

Crean frente nacional sobre ciberseguridad

Edgar Juárez Y Fernando Gutiérrez / El Economista

MEADE PRESENTA LOS CINCO PRINCIPIOS BÁSICOS

Firman gobierno y sectores declaración con sus compromisos.

A la par que crece la innovación tecnológica en los sistemas financieros, crecen los ciberdelitos a través de estos canales.

De acuerdo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), en el primer semestre del año las reclamaciones por posibles fraudes financieros alcanzaron los 1.6 millones.

En el Foro de Ciberseguridad celebrado en Palacio Nacional, el secretario de Hacienda, José Antonio Meade, destacó que la inclusión financiera permite a muchos más mexicanos tener acceso a vehículos de ahorro, crédito y seguros.

"Y cuando estos dos mundos coexisten, el mundo digital y el de inclusión financiera, el beneficio para los mexicanos sin duda es cada vez mayor, como lo es la responsabilidad que tenemos de asegurar que esa participación, en esa dimensión, sea cada vez más segura", dijo.

Añadió: "Como es un entorno que cambia todos los días, todos los días las vulnerabilidades son distintas, la forma de los ataques es diferente. Exige el tener protocolos actualizados y el tener esta respuesta vigente".

En este sentido, el funcionario destacó que por primera vez la administración tiene ya una estrategia nacional en materia de ciberseguridad, misma que se trabajará sobre cinco principios básicos.

Con base en ello, entidades privadas como las asociaciones de Bancos de México, de Intermediarios Bursátiles, de Sociedades Financieras Populares, así como el Consejo Mexicano de Uniones de Crédito y la Confederación de Cooperativas de Ahorro y Préstamos, además de la Asociación Fintech de México, firmaron una Declaración de Principios para el Fortalecimiento de la Ciberseguridad para la Estabilidad del Sistema Financiero Mexicano.

Estos principios son: adoptar y mantener actualizadas las políticas, métodos y controles para identificar, evaluar, prevenir y mitigar los riesgos de ciberseguridad, que se autoricen por los órganos de gobierno de mayor decisión y permeen a todos los niveles de la organización.

También: establecer mecanismos seguros para el intercambio de información entre los integrantes del sistema financiero y las autoridades, sobre ataques

ocurridos en tiempo real y su modo de operación, estrategias de respuesta, nuevas amenazas, así como del resultado de investigaciones y estudios, que permitan a las entidades anticipar acciones para mitigar los riesgos de ciberataques; lo anterior, protegiendo la confidencialidad de la información.

De igual forma: impulsar iniciativas para actualizar los marcos regulatorios y legales que den soporte, y hagan converger las acciones y esfuerzos de las partes, considerando las mejores prácticas y acuerdos internacionales.

Asimismo, colaborar en proyectos para fortalecer los controles de seguridad de los distintos componentes de las infraestructuras y plataformas operativas que soportan los servicios financieros del país, promoviendo el aprovechamiento de las tecnologías de información para prevenir, identificar, reaccionar, comunicar, tipificar y hacer un frente común ante las amenazas presentes y futuras.

Y finalmente, fomentar la educación y cultura de ciberseguridad entre los usuarios finales y el personal de las propias instituciones que, a través de una capacitación continua, redunde en una participación activa para mitigar los riesgos actuales de ciberataques.

“Hemos pasado poco a poco de vivir en un mundo donde las respuestas eran específicas, eran a bote pronto, eran de manera ad hoc al riesgo o al ataque puntual que habíamos enfrentado. a un mundo, a un marco regulatorio, en el que tenemos un enfoque sistémico, en donde de manera clara lo enfrentamos como una estrategia, en donde, sabiendo que habrá ataques, nos anticipamos para poder tener ante ellos una capacidad de respuesta ordenada, un protocolo claro, una forma de dar seguridad a quien se ubica y se desempeña en este entorno, de que sus transacciones, su información, su dinero, sus recursos, están debidamente protegidos”, concluyó.