SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

FORO CIBER SEGURIDAD

CNBV COMISIÓN NACIONAL BANCARIA Y DE VALORES

"Fortaleciendo la ciberseguridad para la estabilidad del Sistema Financiero Mexicano"

Con la participación de representantes de las instituciones financieras, industria tecnológica, academia y asociaciones gremiales, además de expertos nacionales e internacionales, el pasado 23 de octubre se realizó en Palacio Nacional el primer Foro de Ciberseguridad cuyo objetivo fue poner sobre la mesa de análisis el fenómeno de seguridad en las tecnologías de información, para generar conciencia y una cultura de prevención tanto en las instituciones que conforman el sistema financiero mexicano, como en sus usuarios.

En la inauguración del Foro, participaron el Secretario de Hacienda y Crédito Público, el Doctor José Antonio Meade Kuribreña, el Subgobernador del Banco de México, el Maestro Alejandro Díaz de León y el Presidente de la Comisión Nacional Bancaria y de Valores (CNBV), el Maestro Jaime González Aguadé. Durante la sesión, las autoridades comentaron sobre la relevancia del tema para el sector financiero ya que a diferencia de otros sectores, los ataques cibernéticos ponen en riesgo no sólo la información de los usuarios, sino también, el patrimonio de los depositantes. Se destacó que las autoridades financieras han puesto especial interés en la regulación para que ésta incorpore mejores prácticas y recomendaciones internacionales.

El tema de seguridad es muy amplio y se basa en gran parte en la comunicación y cooperación de todos los participantes en la industria; por ello, durante el foro se firmó la declaración de los principios para el fortalecimiento de la ciberseguridad. Esto representa un esfuerzo pionero que permitirá a todos los participantes del sistema financiero mexicano, autoridades y entidades del sector privado, trazar una agenda y coordinar esfuerzos.

Durante el evento se contó con la ponencia magistral del Doctor Earl Crane, Fundador y Director General de Emergent Network Defense. El Dr. Crane, quien también fue Director de Política de Ciberseguridad en el Consejo Nacional de Seguridad durante la administración del Presidente de EUA, Barack Obama, recalcó sobre la relevancia de concientizar el manejo y administración de los ciberriesgos y el papel de los reguladores, temas que resonaron en las distintas sesiones del Foro. Por su parte, los tres diferentes paneles abordaron las temáticas de la ciberseguridad y la estabilidad del sistema en el sector de la banca múltiple, las alternativas de seguridad para medios electrónicos y los retos para el desarrollo del sector FinTech en un ambiente seguro.

Principios para el Fortalecimiento de la Ciberseguridad para la Estabilidad del Sistema Financiero Mexicano

1. Adoptar y mantener actualizadas 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.
2. 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.
3. 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.
4. 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.
5. 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.

Se adhirieron a los principios, la Asociación de Bancos de México, la Asociación Mexicana de Intermediarios Bursátiles, la Asociación Mexicana de Sociedades Financieras Populares, el Consejo Mexicano de Uniones de Crédito, la Confederación de Coativas de Ahorro y Préstamo de México, y la Asociación Fintech de México.

De las sesiones del foro, destacan cinco grandes temas de discusión:

1) La importancia de la **colaboración** entre todos los actores, incluyendo a las instituciones financieras, proveedores, autoridades y clientes. Se discutió la necesidad de no ver la ciberseguridad como una ventaja competitiva que inhiba la comunicación sobre experiencias y mejores prácticas ya que el compartir información mejora significativamente la habilidad de las instituciones financieras de defenderse. Sin embargo, esta colaboración no puede basarse en la voluntad de las propias instituciones para compartir información, sino que debe estar basada en procedimientos formales y ocurrir a través de canales establecidos.

2) Se destacó el **rol del regulador** para lograr la participación adecuada. En este contexto y dado el componente transfronterizo de las transacciones financieras digitales, se denotó el rol del regulador para fomentar el desarrollo de un marco legal que elimine la sensación de impunidad al dificultarse la persecución de estos criminales entre países, así como desarrollar un marco regulatorio adecuado para que las instituciones con operaciones globales no se vean en la complejidad de cumplir con diferentes requerimientos regulatorios.

3) La importancia de la **confianza** en el Sector Financiero. Se destacó que, conforme se va transformando y digitalizando la relación con los clientes, se tiene que avanzar, también, en generar la confianza en los procesos digitales para que todos los participantes en el sector financiero puedan realizar transacciones y operar en condiciones de seguridad y certeza.

4) Las organizaciones deben estar listas para actuar. El cibercrimen es un **riesgo latente** por lo que hay que estar listos para cuando suceda. Por ello la agilidad y la capacidad de detectar temprano vulnerabilidades en los sistemas de defensa son fundamentales. Se requiere tener mecanismos para protegerse y para detectar posibles fallas y vulnerabilidades en los sistemas de información, así como contar con mecanismos de respuestas.

5) Finalmente, se tocó el tema de la **educación** de ciberseguridad desde dos puntos vista. Por un lado, se denotó la importancia de sensibilizar, informar y entrenar a los clientes y a los empleados de las propias instituciones financieras. Por otra parte, se destacó la necesidad de desarrollar talento en materia de ciberseguridad. Al respecto, se hizo un llamado para trabajar de la mano con las universidades para generar un mayor interés y mayor flujo de estudiantes interesados en participar en estos temas.

En la clausura y para resumir los aprendizajes del Foro, el Presidente de la CNBV conversó con el ponente magistral. En sus conclusiones ambos resaltaron la importancia de la detección temprana y de trabajar de manera conjunta para mejorar la predicción de los ataques; desarrollando la capacidad de identificar las tendencias de hacia dónde va la tecnología y los atacantes ya que sólo de esa manera se podrá ir un paso delante de ellos.