SEGURIDAD DE LA INFORMACIÓN, EL GRAN DESAFÍO

GASTO MUNDIAL DE LOS USUARIOS FINALES EN SEGURIDAD Y GESTIÓN DE RIESGOS ASCENDERÁ A LOS 215 MIL MDD EN 2024, UN AUMENTO DEL 14,3% CON RESPECTO A 2023: GATNER

ROSA MARÍA VERJÁN

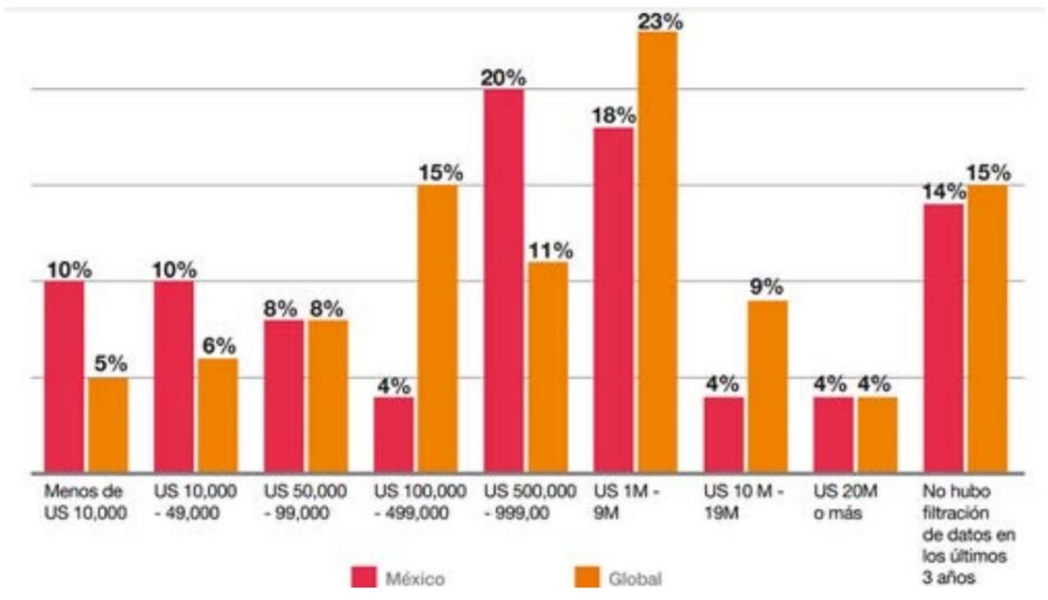
La vulnerabilidad en la que se encuentran tanto usuarios como empresas en materia de ciberseguridad aún es grande, por ello, es necesario identificar cualquier tipo de amenaza que pueda poner en peligro la información que manejamos tanto a nivel personal como público.

La desinformación, así como la inseguridad cibernética son dos de los riesgos más importantes que pueden padecer tanto las empresas, como la sociedad en general, esto, según el Reporte Global de Riesgos 2024 del Foro Económico Mundial, que realizó en colaboración con Zurich y Marsh McLennan.

Incluso, estudios revelan que la cantidad de datos que se crean, capturan, copian y consumen a nivel mundial cada año es de 97 zettabytes, una cifra que se prevé que aumente a 181 zettabytes para 2025. Búsquedas de Google, mensajes de texto, imágenes publicadas en las redes sociales y compras online: todos esos datos generan un universo de información que puede ser utilizada de manera positiva o negativa.

Si nos vamos por el ámbito empresarial, el estudio El estado de la ciberseguridad Latinoamérica 2024, de ManageEngine, la división de gestión de TI empresarial de Zoho Corp., refiere que los ataques cibernéticos en 2023 aumentaron considerablemente.

Andrés Mendoza, director técnico para LATAM y el sur de Europa de la compañía, apuntó que ante este panorama "es esencial pensar más allá de los paradigmas de seguridad tradicionales, adoptar marcos integrales de ciberseguridad y explorar estrategias innovadoras para anticiparnos a las tendencias emergentes, salvaguardando la confianza que los clientes depositan en la organización".



FUENTE: DIGITAL TRUST INSIGHTS 2024, EDICIÓN MÉXICO, PWC

De aquí podemos hablar de la relevancia que tiene el papel del profesional en tecnología, pero también el foco que las compañías le dan al tema de la seguridad en internet. De hecho, el estudio de Kaspersky The portrait of modern information security profesional, indica que más del 70% de las empresas destinan anualmente más de 100 mil dólares en formación para mantener al día los conocimientos de dichos colaboradores.

Veniamin Levtsov, vicepresidente del Centro de Experiencia en Negocios Corporativos de Kaspersky asegura que "el desarrollo de especialistas de alto perfil dentro de la empresa y la creación de experiencia interna puede resultar en una estrategia eficaz para las organizaciones que pretenden retener a los empleados existentes y permitirles crecer profesionalmente".

Relacionado con lo anterior, la Inteligencia Artificial cobra un papel relevante, puesto que especialistas y empresarios aseguran que esta herramienta les permitiría "implementar cambios adecuados, manejar respuestas a ataques y realizar otras tareas sin la necesidad de una revisión manual antes de la implementación de las estrategias de ciberseguridad".

Subin George, gerente de operaciones regionales para LATAM de ManageEngin expuso que es evidente cómo es que en nuestro país el uso de la IA es ya una realidad en el combate a las amenazas cibernéticas. Por supuesto, dijo, esto debe de ir acompañado de protocolos de seguridad sólidos y soluciones integrales, pero a la vez, "fomentar una cultura de concienciación sobre la ciberseguridad entre los empleados. Al incorporarla en la cultura de cualquier organización, podemos mitigar eficazmente el riesgo de ciberamenazas".

Según Statista Market Insights, el mercado mexicano de Inteligencia Artificial alcanzará un valor de 3,700 millones de dólares en 2024, un incremento del 30% con respecto al año previo, cuando su valor fue de 2,820 millones de dólares. Se espera que, en 2030, 8.4 millones de personas utilicen esta tecnología en México, cuyo valor rozará los 10 millones de dólares.

Para Jaime Balañá, director Técnico de NetApp para Iberia y Latam, "las empresas que manejan adecuadamente sus datos, conectando y unificando diversos conjuntos de datos estructu-

rados y no estructurados mediante una infraestructura inteligente, se encuentran en una posición de ventaja para conseguir los mejores resultados en la era de la IA".

Además, especialistas de EPAM Systems Inc., "El cambio hacia la IA requiere un cambio de paradigma en cómo percibimos la seguridad de datos y la gestión de riesgos. Es crucial para las empresas: a) tener en cuenta aceptar la naturaleza de 'escala de grises' de la seguridad de IA, reconociendo que las visiones binarias de la seguridad de los datos son insuficientes; b) equilibrar la innovación con la mitigación de riesgos, asegurando que las exploraciones en IA no comprometan la seguridad de los datos; c) revisar estrategias de seguridad: adoptar enfoques de ciberseguridad multifacéticos y ágiles que evolucionen con la tecnología".

Pensando en la cantidad de información que se concentra actualmente en la nube, la atención también debe estar puesta ahí, pues si bien, una de las ventajas es que se puede acceder a esos datos desde cualquier lugar, e incluso, es más económico para las compañías que tener grandes servidores, los problemas de seguridad también existen ahí. Según las investigaciones de PwC, pese a que los ataque en la nube son una preocupación, cerca de un tercio de las organizaciones en el mundo no cuentan con un plan de gestión de riesgos para enfrentar los desafíos de los proveedores de servicios en la nube.

EN AMÉRICA LATINA, EL 51% DE LOS PROFESIONALES ESTÁ DISPUESTO A PAGAR CURSOS DE FORMACIÓN ADICIONALES PARA SEGUIR SIENDO COMPETITIVOS EN EL MERCADO: KASPERSKY.

Cabe destacar que, "si bien, tecnologías como el cómputo en la nube representan un motor de crecimiento, también imponen un riesgo y aumento de vulnerabilidades cibernéticas importantes".

Por otro lado, si consideramos los resultados que arrojó el estudio Digital Trust Insights 2024 de PwC, 5 de cada 10 empresas mexicanas tuvieron pérdidas de hasta 999 mil dólares como resultado de una filtración de datos en los últimos tres años.

Es una realidad que el tema de la ciberseguridad empresarial ya va más allá de sólo tener un área de TI, es crucial generar estrategias acordes a las necesidades de cada empresa, considerando el sector y el tamaño de la misma.

No debemos perder de vista que los problemas y ataques cibernéticos además de vulnerar la Información significan pérdidas económicas qué a veces se forman incuantificables. De hecho, empresas encuestadas por PwC refirieron que en los últimos tres años, el costo por la filtración de datos estuvo entre 1 y 9 millones de dólares.

Finalmente, cabe señalar que datos de la Universidad de Guadalajara y de la Dirección General Científica de la Guardia Nacional revelan que de septiembre de 2020 a abril de 2022 se atendieron 34 mil reportes ciudadanos en materia de ciberseguridad, principalmente relacionados con secuestro de datos bancarios, institucionales o personales.