Información sobre los ataques a los Participantes del SPEI

Banco de México

Mayo, 2018

BANCO DE MÉXICO

1. Resumen de Eventos de Ciberseguridad Abril-Mayo

2. Protocolo General de Reacción

3. Resiliencia del SPEI

4. Requerimientos de Ciberseguridad Aplicables a los Participantes

5. Comunicación con Participantes y con el Público

6. Acciones Particulares para Mitigar Riesgos

1. Resumen de Sucesos Operativos de SPEI Abril-Mayo

- El 17 de abril un participante del SPEI registró un ataque cibernético. A partir de esa fecha se han identificado 4 eventos adicionales de ataque cibernético: dos el 24 de abril, uno el 26 de abril y uno más el 8 de mayo.

- En todos los casos, **los ataques se presentaron en los aplicativos que usan los participantes afectados para preparar las órdenes de transferencia y conectarse al SPEI**. Dichos aplicativos pueden ser desarrollados por la propia institución o bien provistos a esta por un tercero, y radican en equipos de los participantes.

- **Los ataques que se han presentado están focalizados en diversos elementos que componen dichos aplicativos y en la infraestructura de cómputo y telecomunicaciones de los participantes** en la que se operan estos aplicativos.

- Estos aplicativos operan con recursos de los participantes (bancos, casas de bolsa, etc.). **Los mencionados ataques no afectaron las cuentas ni los recursos de los clientes**.

- **El Banco de México y el sistema central del SPEI no han sido blanco de ataques** ni han sido vulnerados, y no se han presentado afectaciones en su operación.

- **El SPEI sigue procesando normalmente órdenes de transferencias electrónicas entre los participantes con seguridad, y solo en algunos casos, con mayores tiempos de procesamiento.**

1. Resumen de Sucesos Operativos de SPEI Abril-Mayo

- En todos los casos identificados y reportados como un evento de ciberseguridad, los participantes tenían aplicativos de conexión al SPEI desarrollados por un tercero. No obstante, la vulnerabilidad pudo tener su origen tanto en los sistemas, como en la infraestructura en la que fue instalado.

- En la mayoría de los casos, los participantes recurren a proveedores externos para realizar dicha conexión entre sus sistemas centrales (denominados *core*) y la infraestructura del Banco de México. Cabe señalar que el Banco de México no certifica o valida a los proveedores de este tipo de servicios, el adecuado funcionamiento de dichos aplicativos es responsabilidad de cada participante.

- La proporción de mercado por volumen y monto de los diferentes proveedores es como sigue:

	Número de operaciones (% del total)	Monto de operaciones* (% del total)
Instituciones directamente atacadas (5)	13.09	7.64
Instituciones con un perfil de riesgo alto y que deben usar COAS (incluye las directamente atacadas)	19.46	28.80
Instituciones no afectadas con proveedor externo	7.16	14.67
Instituciones no afectadas con desarrollo propio	73.38	56.53

* Los montos de operaciones excluyen al sistema de liquidación de valores por no tener instrucciones directas del público en general.

1. Resumen de Sucesos Operativos de SPEI Abril-Mayo

- El ataque consistió en la fabricación o inyección de órdenes de transferencia apócrifas en los sistemas de los participantes donde se procesan las instrucciones de pago de los participantes afectados. El “modus operandi” identificado hasta el momento es el siguiente:
  - Los atacantes vulneran la infraestructura tecnológica de los participantes y generan en sus sistemas órdenes de transferencias ilegítimas, con cargo a las cuentas de los participantes, en alguna etapa del proceso previa a su conexión al SPEI.
  - Las órdenes de transferencias siempre incluyen el número de la cuenta emisora y de la receptora. En el caso de las generadas ilegítimamente, los números de las cuentas emisoras son inventados y no corresponden a cuentas de clientes, mientras que las cuentas receptoras son reales. La inserción de estas órdenes de transferencia se realizó en una etapa del proceso ejecutado en los sistemas de los participantes que no contaba con controles para asegurar que dichas órdenes fuesen legítimas.
  - Los sistemas de los participantes que fueron atacados firmaron y enviaron al SPEI las órdenes de transferencias ilegítimas validadas como si fueran legítimas.
  - El SPEI, al recibir las órdenes de transferencias, revisa que estén firmadas por los participantes, las procesa y abona el monto respectivo en la cuenta que le lleva al participante receptor.
  - El participante receptor, una vez que recibe del SPEI la confirmación de la liquidación, a su vez hace el correspondiente abono en la cuenta que este le lleva a su cliente receptor (en este caso, la cuenta especificada en la orden de transferencia de pago ilegítima).
  - Finalmente, los recursos ilegítimos son retirados mediante disposiciones de efectivo.

1. Resumen de Sucesos Operativos de SPEI Abril-Mayo

- Los participantes afectados se percatan de las instrucciones de pago ilegítimas por dos vías:

  i. mediante alertas internas producto de sus procesos de validación de operaciones; y

  ii. por medio de alertas por parte de otros participantes receptores de operaciones sospechosas.

- Debido a estos mecanismos de alerta, algunas de las transacciones identificadas fueron detenidas por los participantes receptores, con lo que se evitó la disposición indebida de parte de los recursos de procedencia fraudulenta.

- **Los recursos de los clientes no han estado en riesgo.** Como ya se mencionó, los atacantes han buscado vulnerar las conexiones de las instituciones con el SPEI, lo cual involucra únicamente recursos de la institución afectada.

- De hecho, los recursos de los clientes radican en un sistema separado con validaciones de autenticidad individuales por operación de las cuales no se cuenta con indicio alguno de que hayan sido atacadas.

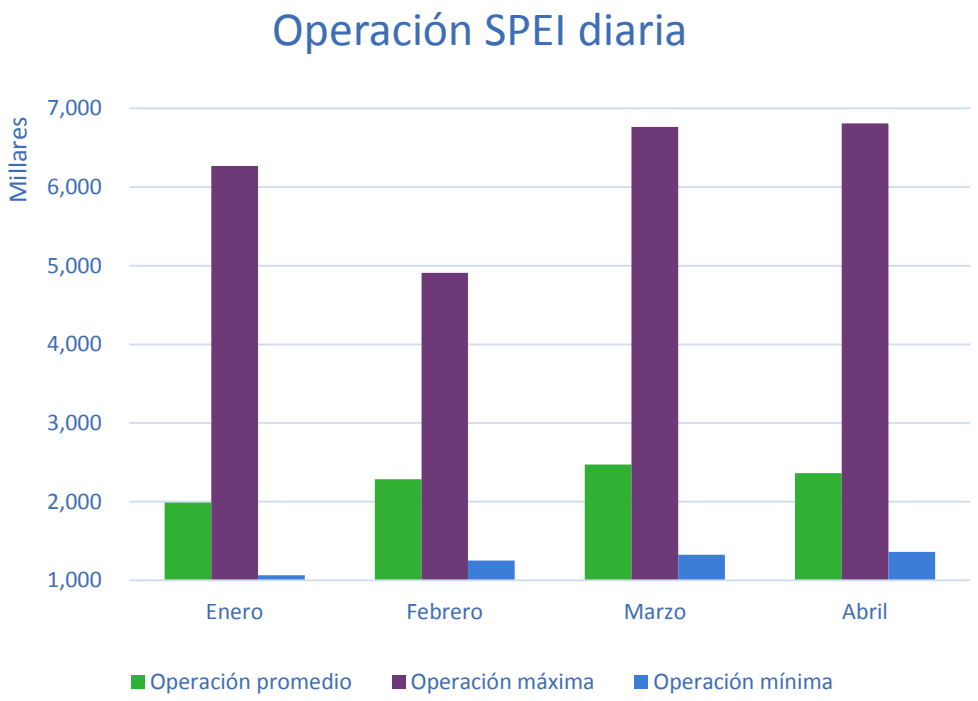
- **La afectación a los clientes ha sido la ralentización de los pagos para aquellas transacciones en las que participa alguna institución afectada o que opera bajo el esquema alterno para enviar órdenes de pago a través del SPEI.**

2. Protocolo General de Reacción

- En cada caso de evento relacionado con ciberseguridad, se aplicó un protocolo que implica la desconexión de la institución atacada y el inicio de operación a través de esquemas de contingencia.
  - Para estos fines, el Banco de México cuenta con un esquema de conexión paralelo de operación alterna para hacer transacciones en el SPEI (COAS), este es un procedimiento semiautomático, que ha permitido a los participantes operar desde una plataforma distinta y por lo tanto, más segura.
  - Conforme a la Circular 14/2017 todos los participantes deben contar con el sistema alterno (COAS) y su personal debe estar capacitado para usarlo. Esto para cumplir con la obligación de usarlo cuando el Banco de México lo indique.
- Una vez identificados los casos de ataques a alguna institución, se identifican elementos de riesgo que pueden resultar comunes a otros participantes. Con base en esta información, se emite un comunicado avisando a aquellos participantes en los que se identificó un mayor riesgo que tendrán que conectarse al SPEI a través del COAS desde sus instalaciones en fecha futura.
- **La operación a través del esquema de contingencia reduce los riesgos al tratarse de una infraestructura distinta a la que se ha visto afectada**, sin embargo, la operación en este esquema es semiautomática, lo que hace que las transferencias no se envíen y/o abonen en tiempo real.
- **La operación de 48 participantes por sistemas alternos propició la ralentización de algunas órdenes de transferencia a través del SPEI.**

3. Resiliencia del SPEI

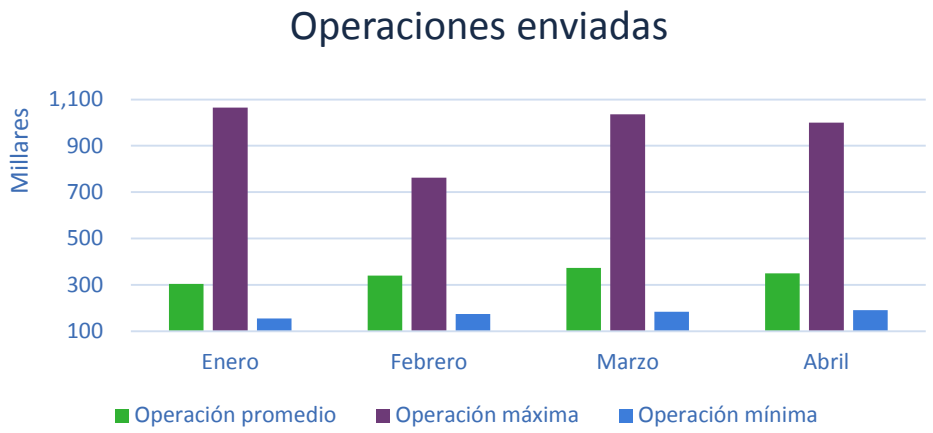
- **Pese a los ataques, el SPEI ha continuado brindando sus servicios de manera segura y procesando grandes cantidades de pagos.** Cabe resaltar que el 30 de abril, este sistema de pagos alcanzó su máximo histórico al procesar más de 6.8 millones de pagos.
- **El SPEI sigue procesando órdenes de transferencia electrónicas entre los participantes con seguridad, y en algunos casos con retrasos en los tiempos de servicio.**

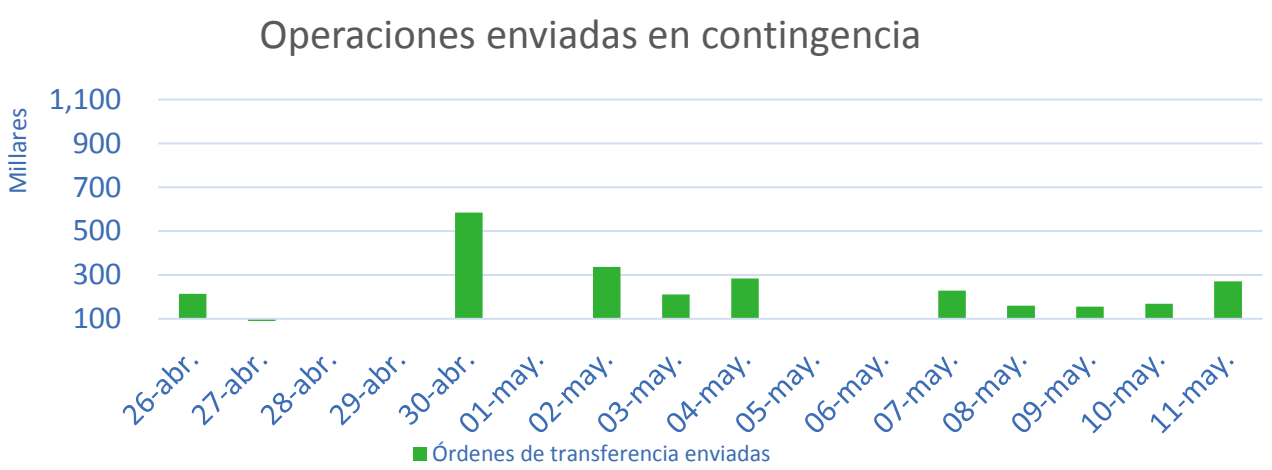


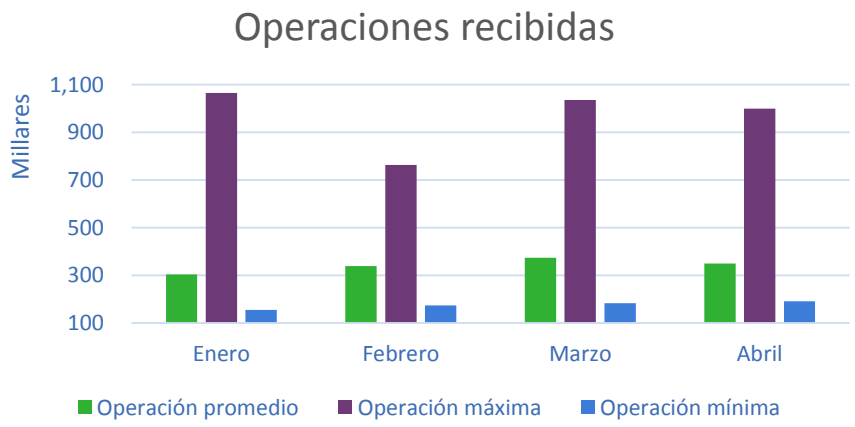
3. Resiliencia del SPEI

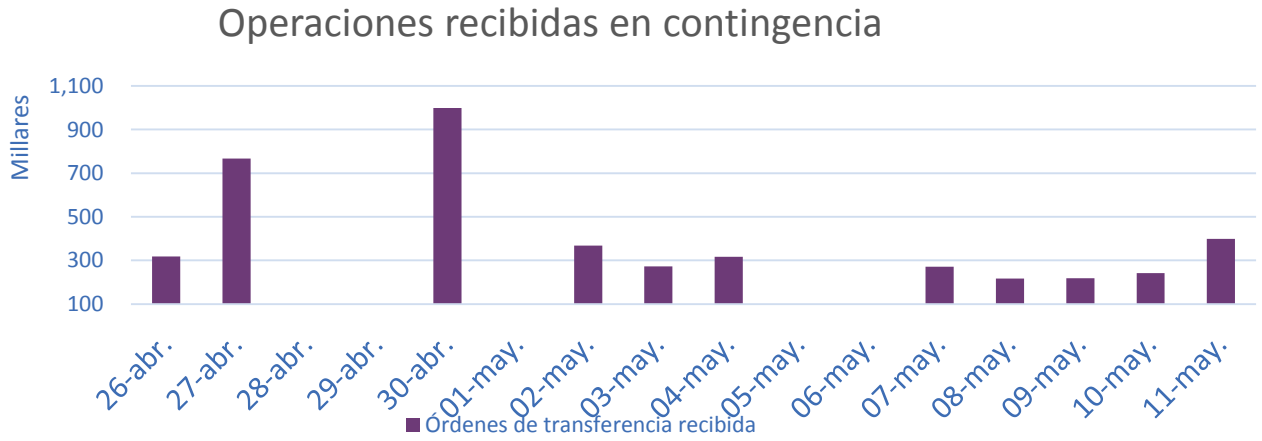
- De igual forma, los participantes que han sido afectados han recuperado el nivel de operación en el SPEI una vez que se estabilizaron sus procesos contingentes

Volumen y Monto Operado por el Participante Afectado con Mayor Operatividad









4. Requerimientos de Ciberseguridad Aplicables a los Participantes

- **Todos los participantes del SPEI deben de cumplir con requerimientos estrictos en materia de ciberseguridad informática y continuidad operativa.**

- Estos requerimientos se establecieron para los participantes del SPEI y entidades que pretenden incorporarse al sistema mediante la Circular 14/2017, emitida en julio de 2017, y quedaron obligados a cumplirlos a más tardar el 31 de enero del presente año, tiempo considerado por el Banco de México como suficiente para que los participantes hicieran las modificaciones necesarias a sus sistemas de cómputo y demás modificaciones necesarias para cumplir con la regulación.

- **Los requerimientos de ciberseguridad y de continuidad operativa contenidos en la Circular 14/2017 incluyen medidas preventivas encaminadas a prevenir y evitar ataques como los presentados en las últimas semanas.**

- El cabal cumplimiento de todas las disposiciones relativas a la operación y conexión al SPEI es un elemento indispensable para todos los participantes del SPEI.

- El incumplimiento de las disposiciones por parte de algunos participantes vulnera a todo el sistema, incrementando la probabilidad de ocurrencia de ataques como los descritos, con claras afectaciones a todos los usuarios de los servicios de transferencias electrónicas. Los procesos de supervisión están siendo ejecutados con la más alta prioridad para asegurar el cabal cumplimiento de la normatividad por todos los participantes.

4. Requerimientos de Ciberseguridad Aplicables a los Participantes

- Entre estos requerimientos destacan aquellos relacionados con la seguridad de los aplicativos de conexión al SPEI y con el esquema de operación alterna COAS, tales como*:
  - Contar con procedimientos para evaluar los protocolos de comunicación utilizados en la infraestructura tecnológica y prescindir de aquellos que se consideren inseguros;
  - Contar con procedimientos que permitan administrar las vulnerabilidades de seguridad informática derivadas de, entre otros factores, cambios, actualizaciones o errores en la infraestructura tecnológica;
  - Contar con procedimientos para detectar y gestionar incidentes de seguridad informática en la infraestructura tecnológica, que aseguren su identificación, contención y la adecuada recolección y resguardo de evidencia de seguridad;
  - Contar con procedimientos que aseguren que los componentes que brindan seguridad a sus sistemas informáticos se encuentren vigentes;

* Para un listado completo del los requerimientos de ciberseguridad y continuidad operativa aplicables a los Participantes del SPEI ver el "*Resumen de requerimientos en materia de seguridad informática y continuidad operativa a los participantes del SPEI*" publicado en el sitio de Información Importante sobre la Situación del SPEI. http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/spei.html

4. Requerimientos de Ciberseguridad Aplicables a los Participantes

- Requerimientos relacionados con la seguridad de los aplicativos de conexión al SPEI y con el esquema de operación alterna COAS (cont.):
  - Contar con procedimientos que permitan vigilar, auditar y rastrear todas las operaciones realizadas por los sistemas informáticos;
  - Contar con procedimientos de contratación y capacitación del personal para asegurar que aquel relacionado con la operación con el SPEI, cuente con las habilidades, competencias y conocimientos requeridos para el puesto que desempeña; y
  - Acreditar que pueden continuar con su operación ante la activación del "Procedimiento de Operación Alterno SPEI" (POA-SPEI), así como operar mediante el procedimiento de contingencia denominado "Cliente de Operación Alterno SPEI" (COA-SPEI).
- Derivado de los procesos de supervisión iniciados durante 2017 a los participantes del SPEI y otros sistemas de pagos operados por el Banco de México, se detectó un nivel de cumplimiento heterogéneo en los requerimientos de ciberseguridad y continuidad operativa.
- Es importante mencionar que el Banco de México está intensificando sus procesos de supervisión en esta materia.

5. Comunicación con Participantes y con el Público

Comunicación con los participantes

- Se generaron comunicados hacia todos los participantes para incrementar el monitoreo y vigilancia en las operaciones y reducir la probabilidad de que se presentaran ataques adicionales.
  - 17 de abril se reporta la detección de vulnerabilidades en una institución y se pide extremar precauciones.
  - 24 de abril se reporta el segundo evento especificando elementos de preocupación y solicitando medidas y controles adicionales.
  - 8 de mayo se les pide establecer controles en sus conexiones con todas las infraestructuras.
  - 10 de mayo se les reitera a las instituciones que por seguridad debe hacerse la conexión a COAS.
- Adicionalmente, se generaron comunicados dirigidos hacia los participantes con riesgos más elevados los días 26 de abril, 7 y 8 de mayo instruyéndoles acciones particulares.

5. Comunicación con Participantes y con el Público

Comunicación al público

- Se emitieron los siguientes comunicados de prensa:
  - 27 de abril se informa de eventos operativos en 3 instituciones y la ralentización del sistema para clientes.
  - 30 de abril se brinda mayor detalle sobre el comunicado anterior y se explican algunas de las medidas preventivas que han adoptado las instituciones (conjunto con la SHCP y la CNBV).
  - 14 de mayo se hacen del conocimiento del público las acciones emprendidas por Banco de México en los ámbitos de ciberseguridad, operativo y regulatorio.
  - 16 de mayo se publica en la página del Banco de México información importante sobre la situación del SPEI en el que se incluyen:
    i. Puntos importantes sobre la situación actual del SPEI
    ii. Estado de pagos particulares
    iii. Información operativa del SPEI
    iv. Requerimientos regulatorios de seguridad
    v. Estrategia de ciberseguridad: del SPEI y del Banco de México
    vi. ¿Qué es y cómo funciona el SPEI?

6. Acciones Particulares para Mitigar Riesgos

Tecnológicas

- Los participantes en los que se detectaron los incidentes operan por vías alternas y mantienen su capacidad para enviar órdenes de transferencias a la infraestructura del SPEI.
- Se establecieron alertas en el SPEI para detectar algunas anomalías en los mensajes.
- Se ha mantenido un soporte técnico reforzado 24/7 para los participantes.
- Se exigió a los proveedores de servicios de conexión al SPEI que incorporen controles adicionales en sus aplicativos.
- Se solicitó a los participantes hacer un análisis profundo de sus infraestructuras para detectar software durmiente.

Operativas

- Se requirió a los participantes cuyos aplicativos e infraestructura de cómputo para conectarse al SPEI resultaron afectados, tomar medidas para renovar los elementos de seguridad de sus operadores para autenticarse en los sistemas de pagos operados por el Banco de México, al tiempo que este Instituto Central ha ampliado y fortalecido el esquema de soporte a todos los participantes del sistema.
- El Banco de México reforzó el monitoreo de su infraestructura y sistemas para detectar cualquier comportamiento anómalo.

6. Acciones Particulares para Mitigar Riesgos

Regulatorias

- **El Banco de México emitió disposiciones que otorgan a las instituciones participantes en el SPEI espacio para que éstas 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 que se realicen en las instituciones de crédito y demás entidades que prestan el servicio de transferencias de fondos.**
  - **Circular 4/2018**
  - **Circular 5/2018**

6. Acciones Particulares para Mitigar Riesgos

Regulatorias

❑ Circular 4/2018

- Se impuso, para todas las entidades que participen en sistemas de transferencias de fondos ejecutadas el mismo día en que se genere su instrucción, la obligación de que los recursos de una transferencia de fondos enviada por otra entidad mediante dichos sistemas o de un traspaso entre cuentas abiertas en la misma entidad sean entregados, en efectivo o cheque de caja, si así lo solicita el cliente beneficiario respectivo, por montos iguales o superiores a $50,000 únicamente al día hábil siguiente a aquel en que se haya recibido la transferencia o traspaso respectivo. Por ejemplo, si un cliente recibe una transferencia o traspaso por un monto de 70 mil pesos, podrá retirar, en efectivo o cheque de caja, hasta $49,999.99 pesos el mismo día en que se acredite dicha transferencia en su cuenta y solo hasta el día hábil siguiente podrá retirar, de la misma manera, la cantidad restante, es decir, los $20,000.01 pesos restantes.
- La obligación referida únicamente será aplicable para el retiro de los recursos de transferencias de fondos que el cliente solicite en efectivo o cheque de caja, por lo que no afecta la disposición, en ese mismo día, de la totalidad o parte de esos recursos que el cliente pueda hacer por otros medios como, por ejemplo, pagos mediante tarjeta de débito o transferencias electrónicas o traspasos a otras cuentas.
- Esta Circular del Banco de México fue publicada en el Diario Oficial de la Federación del 17 de mayo de 2018.

6. Acciones Particulares para Mitigar Riesgos

Regulatorias

❑ Circular 5/2018

- Mediante esta Circular, publicada en el Diario Oficial de la Federación del 17 de mayo de 2018, el Banco de México emitió disposiciones para que los participantes en el SPEI puedan obtener autorizaciones temporales, que este Instituto Central otorgue después de analizar caso por caso, con el fin de que, durante la vigencia de dichas autorizaciones, puedan acreditar en las cuentas de los beneficiarios los recursos de las transferencias de fondos que reciban por montos iguales o superiores a $50000 pesos hasta que hagan validaciones específicas sobre su legitimidad.
- La vigencia de las autorizaciones será por periodos determinados por el Banco de México, que no podrán ser superiores a los seis meses, durante los cuales, los participantes autorizados deberán desarrollar sistemas para que puedan llevar a cabo las validaciones indicadas, de manera automatizada, en los periodos establecidos en la regulación (es decir, 5 segundos para transferencias mayores a 8 mil pesos que reciban instituciones bancarias o 30 segundos para todos los demás casos, ambos en el horario de 6:00 a 17:59:59 horas).
- **En ningún caso, los periodos de tiempo solicitados para llevar a cabo las validaciones referidas excederán del mismo día de operación del SPEI en que el participante reciba una transferencia de fondos**. Dichos periodos serán de un número determinado de minutos y, solo en aquellos supuestos excepcionales debidamente justificados por los participantes que lo soliciten, podrán ser superiores a una hora, pero, en ningún caso, podrán exceder del mismo día de operación del SPEI en que el participante reciba una transferencia de fondos. Los participantes que obtengan la autorización deberán comunicar a su clientela aquellos casos específicos en que podrían abonar en sus cuentas los recursos en los periodos de tiempo mayores, así como los periodos aplicables, el periodo de la autorización respectiva y el propósito de tales periodos autorizados.
- El Banco de México publicará en su portal de internet las autorizaciones que otorgue a los participantes respectivos, en donde indicará sus nombres, así como los periodos de tiempo que haya autorizado para los casos específicos y el periodo de vigencia de dichas autorizaciones.

BANCO DE MÉXICO