BANCO DE MÉXICO

16 de mayo de 2018

Estrategia de Ciberseguridad del SPEI

Banco de México ha adoptado varias medidas para fortalecer la ciberseguridad de los sistemas de pagos, en particular del SPEI.

Estas medidas contemplan tareas y acciones que son implementadas tanto al interior de este Instituto Central, como las que son requeridas a los Participantes del SPEI.

Medidas y acciones al interior de Banco de México.

A continuación se enlistan las medidas existentes:

- Revisiones periódicas de código y funcionalidad: se revisa el código fuente, tanto con herramientas especializadas como de forma manual, y se revisa la funcionalidad de los aplicativos en su conjunto.
- Esquemas de desarrollo seguro de software: los desarrolladores se capacitan en el desarrollo de aplicaciones seguras y se cuenta con herramientas automatizadas para evaluar la seguridad de las mismas. Existe también una revisión de código por pares que se realiza por integrantes de diferentes unidades administrativas a fin de verificar que no exista código malicioso en los nuevos desarrollos. Adicionalmente, se ha establecido un esquema de separación clara de roles para las actividades de desarrollo, pruebas e implantación en los ambientes productivos.
- Actualizaciones periódicas de la infraestructura conforme a mejores prácticas: se realiza el fortalecimiento en la infraestructura de cómputo siguiendo las recomendaciones de los proveedores y las mejores prácticas internacionales. Asimismo, se mantiene la infraestructura criptográfica que se utiliza en el SPEI con los estándares vigentes y se hacen actualizaciones periódicas de los mismos para mantener su fortaleza y confiabilidad.
- Pruebas de penetración: desde hace 5 años se revisa la infraestructura que soporta la operación central del SPEI de manera periódica por personal externo al Banco de México y se atienden las recomendaciones que se emiten en los reportes correspondientes.

- Auditorías internas y externas: se siguen los procesos de la Unidad de Auditoría del Banco de México tanto en temas de tecnologías de información, como en temas de procesos operativos. Al mismo tiempo, a través de la propia Unidad de Auditoría, se presentan informes a unidades externas al Banco, tal es el caso de la Auditoría Superior de la Federación.
- Protocolo de desconexión ante eventos de ciberseguridad: con el fin de proteger al sistema en su conjunto: se tiene desarrollado un protocolo para la conexión y desconexión de Participantes de la Red Financiera, cuando existe una presunta vulneración en temas de ciberseguridad.
- En que lo refiere a continuidad operativa:
    - Se cuenta con esquemas de operación en alta disponibilidad: el SPEI cuenta con mecanismos para permitirle operar aún en caso de falla de componentes de cómputo y telecomunicaciones de su infraestructura primaria de operación.
    - Se cuenta con una versión del SPEI que opera en un sistema operativo diferente a el que opera cotidiamente: en caso de que un evento impida operar en la infraestructura primaria del SPEI, este puede continuar operando y procesando pagos en una infraestructura tecnológica alternativa independiente.
    - Se cuenta con un cliente de operación alterno (COAS): este cliente les permite a aquellos bancos que tengan problemas operativos con su aplicativo, procesar pagos en el SPEI de tal manera que no interrumpan su operación.

Medidas y acciones establecidas por Banco de México para los Participantes.

A continuación se enlistan las medidas existentes:

- Emisión de regulación en temas de ciberseguridad (perimetral: políticas de gestión de contraseñas, restricción de accesos, etc.; específica: por ejemplo, requerimientos y restricciones sobre los aplicativos en ambientes de pruebas y producción) y de continuidad operativa (contar con infraestructura alterna para operar en casos de alguna contingencia, entre otras).

- Supervisión continua del cumplimiento de la regulación: Banco de México cuenta con planes anuales para supervisar *in situ* y *extra situ*, el cumplimiento de la regulación por parte de los participantes en el SPEI.
- En materia de continuidad operativa, que los participantes:
    - Cuenten con planes de recuperación de desastres: los participantes deben tener los procedimientos para la implementación medidas que permitan recuperar su operación ante incidentes en sus aplicativos e infraestructura.
    - Cuenten con centros de cómputo alternos y enlaces de telecomunicaciones redundantes: los participantes deben contar con infraestructura redundante con la cual puedan operar en caso de que su infraestructura principal se vea comprometida.
    - Se certifiquen para su operación en COAS: los participantes deben certificar ante Banco de México que pueden operar en COAS ante un evento en sus aplicativos.