www.mexis.net

REGULACIÓN EN EL SECTOR FINANCIERO IMPULSA LA CIBERSEGURIDAD

Para lograr que se puedan prevenir ataques e incidencias más allá, se debe contar con visibilidad de todo lo que sucede en sus procesos.

Incidentes como la falla en los sistemas de Microsoft que generó afectaciones sobre las operaciones de empresas del sector aéreo, salud y financiero a nivel global, resaltó la importancia de contar con protocolos de ciberseguridad.

El sector financiero es uno de los sectores que lideran este tipo de estrategias maduras y resilientes ante incidentes, de acuerdo con lo mencionado por experto en ciberseguridad, **el segmento ha alcanzado dicha madurez impulsado por la regulación existente.**

“Las instituciones financieras en términos de ciberseguridad, están apalancadas o están soportadas sobre la necesidad de regulaciones. **Sin embargo, la regulación no significa seguridad.** Sí hay muchos casos también en los que empresas que son altamente reguladas y que tienen certificaciones de cumplimiento, han terminado siendo víctimas”, mencionó.

Experto explicó que para lograr que las financieras puedan prevenir ataques e incidencias más allá de lo que se encuentra previsto por la regulación, **deben contar con visibilidad de todo lo que sucede en sus procesos.**

“Las estrategias de ciberseguridad se deberían probar contra el fallo, **intencionalmente deberían asumir que está fallando y saber o tener el criterio para detectar dónde está fallando.** Es uno de los criterios para escoger una buena solución de ciberseguridad”, resaltó.

En materia de ciberseguridad, recientemente la Comisión Nacional Bancaria y de Valores (CNBV) modificó las Disposiciones Generales Aplicables a las Instituciones de Crédito. Además de establecer los lineamientos mínimos para un plan de gestión para prevenir el fraude, **la normativa busca prevenir la vulneración de los medios electrónicos** que son empleados por las instituciones.

Con relación a los planes normativos de ciberseguridad, la Comisión informó, en septiembre del 2023, que **se optaría por homogeneizar los estándares mínimos de ciberseguridad en vez de crear una circular única,** ya que las necesidades de las instituciones del segmento financiero son distintas.

Continuidad en nube

Por otra parte, en el incidente reciente los sistemas Microsoft se vieron impactados por la actualización que se realizó y no representaron una afectación directa a los servicios de nube que ofrece la tecnológica. Sin embargo, experto explicó que es importante para las firmas considerar en sus planes de continuidad la disponibilidad de la nube.

"En ambos casos, nube y actualización de los sistemas si llegará a fallar algo, se debe enfrentar. **Los responsables de la seguridad y de la infraestructura deben pensar en estrategias modernas que permitan ser resilientes y adaptables ante una contingencia que afecte la operación**", mencionó experto.

El especialista resaltó que **las estrategias deben ir más allá de mantener los sistemas modernos o actualizados,** los responsables deben entender el riesgo que representan los propios sistemas.
"Puedes tener el plan de contingencia, pero **una cosa es tener el plan de contingencia en papel y otra cosa es probar tu plan de contingencia** intencionalmente ante una situación", destacó.

La CNBV establece lineamientos a las instituciones financieras para operar a la nube e indicaciones sobre cómo las instituciones financieras pueden gestionar los riesgos, especialmente **se busca minimizar el impacto en las caídas de los servicios que proporcionan los proveedores de nube.**

Fuente de información:
eleconomista.com.mx