que estén bien informadas y preparadas para enfrentar ciberataques.

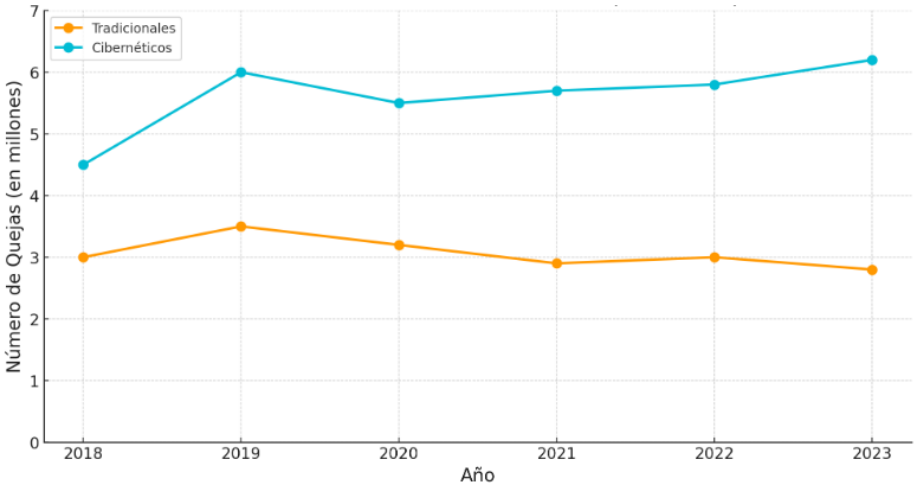


Porcentaje de medidas implementadas en Pymes

Incrementar la ciberseguridad no solo protege a las empresas de ataques, sino que también tiene un **impacto financiero** positivo. Mantener la **integridad de los procesos comerciales** y garantizar el **buen funcionamiento de las operaciones** es crucial para evitar pérdidas económicas y proteger la reputación de la empresa.

FRAUDES CIBERNÉTICOS Y TRADICIONALES

El panorama de la ciberseguridad no se limita a ataques complejos. Al cierre de 2023, las quejas por fraudes cibernéticos aumentaron un 20.1% respecto al mismo periodo de 2022. Esto representa una tendencia al alza: en 2018, el 59% de los fraudes reportados eran de origen cibernético, mientras que en 2023 la cifra subió a 71%. El monto reclamado por estos fraudes ascendió a 20,018 millones de pesos, con una resolución favorable para los usuarios en 70 de cada 100 casos.



Fraudes tradicionales vs cibernéticos

CIBERATAQUES A DISPOSITIVOS MÓVILES

El aumento de los ciberataques a dispositivos móviles en México refleja una tendencia preocupante en América Latina. En lo que va del año, México ha registrado 835,000 ciberataques a celulares, cifra que se espera que continúe incrementando, alcanzando el millón de ataques para 2025. Este incremento del 70% en comparación con años anteriores se debe a la creciente dependencia de los dispositivos móviles para actividades diarias, como compras, entretenimiento y acceso a servicios financieros, lo que aumenta la vulnerabilidad frente a los ciberdelincuentes.

Los tipos de ataques más comunes incluyen phishing, malware, y troyanos de acceso remoto (RATs). Los ataques de phishing buscan engañar a las víctimas para que proporcionen información sensible mediante mensajes fraudulentos que parecen legítimos. Los RATs tienen como objetivo las aplicaciones de banca digital, permitiendo a los atacantes acceder a cuentas bancarias sin ser detectados. Además, otro método utilizado es el intercambio de SIM, en el cual los atacantes toman control de la línea telefónica para recibir códigos de autenticación y acceder a las cuentas de las víctimas.

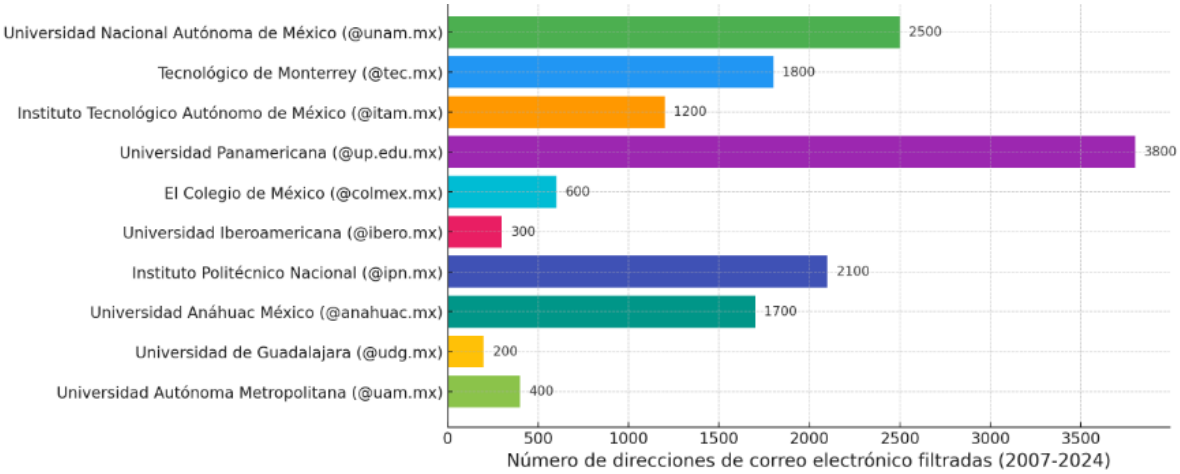
Los expertos advierten que los usuarios deben ser cautelosos con los enlaces y mensajes recibidos, especialmente en aplicaciones de mensajería como SMS o WhatsApp. Además, se recomienda siempre acceder a sitios web oficiales para evitar caer en estafas. La

educación y la configuración de privacidad y seguridad son esenciales para reducir los riesgos asociados a estos ataques.

EVALUACIÓN DE LA HIGIENE DIGITAL EN INSTITUCIONES EDUCATIVAS

Un estudio reciente ha analizado las direcciones de correo electrónico presentes en ficheros de contraseñas vulneradas (en su mayoría filtradas por infostealers) desde 2007, permitiendo evaluar la higiene digital de las principales instituciones mexicanas. Las universidades, al ser organismos de gran envergadura, también son un blanco común para los ciberdelincuentes.

En la siguiente imagen, se muestra el estado de la ciberseguridad de las 10 mejores universidades de México donde se visualiza el número de direcciones de correo electrónico comprometidas:



Número de correos electrónicos filtrados en las 10 mejores universidades de México

Entre el 1 y el 16 de octubre de 2024, se reportaron 10 filtraciones en diversas regiones de México. El sector educativo ha sido el más vulnerado en este periodo. Destaca la Ciudad de México con 12 incidentes reportados, seguida de Guanajuato con 3, y otras entidades como Sonora, Baja California y Estado de México con 1 incidente cada una.

¿CUÁNTO INVIERTEN LAS EMPRESAS MEXICANAS EN CIBERSEGURIDAD?

En general, los niveles de inversión en ciberseguridad varían según el tamaño de la empresa. Más del 64% de las empresas en México no tienen un presupuesto específico asignado a la ciberseguridad, y el 59% carece de un estándar o marco de referencia para su estrategia en esta área. Además, el 31% de las organizaciones, incluyendo grandes y medianas empresas, no cuenta con personal dedicado a ciberseguridad, y el 35% solo dispone de una persona especializada para estas tareas. Esto refleja una falta de recursos y planificación adecuados para proteger a las empresas de amenazas cibernéticas crecientes.

Para las pequeñas empresas, la inversión suele ser menor, tanto en porcentaje como en monto absoluto. Muchas veces, estas empresas optan por soluciones más económicas o subcontratan servicios de ciberseguridad para garantizar una protección básica. A medida que crece la conciencia de los riesgos digitales, se espera que estas inversiones sigan aumentando.

El panorama general de la ciberseguridad en México

A nivel nacional, México ha avanzado en la creación de regulaciones y leyes que promuevan la seguridad digital. Un ejemplo es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), que establece pautas claras para el manejo y protección de datos personales.

Las regulaciones sobre ciberseguridad serán cada vez más estrictas, requiriendo a las empresas información sobre su infraestructura y planes de seguridad. Un ciberataque a una pyme puede tener graves consecuencias económicas y de reputación, con un estudio de Google indicando que el 49% de las pymes han enfrentado problemas de ciberseguridad, y el 70% ha experimentado robos de información o pérdida de datos. México es un país vulnerable, con un 23% de los ciberataques en América Latina y ocupando el puesto 15 en delitos cibernéticos.

Todavía queda mucho por hacer en términos de adopción y cumplimiento, especialmente en el sector PyME, donde muchos aún consideran la ciberseguridad como un gasto opcional. Con la transformación digital acelerada por la pandemia de COVID-19, el uso de herramientas en la nube y el trabajo remoto, las vulnerabilidades han crecido, lo que hace más urgente que nunca que las empresas refuercen sus defensas.

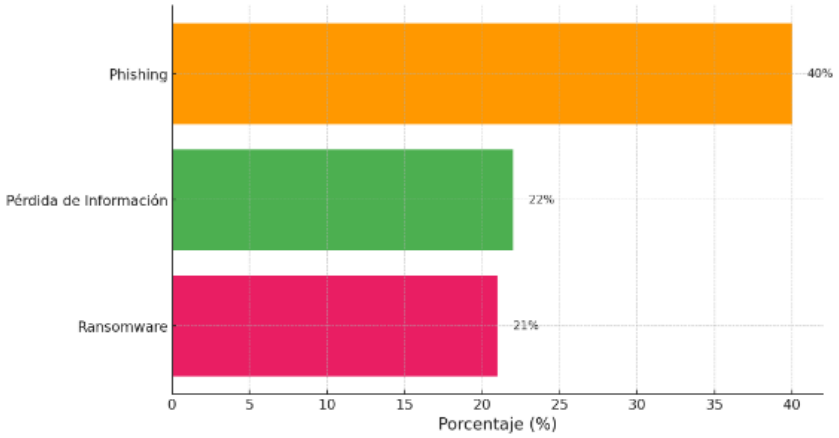
Tener un programa de ciberseguridad no es solo una opción, sino una necesidad creciente para las pequeñas y medianas empresas (pymes) que utilizan herramientas de inteligencia artificial, tienen presencia en internet, digitalizan sus procesos o manejan datos de clientes y proveedores.

Principales amenazas que enfrentan las empresas mexicanas

En México, el **phishing** ha sido el ataque más detectado por las empresas durante los últimos 18 meses, representando el **40%** de los incidentes reportados. Este ataque se basa en engañar a los usuarios para que proporcionen información confidencial, generalmente mediante correos electrónicos o mensajes fraudulentos que simulan ser de fuentes legítimas.

Otros incidentes destacados incluyen la **pérdida de información** (22%) y los **ataques de ransomware** (21%), que también afectan gravemente la operatividad de las organizaciones. La pérdida de información puede resultar en sanciones regulatorias y dañar la reputación, mientras que el ransomware cifra la información y exige un rescate para liberarla.

Además, el phishing y los **fraudes financieros** son los incidentes que más han interrumpido las operaciones empresariales. Estos fraudes incluyen esquemas que buscan obtener acceso a cuentas o realizar transferencias fraudulentas. Para mitigar estos riesgos, es esencial que las empresas capaciten a sus empleados, implementen medidas de detección de amenazas y apliquen prácticas de seguridad sólidas, como la autenticación multifactor. La preparación y la concienciación son clave para enfrentar estas amenazas crecientes.



Top 3 incidentes detectados por empresas en los últimos 18 meses en México

RETOS Y OPORTUNIDADES HACIA EL FUTURO

Uno de los principales retos es la falta de personal capacitado en ciberseguridad. Aunque existen programas y certificaciones en el país, la demanda de profesionales supera con creces la oferta, lo que complica a las empresas encontrar talento adecuado para proteger sus activos digitales ante amenazas cada vez mas avanzadas.

A pesar de estos desafíos, el crecimiento en la adopción de tecnologías emergentes, como inteligencia artificial y blockchain, ofrece oportunidades para mejorar la ciberseguridad en México. Muchas empresas están comenzando a explorar el uso de estas tecnologías para identificar amenazas de manera proactiva y responder a ellas más rápidamente.

CONCLUSIÓN

La ciberseguridad es un aspecto crítico para las empresas en México, independientemente de su tamaño. Aunque las grandes empresas han avanzado significativamente en la implementación de medidas de protección, las PyMEs aún tienen un reto importante por delante. Con el aumento de los ciberataques y la transformación digital, es vital que todas las organizaciones, desde las más grandes hasta las más pequeñas, tomen medidas para proteger sus datos y asegurar su futuro en el mundo digital.

REFERENCIAS:

- Ciberataques a celulares aumentarán a un millón para 2025
- Ciberseguridad en México: entre la inmadurez y la conciencia
- condusef.gob.mx/documentos/comercio/FraudesCiber-4toTrim2023.pdf
- 5 ciberataques más comunes a los celulares en México
- 64% deempresas en México no asigna recursos a ciberseguridad
- Ciberseguridad, el desafío de las Pymes mexicanas – El Financiero
- Panorama de la ciberseguridad en las pymes para el 2024
- https://www.movistar.com.mx/empresas/resultados-SondeoME

info@beaconlab.mx

contact@cybolt.com

beaconlab.mx

cybolt.com

BEACON LAB
C S I R T

CYBOLT
Security Innovation