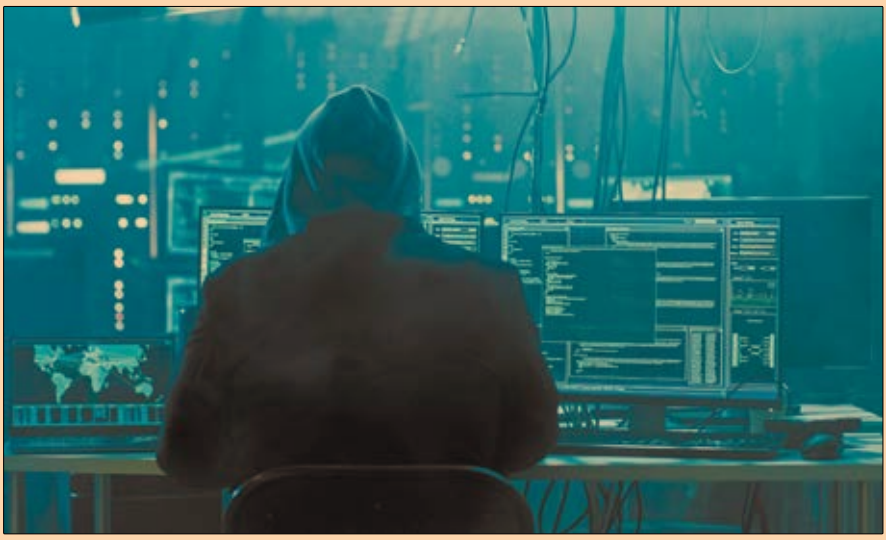

Los bancos deben realizar pruebas de penetración en sus sistemas a través de la contratación de los llamados *hackers* éticos. FOTO: SHUTTERSTOCK

SE REQUIERE MÁS INVERSIÓN AL RESPECTO

Ciberseguridad, uno de los principales retos para la banca

De mayo a octubre se habría registrado al menos media docena de ciberataques al sistema financiero mexicano: CNBV

Edgar Juárez
EL ECONOMISTA

PARA EL sistema financiero este año estuvo marcado, entre otras cosas, por los ciberataques que sufrieron los sistemas de conexión al Sistema de Pagos Electrónicos Interbancarios (SPEI) de algunos bancos durante abril y mayo y que derivaron en pérdidas superiores a 300 millones de pesos.

Las autoridades y los propios bancos lo han reconocido: es un tema que llegó para quedarse, y por lo tanto las inversiones y la atención de este rubro son de los principales retos que enfrentan.

De acuerdo con un reciente reporte de Fitch Ratings, el sistema financiero de América Latina es un objetivo importante de los delitos cibernéticos con ataques que cuestan aproximadamente 809 millones de dólares anuales, según la Organización de Estados Americanos (OEA).

"Se calcula que el ataque cibernético a México ocurrido en abril del 2018 costó a la industria aproximadamente 400 millones de pesos, según el Banco de México (Banxico)", reportó.

Pero los bancos en México saben de esta problemática, saben que es constante, y que por lo tanto tienen que realizar inversiones millonarias en seguridad, tal y como lo ha sugerido la propia autoridad.

> *"Se calcula que el ataque cibernético a México ocurrido en abril del 2018 costó a la industria aproximadamente 400 millones de pesos, según el Banco de México".*
>
> **Fitch Ratings**

¿QUÉ SE ESTÁ HACIENDO?

Los ciberataques de abril y mayo derivaron en una serie de medidas por parte de la autoridad y los bancos en general, para tratar de combatir este delito, o al menos actuar a tiempo antes de que un posible ataque se propague o afecte al resto del sistema financiero.

Unos días después de los ataques, los integrantes del sistema financiero en su conjunto firmaron unas bases de colaboración que, entre otros puntos, obliga a los bancos a fortalecer sus áreas de ciberseguridad y actuar de forma rápida ante cualquier indicio de ciberataque.

Por ello, debe reaccionar de forma inmediata e informar a la autoridad de cualquier incidente, para que ésta a su vez dé la voz de alerta al resto del sistema.

Esto dio como resultado que, en julio y octubre pasado, cuando se *hackearon* los sistemas de la plataforma Bitso y Axa respectivamente, se informara de inmediato, se encendiera la alerta, y se evitara así un contagio al resto del sistema.

A decir de la Comisión Nacional Bancaria y de Valores (CNBV) de mayo a octubre, se habría registrado al menos media docena de ciberataques al sistema financiero mexicano, pero sin consecuencias mayores.

NUEVAS REGLAS

Como consecuencia también de estos ciberataques, apenas hace unas semanas la CNBV publicó reglas adicionales y más estrictas para la banca y disminuir con ello los intentos de ciberataques.

Entre éstas destacan: la existencia de un plan director de seguridad y que el oficial de seguridad pasa de un cuarto nivel, a reportarle directamente al director general de la institución financiera.

También se pide que los bancos contraten información de mercado sobre ataques cibernéticos, a fin de saber cuáles son las tipologías más comunes; que haya controles de confianza para el personal, y realizar pruebas de penetración, con la contratación de los llamados *hackers* éticos, que son los que,contratados por los bancos, intentan vulnerar los sistemas y con ello saber las debilidades y fortalezas.

No obstante, las autoridades coinciden en que una mayor inversión en sistemas de seguridad es la clave para combatir el mal de los ciberataques.