

22 de mayo de 2018

Puntos Importantes sobre la Situación Actual del SPEI.

1. **Se tienen registrados 5 participantes con vulneraciones de ciberseguridad. Todos los ataques que se han observado han sido dirigidos hacia los bancos, casas de bolsa y otros participantes del sistema de pagos.** Estos han estado enfocados en los sistemas de los participantes con los que se conectan al SPEI.
2. **El sistema central del SPEI, que opera el Banco de México, no se ha visto afectado y no ha sido blanco de ningún ataque.** El sistema central opera de manera segura y eficiente como lo ha hecho desde su creación.
3. **Los recursos de los clientes de instituciones financieras están seguros, no estuvieron en peligro y no han sido el objetivo de los ataques.** Los recursos que se han extraído han sido de los participantes (bancos, casas de bolsa, etc.). Los atacantes han buscado vulnerar las conexiones de las instituciones con el SPEI, inyectando instrucciones de pago fraudulentas a partir de cuentas inexistentes, lo cual afecta la cuenta transaccional de los participantes en el SPEI, pero no las cuentas de los clientes finales. Los recursos de los clientes están seguros porque radican en un sistema separado con validaciones individuales por operación.
4. **Para salvaguardar la continuidad operativa, el Banco de México alertó a los participantes en el SPEI y solicitó a los participantes con un mayor perfil de riesgo migrar la operación a una plataforma contingente. Este esquema de operación contingente y las validaciones adicionales que han implementado los participantes han propiciado la ralentización de los flujos de pagos.**
5. Una vez recibidas en el SPEI, el 100% de las operaciones son procesadas y enviadas a los participantes receptores en segundos. Por otra parte, desde que se recibe la solicitud por parte de un cliente en los sistemas del participante hasta el abono final el 55% de las operaciones fluye por el sistema y los participantes con normalidad en cuestión de segundos, mientras que el 99% se opera en menos de dos horas. No obstante, en algunos casos estas acreditaciones pueden tardar uno o más días. **El Banco de México, consciente de la preocupación y malestar de los clientes, trabaja arduamente para que los participantes agilicen sus procesos para abonar en el menor tiempo posible los recursos de sus clientes y con ello minimizar la afectación a los mismos.**
6. **Con la información disponible, los montos involucrados en envíos irregulares y sujetos a revisión son de aproximadamente 300 millones de pesos.**

7. **Los participantes de SPEI tienen obligaciones de ciberseguridad establecidas en la regulación que emitió el Banco de México desde julio de 2017.** Las principales medidas en materia de seguridad debían estar aplicadas a finales de 2017. Cabe destacar que parte de la regulación emitida se refiere a los aplicativos que fueron vulnerados en algunos participantes.
8. **El Banco de México inició los procesos de supervisión para el cumplimiento de requerimientos de ciberseguridad durante 2017 detectando un nivel de cumplimiento heterogéneo.** A la fecha se tienen iniciados procesos de supervisión sobre el cumplimiento de requerimientos de ciberseguridad por parte de los participantes en diferentes sistemas del Banco de México.
9. **El Banco de México cuenta con esquemas de ciberseguridad que han venido fortaleciéndose en los últimos años,** los cuales incluyen auditorías internas y externas por parte de especialistas con reconocimiento internacional.
10. **El Banco de México emitió disposiciones que otorgan a las instituciones de crédito y demás entidades que prestan el servicio de transferencias de fondos, espacio para que estas implementen medidas de control adicionales encaminadas a fortalecer sus sistemas de detección de transferencias irregulares, verificar la integridad de sus operaciones y evitar posibles afectaciones a dichas instituciones, al resto de los participantes y al sistema en su conjunto. Adicionalmente, estas disposiciones consideran espacios para verificar la seguridad en los retiros de efectivo.**
 - **Circular 4/2018**
<http://www.banxico.org.mx/disposiciones/normativa/circular-13-2017/%7B5AB6422C-9129-C863-5F58-25737DA8766A%7D.pdf>
 - **Circular 5/2018**
<http://www.banxico.org.mx/disposiciones/normativa/circular-14-2017/%7B2C64D992-D986-9BCF-FD70-5AB2E70D70BA%7D.pdf>
11. **La seguridad de los datos personales que se encuentran en posesión del Banco Central con motivo de la operación del referido sistema pagos no ha sufrido vulneración alguna.** Al respecto, debe destacarse que el Banco de México tiene implementadas las medidas de seguridad necesarias para la debida protección de los datos personales y los recursos involucrados en su tratamiento, las cuales cumplen con los estándares nacionales e internacionales y buenas prácticas en la materia. Lo anterior, de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

De igual forma, ninguno de los participantes en el SPEI ha hecho del conocimiento de este Banco Central la existencia de algún tipo de vulneración a la seguridad de los datos personales en su posesión. Como se ha informado, los ciberataques que dichos participantes sufrieron buscaron afectar la cuenta transaccional de esas instituciones en el SPEI, no así las cuentas de los clientes finales. No obstante lo anterior, de detectarse algún caso de vulneración, dichos participantes deberán proceder de conformidad con lo dispuesto en Ley Federal de Protección de Datos Personales en Posesión de los Particulares y hacerlo del conocimiento de los titulares respectivos.