Palabras del Lic. Alejandro Díaz de León, Subgobernador del Banco de México, durante el foro "Fortaleciendo la ciberseguridad para la estabilidad del sistema financiero mexicano".

23 de octubre de 20017, Ciudad de México

Muy estimados

Dr. José Antonio Meade Kuribreña, Secretario de Hacienda y Crédito Público;

Lic. Jaime González Aguadé, Presidente de la Comisión Nacional Bancaria y de Valores;

Señoras y señores:

Es un honor participar en el Foro "Fortaleciendo la ciberseguridad para la estabilidad del Sistema Financiero Mexicano", que organiza la Comisión Nacional Bancaria y de Valores.

Las nuevas tecnologías brindan una oportunidad única para ampliar la cobertura del sistema financiero, agilizar las operaciones y diseñar nuevos productos. Gracias a la tecnología, se han logrado avances extraordinarios en materia de inclusión financiera, promoviendo, con ello, mayor equidad de oportunidades y mejores condiciones de desarrollo para millones de personas.

Sin embargo, estas tecnologías conllevan riesgos intrínsecos y plantean retos para garantizar la seguridad de los usuarios, las instituciones y el sistema en general.

Los riesgos cibernéticos son de naturaleza cambiante y su creciente sofisticación, frecuencia y persistencia puede perturbar considerablemente al sistema financiero tanto por su efecto directo en las instituciones, como por el alto grado de interconexión entre ellas.

Así, los delitos cibernéticos y los ataques a las infraestructuras tecnológicas del sistema financiero no sólo generarían pérdidas de información o patrimoniales para clientes e instituciones, también podrían provocar afectaciones al sistema financiero en su conjunto.

De ahí la importancia, como lo hace este Foro, de analizar las distintas dimensiones del reto de la ciberseguridad, intercambiar experiencias entre diversos integrantes del sistema y coordinar esfuerzos a todos los niveles para la prevención y mitigación de riesgos.

A continuación, destacaré algunos de los retos que enfrentamos en materia de ciberseguridad y la necesidad de una estrategia integral para superarlos.

La magnitud de los retos

Las amenazas a la ciberseguridad del sistema financiero se han multiplicado en los últimos años. Éstas son de distinta índole e involucran daños considerables tanto a corporaciones como a personas en su patrimonio y en el uso de su información.

Estos incidentes rebasan fronteras y constituyen un desafío global. Por mencionar algunos ejemplos, en 2016, tras un periodo de incubación, delincuentes cibernéticos lograron vulnerar los sistemas informáticos del banco central de Bangladesh y extrajeron 81 millones de dólares de sus cuentas en la Reserva Federal de Nueva York. Si bien esto fue un evento aislado, demostró la capacidad de afectar todo tipo de instituciones.

De igual manera, en mayo de 2017, se presentó un secuestro de información a instituciones de varios países, mediante el virus conocido como WannaCry, que afectó a las computadoras encriptando su información y solicitando un rescate para liberarla. Este ataque destaca por su dimensión internacional, el amplio rango de usuarios afectados y la sofisticación del método utilizado para penetrar los filtros de seguridad.

En estos y otros casos de ciberataques pueden encontrase denominadores comunes, uno de ellos es que pueden originarse en descuidos aparentemente menores, como el de un empleado que abre un correo sin identificar la fuente adecuadamente, otro radica en el hecho de que los ataques pueden incubar por largo tiempo dentro de los sistemas de la institución para estudiar cómo ocasionar el mayor daño.

Además de estos sucesos de alto impacto, los delitos comunes, como el *phishing* o la suplantación de identidad, amenazan el patrimonio de usuarios y podrían generar desconfianza en los procesos más modernos del sistema financiero.

Una estrategia integral

Por todo lo anterior, es imprescindible adoptar una estrategia integral que fortalezca nuestra capacidad para detectar, contener y mitigar los ciberataques.

Especialmente si consideramos que la ciberseguridad no sólo entraña un reto tecnológico, sino para toda la organización corporativa y su personal, así como de concientización e información a los consumidores. Además, se debe tener especial cuidado en las redes y la interconexión entre instituciones.

Por tanto, para promover la seguridad del sistema financiero y su pleno desarrollo se requiere trabajar en la totalidad del ecosistema, a tres niveles:

1. en las instituciones,
2. en las redes de interconexión y,
3. en favor de los usuarios o consumidores.

A nivel institucional, deben adoptarse las mejores prácticas en aspectos como:

1. la gobernanza del sistema de seguridad, que debe contemplar la responsabilidad al más alto nivel corporativo,
2. la protección de datos en todas las unidades,
3. los controles de identidad, acceso y la segregación de funciones,
4. la coordinación con terceros relacionados (proveedores),
5. la protección de equipos de cómputo y centros de datos,

6. el resguardo de la red de comunicación,
7. una cultura de seguridad proactiva que mejore la capacidad de respuesta ante eventuales incidentes, y
8. muy importante, la concientización y capacitación tanto de los operadores de procesos críticos como del personal en general.

A nivel de redes de interconexión, y considerando los potenciales riesgos sistémicos, deben prevalecer criterios de seguridad estrictos y acordes a las mejores prácticas. En este nivel la participación de las entidades reguladoras resulta clave.

Por ejemplo, en el sistema de pagos, el Banco de México ha emitido lineamientos precisos para mitigar el ciber-riesgo. Dichos lineamientos consideran aspectos como:

1. canales de comunicación dedicados y encriptados,
2. la obligación de contar con equipos de cómputo de uso exclusivo para el sistema de pagos,
3. la prohibición de conectividad a internet, y
4. el uso de la firma electrónica en las operaciones, entre otros.

Finalmente, a nivel del usuario, quien suele ser el eslabón más débil de la cadena y el más susceptible y sensible de afectaciones a su patrimonio, éste debe ser incorporado de manera activa a la estrategia integral de protección. Al respecto,

además de las medidas de protección al consumidor, las autoridades e instituciones deben facilitar procesos y proporcionar al público la formación e información necesaria para resguardar su ciberseguridad y prevenir los delitos más comunes.

Señoras y señores:

Es importante reiterar que las nuevas tecnologías, aplicadas al sistema financiero, brindan una oportunidad única, especialmente para las naciones emergentes, para abatir rezagos e incorporar a un mayor número de personas a los beneficios de la intermediación financiera moderna y coadyuvar, con ello, a elevar sus oportunidades de desarrollo y mejorar su calidad de vida.

Para ello, es imprescindible dar confianza a todos los participantes del sistema financiero y hacer frente a los retos de la ciberseguridad a través de soluciones integrales. Este Foro resulta significativo para este propósito, pues reúne autoridades, representantes de instituciones financieras y expertos nacionales e internacionales en la materia.

Adicionalmente, la firma de la “Declaración de principios para el fortalecimiento de la ciberseguridad y la estabilidad del Sistema Financiero Mexicano” es un esfuerzo pionero que permite trazar una agenda y coordinar esfuerzos entre autoridades y sector privado.

Considero que solo así, con el trabajo conjunto, será posible arraigar tanto al interior de las instituciones, como en el público en general, una cultura de ciberseguridad que ayude a desplegar cabalmente el potencial de la actual evolución tecnológica en favor de la inclusión y el desarrollo.

Muchas gracias y felicidades