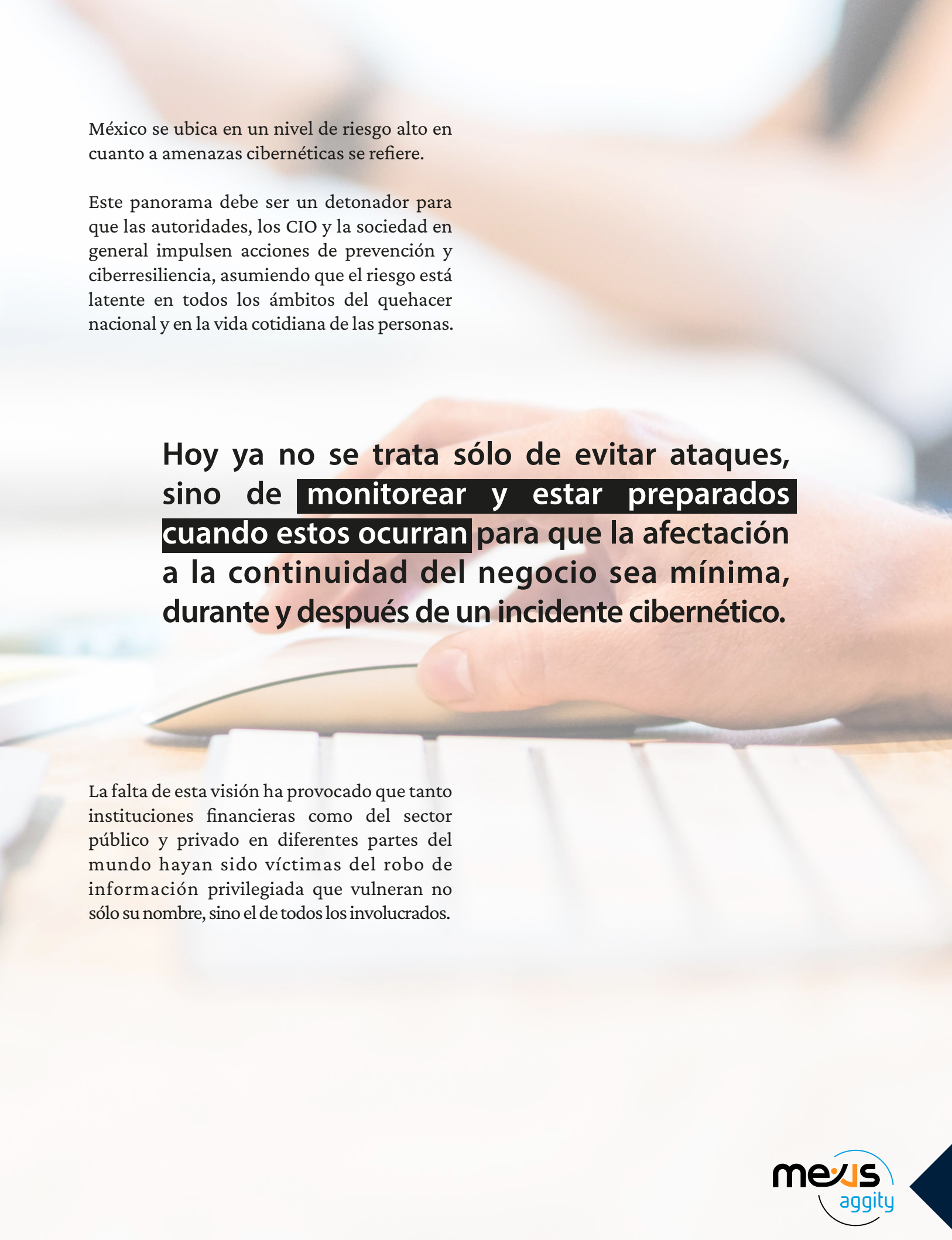
¿Cómo pueden los CIO protegerse de los ciberataques?

> En los últimos meses, el robo y la filtración de datos de organizaciones públicas y privadas han sido una constante en México y en el mundo. **Sin importar el nivel de seguridad** que presumiblemente se tenga, los ciberdelincuentes han logrado inmiscuirse dentro de los sistemas para extraer información confidencial, un delito que en América Latina deja pérdidas de **2.09 millones de dólares,** de acuerdo a un estudio.

Los ciberdelincuentes han encontrado en el robo de información una manera más efectiva para hacer daño a sus blancos de ataque, porque más allá de lo económico, las organizaciones pierden la confianza y credibilidad de sus usuarios, mientras que los agentes maliciosos ganan reputación entre el gremio ilegal.

Así, durante este tiempo, las diferentes filtraciones de seguridad en México han evidenciado, una vez más, la necesidad de priorizar la inversión en ciberseguridad y en la protección de los datos en todos los ámbitos tantos públicos como privados, ya que nuestro país sigue siendo vulnerable ante la falta o laxitud de leyes que tipifiquen los diversos tipos de ciberdelitos, así como las penas para su sanción correspondiente.



México se ubica en un nivel de riesgo alto en cuanto a amenazas cibernéticas se refiere.

Este panorama debe ser un detonador para que las autoridades, los CIO y la sociedad en general impulsen acciones de prevención y ciberresiliencia, asumiendo que el riesgo está latente en todos los ámbitos del quehacer nacional y en la vida cotidiana de las personas.

Hoy ya no se trata sólo de evitar ataques, sino de monitorear y estar preparados cuando estos ocurran para que la afectación a la continuidad del negocio sea mínima, durante y después de un incidente cibernético.

La falta de esta visión ha provocado que tanto instituciones financieras como del sector público y privado en diferentes partes del mundo hayan sido víctimas del robo de información privilegiada que vulneran no sólo su nombre, sino el de todos los involucrados.

De hecho, el robo de datos personales es la principal preocupación de las personas usuarias de internet. El 18° Estudio sobre los Hábitos de Personas Usuarias de Internet en México 2022, de la Asociación de Internet MX, refiere que aproximadamente 7 de cada 10 internautas se encuentran preocupados por la filtración de su información, seguido de la posibilidad de recibir un virus y la invasión a su privacidad con 37.8% y 29.1%, respectivamente

Frente a ello, ¿qué pueden hacer los CIO?
Para mitigar estas cifras, los CIO tienen la titánica tarea de hacer la diferencia en ciberseguridad, implementando estrategias eficaces de ciberresiliencia.

El plan debe estar diseñado con base en un análisis de riesgos real, ya sea propio o asistido por algún aliado idóneo, que además realice una evaluación de su nivel de madurez de seguridad informática, a fin de solventar las áreas de oportunidad y proteger la información crítica ante los inminentes ciberataques. Otro punto fundamental es la implementación de Gestión de Accesos Privilegiados (PAM) para contrarrestar el uso indebido de privilegios o el robo de credenciales, muchas veces obtenidas con técnicas de ingeniería social, basadas en la falta de adopción de prácticas seguras de protección o ciberhigiene de las personas.

Por ello, finalmente, es importante incluir tareas de concientización sobre las ciberamenazas, considerando que el fallo humano es el eslabón más débil de seguridad. Bajo esa óptica, desde 2004, cada octubre se conmemora a nivel global el mes de la Ciberseguridad, instaurado para prevenir e informar sobre las amenazas existentes en la web.

Fuente de información: cio.com.mx