ACUSE

BANCO DE MÉXICO

Ciudad de México a 21 de junio de 2018

H. CÁMARA DE SENADORES
2018 JUN 21 PM 6 35
Presidencia de la Mesa Directiva
SECRETARÍA TÉCNICA

0087 39

SENADOR ERNESTO CORDERO ARROYO
Presidente de la Mesa Directiva de la Comisión Permanente
Del H. Congreso de la Unión,
P r e s e n t e.

Me refiero al Oficio número CP2R3A.-983, dirigido al Maestro Alejandro Díaz de León Carrillo, Gobernador del Banco de México, mediante el cual se hizo de su conocimiento que en la sesión celebrada el 6 de junio del año en curso, el Pleno de la Comisión Permanente del H. Congreso de la Unión, aprobó un dictamen de la Tercera Comisión en el que se contiene un Punto de Acuerdo por el que el citado órgano legislativo exhorta respetuosamente al Banco de México a fin de que remita un informe, dentro del marco de la ley, en torno a la intervención cibernética que vulneró los Sistemas de Transferencias Electrónicas de las instituciones financieras, incluyendo el alcance de la afectación, las autoridades responsables y las medidas de prevención establecidas.

Sobre el particular, de conformidad con lo previsto en los artículos 1o., 4o., 8o., párrafos primero, segundo y tercero, 10, 12, 14 Bis y 20, fracciones I, XI y XV del Reglamento Interior del Banco de México, así como el artículo Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, nos permitimos remitirle el presente informe cuyo contenido se integra de ocho secciones, en los términos siguientes:

I. Antecedentes;

II. Breve descripción del Sistema de Pagos Electrónicos interbancarios (SPEI);

II.1 Regulación del SPEI

II.2 El SPEI en comparación con otros Sistemas de Pagos a Nivel Internacional.

III. Descripción de los eventos de seguridad de la información recientes;

IV. Acciones adoptadas ante los eventos;

V. Procesos y mecanismos para salir de la contingencia;

VI. Supervisión;

VII. Coordinación entre autoridades, y

VIII. Consideraciones finales.

ANEXO 1. Disposiciones emitidas para mitigar las afectaciones por los incidentes de seguridad informática

I. Antecedentes.

La Comisión Permanente del H. Congreso de la Unión, en sesión celebrada el 6 de junio de 2018, adoptó el punto de acuerdo que, en su parte resolutiva, señala:

"ÚNICO.- La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente al Banco de México a fin de que remita un informe, dentro del marco de la ley, en torno a la intervención cibernética que vulneró los sistemas de transferencias electrónicas de las instituciones financieras, incluyendo el alcance de la afectación, las autoridades responsables y las medidas de prevención establecidas al efecto."

En atención al exhorto referido, el presente documento proporciona una descripción completa de los incidentes ocurridos durante los meses de abril y mayo del presente año en los sistemas que utilizan algunos participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI), así como las acciones que el Banco de México ha adoptado para resolver las contingencias asociadas a estos eventos. Asimismo, presenta las medidas ya adoptadas, además de aquellas que están en proceso de implementación, orientadas a reducir la probabilidad de que eventos similares ocurran en el futuro.

El artículo 2 de la Ley del Banco de México establece entre sus finalidades las de promover el sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos, lo que implica que el Banco de México debe velar por que las infraestructuras de los mercados financieros (IMF) funcionen adecuadamente. Las IMF son arreglos multilaterales entre instituciones participantes, incluyendo al operador del sistema, utilizados para los propósitos de compensación, liquidación o registro de pagos, valores, instrumentos derivados y otras transacciones financieras. Las IMF se conforman de los sistemas de pagos, los depósitos centrales de valores, los sistemas de liquidación de operaciones con valores, las contrapartes centrales y los repositorios de operaciones[1].

Las principales IMF del país están constituidas por el depósito central y sistema de liquidación de valores, denominados Indeval-DALI, la contraparte central para valores del mercado de capitales, conocida como CCV, la contraparte central de derivados denominada Asigna[2], el registro de operaciones derivadas del Banco de México y los sistemas de pagos. En este último rubro se encuentran los sistemas operados por el Banco de México, en particular el SPEI y el Sistema de Pagos Interbancarios en Dólares (SPID), así como el sistema internacional de liquidación de operaciones cambiarias denominado CLS[3]. Además, se cuenta con la cámara de compensación de cheques y transferencias

---

[1] En el documento "Política y funciones del Banco de México respecto a las infraestructuras de los mercados financieros", publicado en el sitio de Internet del Banco Central, de describen las características de cada infraestructura.

[2] S.D. Indeval Institución para el Depósito de Valores, S.A. de C.V. es la entidad que funge como depósito central de valores en México que opera el sistema DALI y forma parte del Grupo BMV, integrado por la Bolsa Mexicana de Valores, S.A.B. de C.V. Asimismo, la Contraparte Central de Valores de México, S.A. de C.V.(CCV) y el fideicomiso denominado Asigna, Compensación y Liquidación son operados por este grupo.

[3] Continuous Linked Settlement, es un sistema de pagos internacional para la liquidación de operaciones en divisa alrededor del mundo en el que el peso mexicano es una de las monedas que se liquida desde 2008.

electrónicas diferidas operada por Cecoban, S.A. de C.V. y los sistemas utilizados para operaciones con tarjetas bancarias.

El SPEI es la infraestructura de pagos operada por el Banco de México que permite a las instituciones financieras participantes (instituciones de crédito, casas de bolsa, sociedades financieras populares -Sofipos- y otras entidades financieras reguladas) enviar y recibir transferencias de fondos en moneda nacional entre sí para poder brindar a sus clientes el servicio de transferencias electrónicas de fondos en tiempo real. El Sistema de Pagos de Uso Ampliado (SPEUA), que entró en operación en 1995, antecesor del SPEI, fue el primer sistema de pagos en el país en permitir la transferencia de recursos entre los clientes de los participantes. La principal función del SPEI, así como del SPEUA en su tiempo, es procesar los grandes pagos de las instituciones financieras y tesorerías de empresas; sin embargo, el Banco de México considera muy relevante ofrecer el servicio de transferencias electrónicas en tiempo real a la población en general. El SPEUA no restringía el envío de tales transferencias por el tipo de cliente, pero estaba enfocado principalmente a empresas y, en sus inicios, el monto mínimo por transferencia era de 500 mil pesos, y posteriormente se redujo hasta quedar en 50 mil pesos. En 2004 el Banco de México puso en operación el SPEI, un sistema que fue diseñado para cumplir con las características de procesar pagos con alta seguridad y eficiencia y con un alto rendimiento, lo que permitió desde un principio a sus participantes ofrecer transferencias de fondos al público en general y sin monto mínimo por dichas transferencias. Las características del SPEI permitieron su rápida adopción y de un promedio de 20 mil transferencias por día que llegó a tener el SPEUA, actualmente se liquidan en promedio alrededor de 2 millones de transferencias en el SPEI, la gran mayoría de estas corresponden a operaciones de bajo monto instruidas por el público en general.

El Banco de México, con el fin de lograr el funcionamiento seguro y eficiente del SPEI, contempla acciones para hacer frente a episodios disruptivos, como es el caso de los relacionados con la seguridad informática. En ese sentido, el Banco de México establece planes de respuesta ante los incidentes de seguridad informática que detecta o le reportan las instituciones financieras participantes; planes de contingencia para mantener la continuidad operativa del sistema, así como mecanismos claros para el regreso a la operación normal. El SPEI tiene múltiples elementos de redundancia y distintos niveles de operación que atienden a muy diversos tipos de eventos potenciales. Además de esto, incluso si se realizase un evento no considerado que implicase la imposibilidad de usar alguno de los elementos de contingencia, los clientes podrían continuar realizando operaciones al menudeo a través de Cecoban y las instituciones de crédito podrían realizar sus operaciones entre sí a través de otro sistema del Banco de México conocido como Sistema de Atención a Cuentahabientes del Banco de México (SIAC-BANXICO).

La seguridad de la información es indispensable para el buen funcionamiento del sistema financiero. De hecho, las transacciones que en él se celebran se pueden conceptualizar como mensajes compartidos entre distintos participantes, los cuales les permiten establecer obligaciones financieras entre sí. El hecho de que las instituciones financieras se encuentren interconectadas a nivel informático, lo cual conlleva un flujo más eficiente de los mencionados mensajes o transacciones, genera una red, en la que todos los participantes comparten tanto los beneficios como los riesgos de la misma. Es decir, lo que hace cualquier participante no sólo le afecta a ese participante en lo particular, sino a todo aquel que está conectado en la mencionada red. Si bien existen medidas para mitigar la probabilidad de que un problema con algún participante se contagie al interior de la red, cuando esto llega a suceder, se afecta la confianza de los usuarios en el sistema en su conjunto. Por ello, cuando se trata de elegir el nivel de seguridad informática que se implementará por todos los participantes, se deben establecer mínimos indispensables para garantizar un nivel de seguridad adecuado para toda la red, ya que la seguridad de la información depende del eslabón más vulnerable de la cadena y un ataque que no sea mitigado adecuadamente puede convertir un problema individual en uno sistémico. En este sentido, el Banco de México, desde julio de 2017, fortaleció la regulación del SPEI, la cual contempla la imposición de estándares mínimos de seguridad de la información que este Instituto Central requiere para operar en sus sistemas, de manera particular en el SPEI y en el SPID.

Es importante resaltar que estos esfuerzos para establecer reglas y procesos de supervisión y sanción claros para fortalecer los estándares de seguridad de la información deben estar coordinados entre las distintas autoridades financieras. En ese sentido, el pasado 24 de mayo las distintas autoridades financieras del país, en conjunto con las asociaciones que representan a los gremios del sistema financiero y la Procuraduría General de la República, suscribieron las Bases de Coordinación en Materia de Seguridad de la Información.

Finalmente, es relevante señalar que los avances en tecnologías de la información nunca están exentos de riesgos. Si bien estos avances han redituado en notables beneficios para el sistema financiero y para el público en general, estos beneficios siempre estarán acompañados de riesgos, mismos que deben ser reducidos y mitigados.

Recientemente, algunos participantes del SPEI experimentaron incidentes en sus aplicativos que utilizan para preparar sus órdenes de transferencia y conectarse con el SPEI. Es importante resaltar que, a pesar de los incidentes mencionados, el SPEI y la infraestructura del Banco de México no fueron blanco de ataque alguno y, por lo tanto no fueron vulnerados. Asimismo, debido a que los aplicativos de las instituciones financieras que fueron vulnerados radican entre el sistema que administra las cuentas de sus clientes y el sistema SPEI, los recursos y la información de los clientes de las instituciones financieras afectadas estuvieron seguros y fuera de peligro. En respuesta a estos eventos, el Banco de México adoptó una serie de medidas que ayudaron a contener las posibles

afectaciones de estos incidentes sobre los participantes afectados, así como en el sistema de pagos en general. Dichas medidas incluyeron acciones de continuidad operativa, de supervisión y regulatorias, las cuales se explican a continuación. Adicionalmente, con el objetivo de regresar a la operación habitual del sistema, el Banco de México ha definido las acciones específicas que deben cumplir las instituciones participantes que se encuentran operando en un esquema contingente para regresar a la operación habitual con un mayor nivel de seguridad de la información.

II. Breve descripción del Sistema de Pagos Electrónico Interbancario (SPEI).

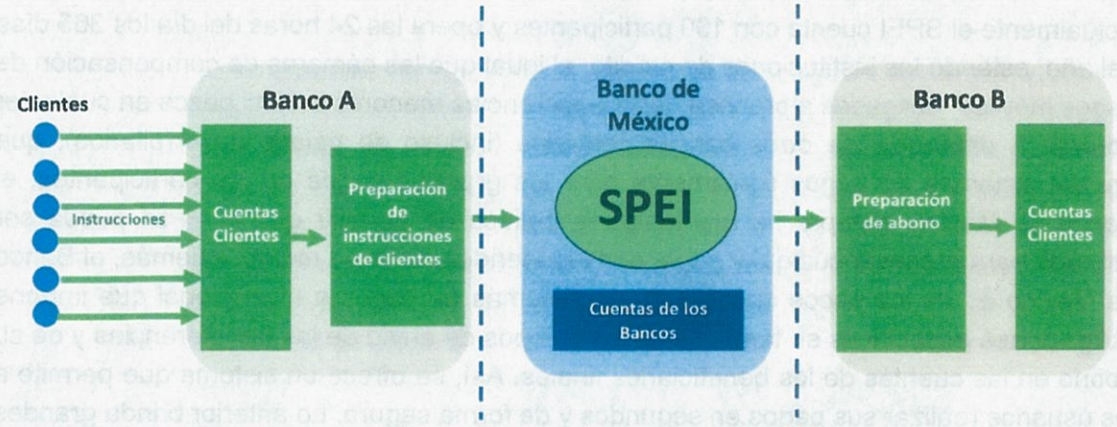
El SPEI tiene por objetivo la liquidación de órdenes de transferencia de fondos de sus participantes de manera oportuna, eficiente, segura y a bajo costo, considerando tanto las relacionadas con los mercados financieros, como los pagos al menudeo. El SPEI proporciona la infraestructura central a la que se conectan los participantes y sobre la cual, de manera eficiente y segura, se cargan y abonan las cuentas que las instituciones participantes mantienen con el Banco de México, para liquidar las operaciones entre participantes. Para realizar la preparación de las transferencias de fondos y lograr la conexión con el SPEI los participantes realizan desarrollos informáticos propios o contratan a terceros para que les brinden estos servicios.

Actualmente el SPEI cuenta con 100 participantes y opera las 24 horas del día los 365 días del año, estando las instituciones de crédito, al igual que las cámaras de compensación de pagos móviles, obligadas a procesar las transferencias menores a 8 mil pesos en cualquier horario. A diferencia de otros bancos centrales (incluso de países desarrollados), que operan sistemas de pagos únicamente para los grandes pagos de los participantes, el Banco de México siempre ha mantenido la política de permitir que el SPEI pueda ser utilizado para procesar cualquier pago, con independencia de su monto. Además, el Banco de México es de los pocos operadores de sistemas de pagos a nivel global que impone obligaciones específicas en términos de los tiempos de envío de las transferencias y de su abono en las cuentas de los beneficiarios finales. Así, se ofrece un sistema que permite a los usuarios realizar sus pagos en segundos y de forma segura. Lo anterior brinda grandes beneficios a la población, pero también trae consigo una gran responsabilidad para el Banco de México, que incluye el mantener altos estándares de seguridad y esquemas de continuidad operativa para asegurar las transacciones, la integridad de los sistemas y un alto nivel de servicio, todo ello en beneficio de los usuarios finales.

El procesamiento de una transferencia SPEI sigue la siguiente secuencia:

1. El cliente final (cuentahabiente) instruye una transferencia desde su banca electrónica o aplicación móvil a la institución participante que le brinda los servicios. Esto se hace siguiendo rigurosos controles de seguridad como contraseñas, elementos dinámicos (tokens) y pruebas de posesión de dispositivos (como mensajes a teléfonos móviles pre registrados), entre otros.

2. La institución participante valida los elementos de seguridad de la instrucción y guarda evidencia de que realizó esta validación.
3. La institución participante prepara las instrucciones de transferencias de sus clientes, les incluye elementos de seguridad adicionales que prevén las reglas aplicables a este sistema emitidas por el Banco de México (Reglas del SPEI), sobre los cuales únicamente las instituciones participantes tienen el control, y los envían al SPEI de Banco de México.
4. El Banco de México verifica las firmas electrónicas de las instituciones participantes, que dan certeza de su identidad y de la integridad de la instrucción de transferencia, y procede a su procesamiento y posterior liquidación al participante receptor de la transferencia.
5. Se informa a los participantes involucrados en la transferencia de recursos de la liquidación y la institución participante receptora de la transferencia acredita los fondos en la cuenta de su cliente y confirma este hecho mediante el envío al Banco de México de la información para generar el comprobante electrónico de pago (CEP) que queda a disposición del cliente que instruye y el que recibe la transferencia.



II.1 Regulación del SPEI.

El Banco de México, además de sus facultades como autoridad de expedir disposiciones que tengan por propósito el sano desarrollo del sistema financiero y el buen funcionamiento del sistema de pagos, está facultado para administrar dichos sistemas y, por lo tanto, establecer la normatividad interna de aquellos que opere. En tal virtud, emitió las Reglas del SPEI, que establecen las obligaciones que las instituciones financieras que participan en dicho sistema deben observar. Dichas reglas están contenidas en la Circular 14/2017, publicada en el Diario Oficial de la Federación el 4 de julio de 2017. Los principales aspectos de tal regulación se enfocan en la seguridad informática y continuidad operativa del referido sistema de pagos, así como la protección y los niveles de servicio a los clientes de los participantes del sistema.

Seguridad Informática y continuidad operativa

Todos los participantes del SPEI deben de cumplir con requerimientos estrictos en materia de seguridad informática y continuidad operativa. La obligación de cumplir con estos requerimientos entró en vigor el 31 de enero del presente año, tiempo considerado por el Banco de México como suficiente para que los participantes hicieran los cambios necesarios a sus sistemas de cómputo y demás modificaciones necesarias para cumplir con las Reglas del SPEI. Estos requerimientos incluyen medidas preventivas encaminadas a prevenir y evitar incidentes, como los presentados en abril y mayo de este año. Entre los referidos requerimientos a los participantes del SPEI destacan aquellos relacionados con la seguridad de los aplicativos de conexión al sistema y de continuidad operativa relacionados con el esquema de operación alterna denominado "Cliente de Operación Alterno SPEI" (COA SPEI), entre los cuales destacan:

- Contar con procedimientos para procesar de manera segura los mensajes entre sus sistemas y el SPEI;
- Contar con procedimientos que permitan detectar y gestionar vulnerabilidades e incidentes de seguridad informática así como contar con componentes de seguridad informática que se encuentren vigentes;
- Contar con procedimientos que permitan vigilar, auditar y rastrear todas las operaciones realizadas por los sistemas informáticos y establecer políticas para mantener evidencia sobre incidentes de seguridad informática;
- 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 operar mediante el procedimiento de contingencia COA SPEI.

Es importante señalar que el Banco de México está haciendo una revisión profunda de todos los elementos regulatorios de seguridad de la información relacionados con el SPEI. Al respecto, si bien los estándares de seguridad de la información contemplados siguen vigentes, se reforzarán los procesos de supervisión, autoevaluación y el involucramiento de todas las capas de gobierno corporativo de las instituciones participantes en esta materia.

Protección y niveles de servicio a clientes

Las Reglas del SPEI establecen los controles de seguridad que deben tener los participantes en relación con los canales que ofrecen a sus clientes para el envío de transferencias vía el SPEI. Adicionalmente, las Reglas establecen obligaciones para salvaguardar los recursos que los clientes de las instituciones participantes envían a través del SPEI.

Como se mencionó, las instituciones de crédito y las cámaras de compensación de pagos móviles deben ofrecer el servicio de transferencias de fondos a través del SPEI de hasta 8 mil pesos las 24 horas, los 365 días del año, y las Reglas del SPEI establecen límites a los tiempos en que los participantes deben enviar las instrucciones de transferencia al SPEI y deben acreditar en las cuentas de sus clientes beneficiarios el importe de una transferencia recibida. Además, las Reglas establecen un nivel mínimo de disponibilidad de servicio de transferencias SPEI que los participantes deben ofrecer a sus clientes. Por otro lado, las Reglas del SPEI incluyen obligaciones para que los participantes mantengan informados a sus clientes, tanto de manera oportuna como periódica, de los movimientos en sus cuentas generados por transferencias del SPEI. Adicionalmente, los participantes deben incluir en su sitio de internet una página en la que detallen el procedimiento que sus clientes deben seguir para presentar solicitudes de aclaración, consultas sobre el estado o reclamaciones relacionadas con alguna orden de transferencia que estos hayan enviado o recibido por el SPEI.

II.2 El SPEI en comparación con otros sistemas de pagos a nivel internacional.

El funcionamiento de un sistema de pagos tiene dos elementos que lo caracterizan: i) la forma en que se realiza la liquidación de las operaciones entre las cuentas que se mantienen con el operador del sistema, es decir la liquidación entre los participantes directos del sistema, que puede ser en tiempo real o diferida; y, ii) las condiciones en las que las entidades emisoras y receptoras tramitan y abonan respectivamente las instrucciones de pago que se liquidan en el sistema. El SPEI es un sistema que liquida en tiempo real las operaciones entre sus participantes y además es uno en el que el Banco de México establece estrictos requerimientos a los participantes en términos de los tiempos entre la recepción de las instrucciones de pago de los clientes y su envío, así como entre la recepción de los avisos de liquidación por parte del sistema y los abonos en las cuentas de los clientes receptores. Esta combinación no es muy común en el mundo (aunque empiezan a desarrollarse a últimas fechas algunos sistemas de los llamados pagos inmediatos que cubren estas características), y mucho menos lo es el que todas las entidades depositarias participen en el mismo sistema. Esto último garantiza que las personas con cuentas de depósitos de dinero tengan acceso a realizar pagos a cualquier cliente de los demás participantes, con lo que se aprovecha cabalmente la extensión de la red y se reducen los costos de las transferencias (economías de red y de escala).

El SPEI es un sistema híbrido, dado que tiene características de tres diferentes tipos de sistemas de pagos. En primer lugar, tiene las características de los sistemas de pagos de alto valor que algunas jurisdicciones utilizan exclusivamente para liquidar en tiempo real pagos de montos muy grandes. Por otra parte, el SPEI también es un sistema de pagos de bajo valor, en los cuales típicamente se compensan y liquidan los pagos de la población en general y se utiliza un esquema de liquidación diferida (usualmente los beneficiarios reciben los recursos un día hábil después de su instrucción), a diferencia del SPEI en el que los beneficiarios reciben los recursos en tiempo real. Finalmente, el SPEI tiene características de los denominados sistemas de pagos instantáneos, los cuales ofrecen el servicio de pagos de bajo valor en tiempo real a la población en general. Este último es un tipo de sistema de pagos con el que pocos países cuentan y que se han desarrollado (o están bajo desarrollo) en tiempos recientes.

En esta sección se compara al SPEI con los sistemas de pagos de los principales miembros del Comité de Pagos e Infraestructuras de Mercados (CPMI, por sus siglas en inglés), auspiciado por el Banco de Pagos Internacionales (BIS, por sus siglas en inglés), que caen en las categorías de sistemas de pagos citadas. En particular, se compara al SPEI con los principales sistemas de pagos de Estados Unidos, Reino Unido, la Unión Europea, Australia, Suecia, y Japón.

El SPEI en comparación con los sistemas de pagos de alto valor

En la mayoría de los países, los bancos centrales solo están involucrados en la operación de los sistemas de pagos de alto valor. Este tipo de sistemas de los principales miembros del CPMI son Sistemas de Liquidación Bruta en Tiempo Real (LBTR)[4] o equivalentes. Esto los vuelve sistemas rápidos, eficientes y que permiten el procesamiento de pagos irrevocables y definitivos entre instituciones financieras y grandes empresas, condiciones que se consideran necesarias para que los sistemas de pago de alto valor cumplan con su objetivo de contribuir a la estabilidad financiera de los países.

Asimismo, los sistemas de pagos de alto valor están en su gran mayoría restringidos para la sociedad en general, ya que solo permiten el procesamiento de los pagos de sus participantes directos (instituciones financieras), de algunos de los clientes de estos que por su tamaño son relevantes para el sistema financiero, y los correspondientes a la liquidación de otras infraestructuras de los mercados financieros. La mayoría de los sistemas de pagos que no son de alto valor carecen de reglas específicas que normen los tiempos de envío y acreditación de transferencias interbancarias en relación a las instrucciones de pago que reciben de sus clientes.

[4] Un sistema de LBTR liquida operaciones una a una tan pronto estas ingresan al sistema.

En contraste, el SPEI es un sistema que procesa tanto pagos de sus participantes, como de los clientes de sus participantes, sin importar el tamaño de dichos clientes. Adicionalmente, las Reglas del SPEI establecen claramente los tiempos en que sus participantes están obligados a enviar las transferencias que les instruyan sus clientes y a acreditar los montos de las mismas en las cuentas de los beneficiarios finales. Esta regulación permite que los usuarios finales del SPEI cuenten con un alto nivel de servicio, en particular la posibilidad de que los clientes beneficiarios dispongan de los recursos de una transferencia de manera muy rápida.

El cuadro 1 resume los principales sistemas de pago de alto valor, así como si cuentan o no con regulación específica respecto a los tiempos de envío y acreditación de transferencias.

Cuadro 1. Características de los principales sistemas de alto valor

Sistema (jurisdicción)	***Abierto al público en general***	***Regulación sobre tiempos de envío y acreditación***
SPEI (México)	✓	✓
RITS (Australia) [5]	✓	X
BOJ-NET (Japón) [6]	X	X
RIX (Suecia) [7]	X	X
CHAPS (Reino Unido) [8]	X	X
Target 2 (Unión Europea) [9]	X	X
Fed Wire (Estados Unidos) [10]	X	X

El SPEI en comparación con los sistemas de pagos de bajo valor

Si bien en la mayoría de los países los bancos centrales no se involucran en la operación de los sistemas de pagos de bajo valor, sí es común que se involucren en su vigilancia y regulación. En su mayoría, este tipo de sistemas tienen un esquema de liquidación diferido, por lo que requieren de al menos un día para poner los fondos de una transferencia a

[5] Real Time Gross Settlement (RTGS) https://www.rba.gov.au/payments-and-infrastructure/rits/about.html#rtgs
[6] Section 3.2.1.4 " Operation of the system and settlement procedures" https://www.bis.org/cpmi/publ/d105_jp.pdf
[7] Section 3 "Payments systems (funds transfer systems)" https://www.bis.org/cpmi/publ/d97_se.pdf
[8] "The Bank of England´s Real-Time Gross Settlement infrastructure" https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2012/the-boes-real-time-gross-settlement-infrastructure.pdf?la=en&hash=19E2757607F99F5DED483E98AE16E7CBF25CDE05
[9] TARGET2 solo permite la liquidación de operaciones de sus participantes, no obstante que proporciona una amplia gama de servicios, incluyendo la liquidación de varios sistemas de pagos de bajo valor como se indica en la pg. 96 del documento *Payment, clearing and settlement systems in the Euro Area.* https://www.bis.org/cpmi/publ/d105_eu.pdf
[10] Participación de clientes institucionales con cuenta en la Reserva Federal de acuerdo a la página 487 del documento *Payment, clearing and settlement systems in the United States* https://www.bis.org/cpmi/publ/d105_us.pdf
No se establece regulación en cuanto a tiempos de recepción, acreditación, y ejecución de órdenes de pago, de acuerdo a la página 4 del documento *Operating Circular N°6. "Funds transfers through the Fedwire® funds service"* https://www.frbservices.org/assets/resources/rules-regulations/operating-circular-6-102917.pdf

disposición del beneficiario final de la misma. Esto se debe a que estos pagos suelen considerarse como no críticos, por lo que su proceso de compensación y liquidación suele ser neto y al final del día o posterior a la fecha de instrucción de las operaciones. Este tipo de sistemas acumulan un gran número de pagos para luego compensarlos y liquidarlos por lotes en tiempos específicos durante días hábiles bancarios, generalmente una vez al día.

En contraste, el SPEI procesa todos sus pagos en tiempo real, incluyendo aquellos enviados por el público en general. Durante una operación normal esto significa que los fondos de estas transacciones se abonan a su beneficiario final en aproximadamente 60 segundos a partir de su instrucción. Cabe destacar que, incluso bajo un esquema de contingencia, las operaciones procesadas por el SPEI se liquidan el mismo día en que fueron instruidas, lo cual, aun en este entorno, se liquida con mayor oportunidad que en la mayoría de los sistemas de pago de bajo valor de otras jurisdicciones.

El cuadro 2 muestra cómo se compara el SPEI con los principales sistemas de pagos de bajo valor con procesamiento por lotes.

Cuadro 2. Características de los principales sistemas de bajo valor

Sistema (jurisdicción)	***Disponibilidad de fondos para el beneficiario final***	***Liquidación entre participantes del sistema***
SPEI (México)	Inmediata	Inmediata
BECS (Australia) [11]	T+1	5 veces al día [12]
Zengin (Japón)	Inmediata [13]	1 vez al día [14]
BGC (Suecia)	Al final del día [15]	29 veces al día [16]
BACS (Reino Unido) [17]	T+3	1 vez al día
STEP2 (Unión Europea)	Al final del día [18]	Hasta 7 veces al día [19]
FedACH (Estados Unidos)	Al final del día [20]	1 vez al día [21]

[11] https://www.bis.org/cpmi/publ/d97_au.pdf

[12] Los pagos en BECS son compensados y liquidados cinco veces al día, como se indica en la página 30 del artículo *Clearing and Settlement Systems from Around the World: A Qualitative Analysis* de *Payments Canada*, el cual se encuentra disponible en: https://www.bankofcanada.ca/wp-content/uploads/2016/06/sdp2016-14.pdf

[13] Los pagos de bajo monto (menores a 1,000,000 JPY) son compensados y liquidados una vez al día, mientras que los de alto valor se liquidan en tiempo real: https://www.bis.org/cpmi/publ/d105_jp.pdf#page=21?ch=3

[14] Los pagos de bajo monto son compensados y liquidados una vez al día, como se indica en la página 29 del artículo *Clearing and Settlement Systems from Around the World: A Qualitative Analysis* de *Payments Canada*.

[15] Como se indica en: https://www.bankgirot.se/en/about-bankgirot/our-offer/payment-systems/bankgiro-system/

[16] Información extraída del artículo *Clearing and Settlement Systems from Around the World: A Qualitative Analysis* de *Payments Canada*.

[17] Los pagos en BACS tienen un ciclo de compensación y liquidación de 3 días hábiles, como se indica en la página 455 del Libro Rojo del CPMI https://www.bis.org/cpmi/publ/d105_uk.pdf y la página 28 del artículo *Clearing and Settlement Systems from Around the World: A Qualitative Analysis* de *Payments Canada*.

[18] En general, la disponibilidad de fondos puede variar dependiendo de la zona geográfica de la institución receptora. No obstante, existen bancos que acreditan al final del día las trasferencias de sus clientes: https://www.eestipank.ee/en/payments/step2

[19] Los pagos en STEP2 de la Unión Europea son compensados y liquidados hasta siete veces al día, como se indica en la página la *European Banking Association*: https://www.ebaclearing.eu/services/step2-sct/settlement-and-processing-cycles/

[20] A partir de marzo 2016, los pagos hechos por FedACH deben acreditarse en el mismo día en que se liquiden, para pagos de hasta USD 25,000: https://www.frbservices.org/resources/resource-centers/same-day-ach/index.html

[21] FedACH compensa y liquida una vez al día en el mismo día de la instrucción, como se indica en la página 30 del artículo *Clearing and Settlement Systems from Around the World: A Qualitative Analysis* de *Payments Canada*.

El SPEI en comparación con los sistemas de pagos instantáneos

De acuerdo con el reporte *Fast Payments – Enhancing the speed and availability of retail payments* del CPMI,[22] los sistemas de pagos instantáneos están definidos por proveer pagos con dos características: velocidad (disponibilidad de recursos irrevocables para el beneficiario final en tiempo real) y disponibilidad continua de servicio (24/7/365). Cabe señalar que existen dos modalidades en este tipo de sistemas, en una de ellas la liquidación definitiva de las operaciones ocurre en tiempo real, esto es, las afectaciones finales en las cuentas de los participantes ocurre de manera inmediata, al igual que la disponibilidad de los recursos para el beneficiario; en la segunda modalidad la disponibilidad de recursos para el beneficiario es igualmente inmediata, pero la afectación en las cuentas de los participantes ocurre de manera diferida. El citado reporte también señala que, entre los 27 miembros del CPMI se identificaron solo 19 iniciativas de este tipo de sistemas, de las cuales solo 16 estaban en operación en 2016 mientras que se tenía programado que durante 2017 y 2018 entraran en operación 5 adicionales.

Lo anterior refleja que, incluso entre los países más avanzados en el desarrollo de infraestructuras de los mercados financieros, la presencia de sistemas de pagos instantáneos es relativamente baja. En el caso de México el sistema de pagos instantáneos está incluido en el SPEI desde que este inicio operaciones en 2004, aunque el horario 24x7 comenzó hasta 2015 para pagos móviles y en diciembre de 2017 para todos los pagos de bajo valor.

Cabe señalar que en México todas las instituciones de crédito participan en el SPEI, a diferencia de otros países en los que no todas las instituciones deciden participar en los sistemas de pagos instantáneos, lo que hace que en nuestro país los clientes de cualquier banco cuenten con una red completa para realizar sus pagos, y no limitada como es el caso de otros países.

El cuadro 3 muestra las características de algunos sistemas de pagos instantáneos alrededor del mundo[23].

[22] Dicho documento está disponible en: https://www.bis.org/cpmi/publ/d154.pdf

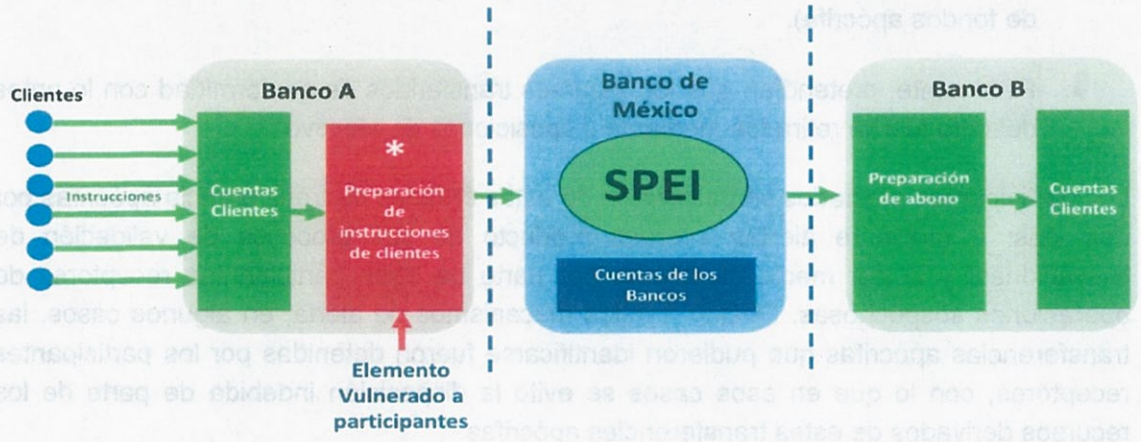
[23] Los datos contenidos en el cuadro se extrajeron del reporte sobre pagos rápidos del BIS y el artículo *Clearing and Settlement Systems from Around the World: A Qualitative Analysis* de Payments Canada. Cabe señalar que si bien algunos sistemas de pagos instantáneos no imponen directamente límites al monto de las transacciones que procesan, las instituciones participantes podrían fijar los límites que consideren adecuados para mitigar riesgos financieros.

Cuadro 3. Características de los principales sistemas de pagos instantáneos

Sistema (jurisdicción)	*Año de inicio de operaciones*	*Disponibilidad de fondos para el beneficiario*	*Liquidación entre participantes del sistema*	*Límites de monto*
SPEI (México)	2004	Inmediata	Inmediata	< 8,000 MXN
NPP (Australia)	2018	Inmediata	Inmediata	Ninguno
Zengin (Japón)	2018	Inmediata	Inmediata	>1,000,000 JPY
BiR (Suecia)	2012	Inmediata	Inmediata	Ninguno
FPS (Reino Unido)	2008	Inmediata	3 veces al día	>265,400 GBP
TIPS (Unión Europea)	2018	Inmediata	Inmediata	Ninguno

III. Descripción de los eventos de seguridad de la información recientes

El 17 de abril del presente año, un participante del SPEI detectó que sus sistemas emitieron órdenes de transferencia de fondos no autorizadas. A partir de esa fecha se han identificado 4 eventos similares en otros participantes, dos el 24 de abril, uno el 26 de abril y uno más el 8 de mayo. En todos los casos, los incidentes se presentaron en los aplicativos que usaban los participantes afectados para preparar las órdenes de transferencia y conectarse al SPEI. Dichos aplicativos pueden ser desarrollados por la propia institución participante o bien, provistos por un tercero contratado por esta y radican en equipos de los participantes. Los incidentes 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 operan estos aplicativos.



El incidente consistió en la fabricación o inyección de órdenes de transferencia apócrifas en los sistemas de donde se envían las instrucciones de pago de los participantes afectados. Si bien las investigaciones de estos incidentes siguen en curso, el "modus operandi" identificado hasta el momento es el siguiente:

- Personas no autorizadas vulneran la infraestructura tecnológica de los participantes y generan en sus sistemas órdenes de transferencias apócrifas, con cargo a las cuentas transaccionales de las instituciones participantes. Ello sucede en alguna etapa del proceso que se realiza en los aplicativos de dichos participantes para conectarse al SPEI.

- Las órdenes de transferencias siempre incluyen una cuenta emisora y una receptora. En el caso de las operaciones apócrifas, 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 vulnerados firmaron y enviaron al SPEI órdenes de transferencias apócrifas validadas por dichos sistemas como si fueran genuinas.

- El SPEI, al recibir las órdenes de transferencias, revisa que estén firmadas por los participantes, las procesa y lleva a cabo su liquidación mediante el abono del monto respectivo en la cuenta que le lleva a la institución participante receptora.

- 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 fondos apócrifa).

- Finalmente, pretendían que los recursos transferidos de conformidad con lo antes descrito fueran retirados mediante disposiciones de efectivo.

Los participantes afectados se percataron de estas órdenes de transferencia apócrifas 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, en algunos casos, las transferencias apócrifas que pudieron identificarse fueron detenidas por los participantes receptores, con lo que en esos casos se evitó la disposición indebida de parte de los recursos derivados de estas transferencias apócrifas.

En todos los casos identificados y reportados en donde hubo un incidente cibernético, los participantes tenían aplicativos de conexión al SPEI desarrollados por un tercero. No obstante, la vulnerabilidad pudo tener su origen tanto en los sistemas desarrollados por terceros, como en la infraestructura de los participantes 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 para la operación del SPEI. Cabe señalar que el Banco de México no certifica ni valida a los proveedores de este tipo de servicios y su adecuado funcionamiento es responsabilidad de cada participante. El cuadro 4 presenta la proporción de mercado por volumen y monto operado a través de los citados proveedores externos, tanto en instituciones participantes vulneradas como en aquellas otras instituciones participantes en riesgo por utilizar estos proveedores, en comparación con la proporción del resto de los participantes.

Los recursos y la información de los clientes nunca estuvieron en riesgo. Quienes cometieron estas acciones buscaron vulnerar las conexiones de los participantes con el SPEI, lo cual involucró únicamente recursos de la institución afectada. Más aún, los recursos y la información de los clientes radican en un sistema independiente al que se usa para procesar las órdenes de transferencia, con validaciones de autenticidad individuales por operación, y a la fecha no se cuenta con indicio alguno de que los sistemas donde radica la información de los recursos de los clientes hayan sido atacados.

Asimismo, 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 las órdenes de transferencias electrónicas entre los participantes con seguridad, y solo en algunos casos, con mayores tiempos de procesamiento.

La afectación a los clientes ha sido la ralentización de las transferencias para aquellas operaciones en las que participa alguna institución afectada o que opera bajo el esquema alterno para enviar órdenes de transferencia a través del SPEI.

Cuadro 4. Porcentaje de mercado de participantes afectados y no afectados*

	Número de operaciones (% del total)	Monto de operaciones (% del total)
Instituciones directamente atacadas (5)	12.89	7.69
Instituciones con un perfil de riesgo alto y que deben usar COA SPEI (incluye las directamente atacadas)	19.38	28.84
Instituciones no afectadas con proveedor externo	10.28	18.55
Instituciones no afectadas con desarrollo propio	70.34	52.61

*Estas cifras consideran el promedio diario operado en el periodo octubre 2017 – mayo 2018. Los datos mostrados excluyen al sistema de liquidación de valores por no tener instrucciones directas del público en general.

IV. Acciones adoptadas ante los eventos

Protocolo general de reacción ante eventos de seguridad de la información

En cada evento presuntamente relacionado con algún posible ataque de seguridad de la información, se aplica un protocolo que implica la desconexión de la institución participante vulnerada y el inicio de operación a través de esquemas de contingencia. Para estos fines, el Banco de México cuenta con el esquema de conexión paralelo de operación alterna para hacer transacciones en el SPEI denominado "Cliente de Operación Alterno SPEI" ("COA SPEI"), el cual es un procedimiento semiautomático que permite a los participantes operar desde una plataforma distinta y por lo tanto, más segura. Conforme a las Reglas del SPEI, todos los participantes deben contar con COA SPEI y su personal debe estar capacitado para cumplir con la obligación de usarlo cuando el Banco de México lo indique.

Una vez identificados los casos de vulneración a alguna institución participante, se identifican elementos de riesgo que pueden resultar comunes a otros participantes. Con base en esta información, el Banco de México emite un comunicado avisando a aquellos participantes en los que se identificó un mayor riesgo que tendrán que conectarse al SPEI a través del COA SPEI 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 de fondos se realicen de manera más lenta debido a que estas no se envían y/o abonan en tiempo real.

Derivado de las vulneraciones a 5 participantes del SPEI, se identificó que otros 43 participantes tenían un alto perfil de riesgo, por lo que el Banco de México les requirió conectarse al SPEI a través del esquema de contingencia COA SPEI. Para lograr un menor impacto sobre los clientes finales, se ha mantenido un esquema continuo de apoyo a los participantes que han presentado dificultades para operar con el COA SPEI. Como resultado de esto, el número de operaciones y los montos operados no han variado respecto a lo observado durante periodos de operación habitual, como se puede apreciar en el número de operaciones y montos operados en el SPEI en las gráficas 1.1, 1.2, 2.1, 2.2, 3.1 y 3.2 siguientes. Cabe destacar que el número de operaciones que involucran el uso del COA SPEI representan alrededor del 40% del total. Si bien algunas de ellas se han ralentizado por lo ya expuesto, prácticamente todas ellas se han liquidado el mismo día de su concertación. El resto de las operaciones (60%), se siguen liquidando en segundos.

Gráfica 1.1. Número de operaciones en el SPEI

Número de operaciones diarias en el SPEI durante la contingencia*

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

** Mes a partir del cual se inició la operación a través de un mecanismo de operación alterno.

*** Información al 20 de junio de 2018.

Gráfica 1.2. Mondo de las operaciones en el SPEI

Monto diario de operaciones en el SPEI durante la contingencia*

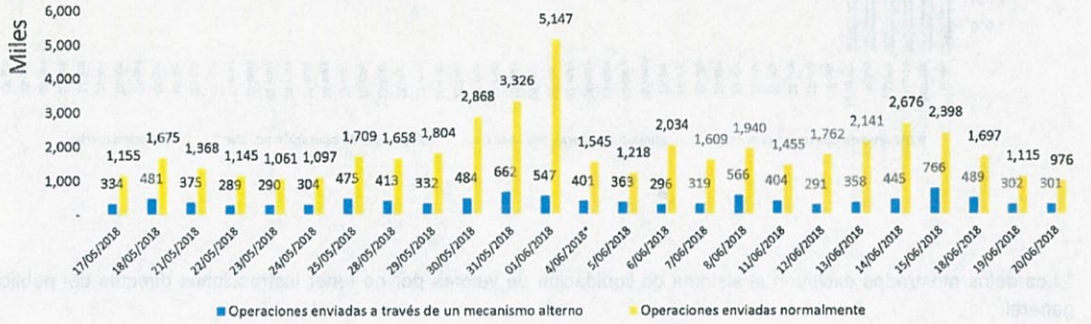
* Los datos mostrados excluyen al sistema de liquidación de valores por no tener instrucciones directas del público en general.

** Mes a partir del cual se inició la operación a través de un mecanismo de operación alterno.

*** Información al 20 de junio de 2018.

Gráfica 2.1. Número de operaciones enviadas en el SPEI

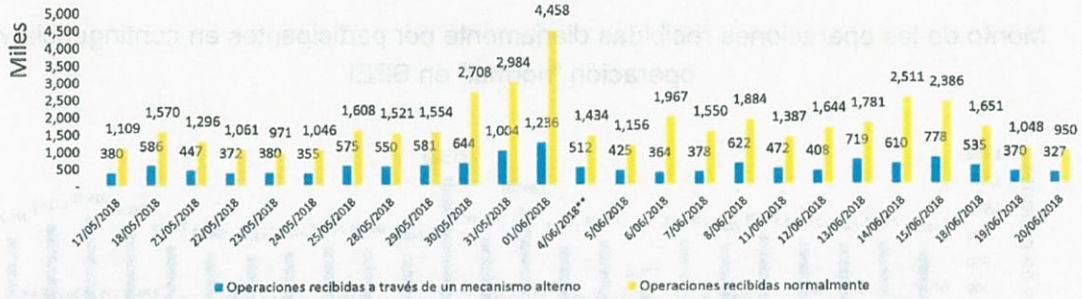
Número de operaciones enviadas diariamente por participantes en contingencia y operación "normal" en SPEI



* Para este caso no se han eliminado las operaciones que tienen a Indeval como receptor.

Gráfica 2.2. Número de operaciones recibidas en el SPEI

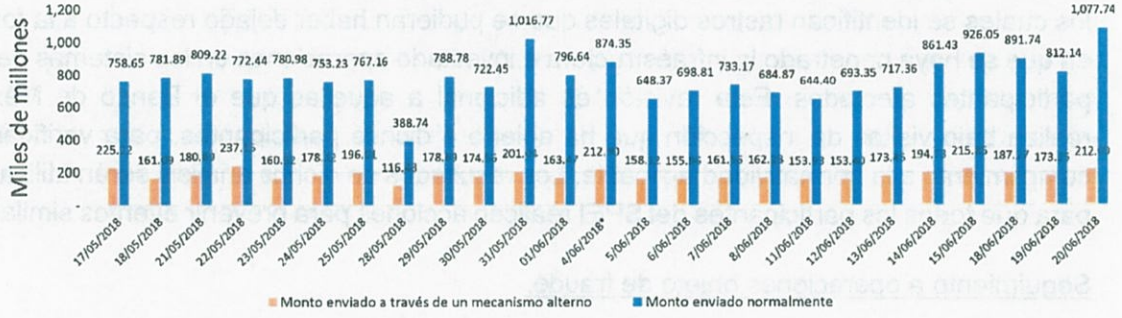
Número de operaciones recibidas diariamente por participantes en contingencia y operación "normal" en SPEI



** Para este caso no se han eliminado las operaciones que tienen a Indeval como emisor.

Gráfica 3.1. Monto de las operaciones enviadas en el SPEI

Monto de las operaciones enviadas diariamente por participantes en contingencia y operación "normal" en SPEI



* Para este caso no se han eliminado las operaciones que tienen a Indeval como receptor.

Gráfica 3.2. Monto de las operaciones recibidas en el SPEI

** Para este caso no se han eliminado las operaciones que tienen a Indeval como emisor.

Acciones tecnológicas.

El Banco de México requirió a los participantes cuyos aplicativos fueron atacados que iniciaran procesos de análisis forense por parte de auditores independientes para identificar las posibles causas de estos incidentes. Estos análisis son procesos técnicos a través de los cuales se identifican rastros digitales que se pudieran haber dejado respecto a la forma en que se haya penetrado la infraestructura e inyectado operaciones en los sistemas de los participantes afectados. Esta revisión es adicional a aquellas que el Banco de México realiza bajo visitas de inspección que ha abierto a dichos participantes, para verificar su cumplimiento a la normatividad aplicable. Los resultados de dichos análisis serán utilizados para que todos los participantes del SPEI realicen acciones para prevenir eventos similares.

Seguimiento a operaciones objeto de fraude.

El Banco de México requirió a las 5 instituciones participantes vulneradas que entregaran información respecto al estado que guardan las operaciones no reconocidas. Conforme a dicha información, estas operaciones se enviaron a 836 diferentes cuentas en 10 instituciones de crédito. Las cuentas se abrieron en 97 diferentes plazas de la República[24] y el 80% del monto total de las transferencias no reconocidas se envió a 23 plazas.

[24] Una plaza constituye una ubicación geográfica en el país, que las instituciones de crédito utilizan para identificar en dónde están abiertas las cuentas de sus clientes.

Acciones legales.

De acuerdo con la información dada a conocer por la Procuraduría General de la República[25], esta autoridad está llevando a cabo las investigaciones conducentes con el fin de identificar y sancionar a los responsables de este probable hecho ilícito.

Acciones regulatorias

El Banco de México emitió disposiciones que otorgan a los participantes en el SPEI la posibilidad de implementar medidas de control adicionales con el fin de 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 SPEI 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. En el Anexo 1 se detallan las citadas disposiciones.

V. Procesos y mecanismos para salir de la contingencia

El SPEI está listo para que todos los participantes que operan bajo el esquema de contingencia COA SPEI se reincorporen a la operación habitual del SPEI, una vez que se tenga la certeza de que los riesgos identificados están mitigados y la operación puede realizarse con plena seguridad. En ese sentido el Banco de México ha definido los requerimientos técnicos y operativos mínimos para que los participantes regresen al esquema de operación habitual. Se tienen dos grupos de requerimientos dependiendo del nivel de afectación de los participantes operando en contingencia.

A los participantes que no fueron afectados por un incidente, pero que operan en contingencia desde sus instalaciones por su condición de riesgo se les solicitará lo siguiente:

- La infraestructura de telecomunicaciones debe tener únicamente las conexiones necesarias para operar el SPEI y debe estar adecuadamente aislada del resto de la red de los participantes.
- La infraestructura de cómputo en la que pretendan operar con su aplicativo debe ser dedicada, estar libre de elementos maliciosos, actualizada y no contener componentes que no sean indispensables para operar con el SPEI.
- Contar con un aplicativo que corrija las vulnerabilidades que fueron atacadas en algún otro participante.

[25] Procuraduría General de la República, Comunicado de Prensa 500/18.

- Una certificación por parte de un auditor externo independiente de que el código de sus aplicativos no presenta código malicioso y se le han subsanado las brechas de seguridad detectadas.

Para los participantes que fueron afectados, además de los requerimientos anteriores se les solicitará lo siguiente:

- Los servidores del *core* bancario deberán contar con herramientas informáticas que permitan la detección de códigos maliciosos. Asimismo, se deberá configurar una revisión automática completa al equipo para identificar y neutralizar código malicioso al menos una vez a la semana.

- Los servidores del *core* bancario y los equipos de telecomunicaciones que controlan el acceso a dichos servidores deberán estar actualizados a versiones publicadas por el fabricante que no tengan vulnerabilidades.

- Los servidores del *core* bancario deberán seguir las mejores prácticas internacionales o las recomendadas por el proveedor para aplicar las configuraciones de seguridad a su sistema operativo.

- En cada uno de los equipos del *core* bancario, instalar solo las aplicaciones, servicios y software necesarios para la operación.

- Cambiar las contraseñas de todas las cuentas con privilegios de administración, en todos los componentes del *core* bancario (servidores, ruteadores, DNS, etc.). Por otro lado, ningún componente deberá usar contraseñas que vengan asignadas por default.

Para que los participantes de ambos grupos puedan regresar al esquema de operación habitual, deberán presentar una carta firmada por su director general, así como por el máximo responsable de sistemas, en la que establezcan que cumplen los requisitos mínimos antes descritos. Dicha carta también tendrá que ser firmada por un auditor.

VI. Supervisión

Como se mencionó, las Reglas del SPEI se publicaron en el Diario Oficial de la Federación el 4 de julio de 2017, y las obligaciones particulares de gestión de riesgo operacional y seguridad informática entraron en vigor a partir del 31 de enero de 2018. La supervisión del cumplimiento de estas obligaciones inició a partir de esa fecha conforme al programa anual instrumentado por Banco de México para estos propósitos. Por otro lado, las Reglas del SPEI establecen como obligación de cada participante evlauar el cumplimiento de, entre otras obligaciones, las de seguridad informática y gestión de riesgo operacional, a través de revisiones que realicen cada dos años, de manera alternada, el titular del área de auditoría interna del propio participante y el, o los auditores externos independientes.

Las Reglas del SPEI establecían la fecha del 28 de febrero del presente año para la entrega por parte de las instituciones participantes del primero de dichos reportes de cumplimiento. Sin embargo, de los 100 participantes del SPEI, 47 entregaron su reporte en tiempo y 50 solicitaron prórroga para su envío con fecha límite el 18 de mayo[26].

Con el fin de verificar el cumplimiento de toda la normatividad emitida por el Banco de México, este puede realizar visitas ordinarias (i.e., programadas para cada año) y extraordinarias. Al final de cada año el Instituto Central realiza un proceso de planeación para definir las visitas de supervisión ordinarias que realizará en el siguiente año, el cual tiene como criterio principal de priorización la importancia de los temas regulatorios a supervisar, así como las entidades cuya operación resulte más relevante en dichos temas. Estas visitas se realizan en coordinación con otras autoridades financieras, para lograr sinergias y para evitar saturar a las instituciones supervisadas. Con el objetivo de atender la contingencia derivada de los ataques informáticos a los participantes, se dio inicio a visitas extraordinarias para obtener la evidencia de los probables incumplimientos a la norma, mismas que han sido priorizadas de manera tal que atiendan los puntos y entidades que mostraron mayor vulnerabilidad durante el proceso reciente y de manera adicional aquellas entidades cuyo volumen de operación sea mayor.

Derivado de los procesos de supervisión iniciados a partir de 2017 a los participantes el SPEI y a otros sistemas de pagos operados por el Banco de México, de la evidencia detectada hasta el momento y de los reportes de los auditores externos, se tienen indicios que pueden llevar a presumir que existe un nivel de cumplimiento heterogéneo y en algunos casos deficiente en los requerimientos de seguridad informática y continuidad operativa.

VII. Coordinación entre autoridades

Para facilitar que se establezcan mecanismos con el objeto de que las entidades participantes consideren la reducción del riesgo que su participación en un sistema genera a otros participantes y al sistema en su conjunto, en relación con la seguridad de la información en sus procesos de toma de decisión, se requiere que las autoridades establezcan reglas claras y procesos de supervisión y sanción que permitan que las decisiones de inversión lleguen al niveles consistentes con el buen funcionamiento del sistema, así como una adecuada coordinación entre autoridades financieras. Bajo esta consideración, el 24 de mayo pasado, el Banco de México celebró las Bases de Coordinación en Materia de Ciberseguridad de la Información, junto con las demás autoridades financieras (SHCP, CNBV, CNSF, CONSAR y CONDUSEF), la PGR y las principales asociaciones gremiales (ABM, AMIB, AMIS, AMIG, AMAFORE, AMSOFIPO,

[26] Cabe señalar que las Reglas exceptúan de la entrega de este requerimiento al Banco de México, a CLS y al Fondo Mexicano del Petróleo para la Estabilidad y Desarrollo, dado que en todos los casos el procesamiento de sus operaciones es realizado por sistemas y personal del Banco de México.

AAGEDE, ASOFOM, Asociación Fintech México, AFICO Y CONCAMEX). En este instrumento se establecen las bases para la colaboración y coordinación entre las instancias públicas y con las asociaciones gremiales en materia de seguridad de la información.

Estas Bases formalizan el acuerdo de las autoridades financieras para mantener una coordinación efectiva entre ellas, con el fin de determinar los principios aplicables que cada una podría implementar mediante la regulación que le corresponde emitir en el ámbito de sus respectivas competencias, de tal manera que procurarán mantener un tratamiento homogéneo sobre los requisitos y prácticas que las entidades financieras deberán observar en esa materia. De conformidad con las Bases, las autoridades financieras establecerán un grupo de trabajo regulatorio encargado de (i) definir las mejores prácticas y estándares que deberían observar todas las entidades financieras y (ii) precisar la regulación que resulte más eficaz para imponer dichas prácticas y estándares. Adicionalmente, entre los principales aspectos contemplados en las Bases se encuentran: i) el acuerdo de las autoridades financieras de mantener una coordinación efectiva entre ellas para determinar los principios en materia de seguridad informática que cada una podría implementar mediante la regulación que le corresponde en el ámbito de sus facultades; ii) la creación por parte de las autoridades financieras del Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información (GRI), el cual coordinará las acciones a implementar por parte de estas autoridades en caso de incidentes sensibles de seguridad de la información; iii) la obligación por parte cada institución reguladas de la creación de un grupo interno de identificación y respuesta a incidentes sensibles de seguridad de la información, así como de informar a la autoridad financiera competente sobre la ocurrencia de dichos incidentes; iv) la colaboración de la Procuraduría General de la República con las autoridades financieras y las instituciones reguladas sobre hechos posiblemente constitutivos de delitos; y v) la promoción por parte de las asociaciones gremiales de la difusión de información sobre seguridad de la información, la colaboración y coordinación con las autoridades financieras y el cumplimiento de las Bases.

En el mismo sentido, el Consejo de Estabilidad del Sistema Financiero (CESF)[27], en su sesión del 14 de junio de 2018, dio seguimiento a las acciones que se vienen realizando para reforzar la regulación y la supervisión en materia de seguridad de la información, y acordó impulsar el reforzamiento de esta sobre la base de los siguientes 10 principios:

[27] El Consejo, constituido conforme a lo dispuesto por la Ley para Regular las Agrupaciones Financieras, está integrado por representantes de la Secretaría de Hacienda y Crédito Público, la Comisión Nacional Bancaria y de Valores, la Comisión Nacional de Seguros y Fianzas, la Comisión Nacional del Sistema de Ahorro para el Retiro, el Instituto para la Protección al Ahorro Bancario y el Banco de México. Sus sesiones son presididas por el Titular de la Secretaría de Hacienda y Crédito Público, en su ausencia por el Gobernador del Banco de México y, en ausencia de ambos, por el Subsecretario de Hacienda y Crédito Público. La Secretaría Ejecutiva del Consejo está a cargo de un funcionario del Banco de México.

1. **Gobierno corporativo en el que la seguridad de la información ocupe un lugar central**: las entidades deben contar con una unidad administrativa en los niveles más altos de la organización, que defina políticas y estrategias, conforme a las mejores prácticas y estándares internacionales, y sea responsable de la seguridad de la información de la entidad.

2. **Esquemas de protección de datos robustos**: contar con mecanismos y procesos para una gestión segura de todos los activos de información de la entidad; independiente de si dicha información se almacena en medios electrónicos o físicos.

3. **Administración de riesgos de seguridad de la información**: la metodología de administración de riesgos de la entidad, deberá contar con un apartado específico de medición y gestión de riesgos de seguridad de la información.

4. **Controles de seguridad en los puntos de acceso**: los procedimientos de acceso a dispositivos, equipos y servidores deberán contemplar esquemas de gestión de claves, permisos y roles; que garanticen que solo pueden acceder quienes lo requieren y por el tiempo que lo requieren. Así mismo, se deberá contar con herramientas que controlen y monitoreen el acceso a dispositivos, equipos y servidores.

5. **Protocolos de respuesta a incidentes y eventos críticos**: las entidades deberán contar con procedimientos claros y documentados para responder ante un incidente que vulnere sus mecanismos de protección, y considerar en dichos protocolos escenarios donde, con motivo del incidente, el impacto escale a nivel sistémico, dentro o fuera de la entidad.

6. **Identificación de exposición a riesgos por parte de terceros (proveedores y usuarios)**: las entidades deberán asegurarse que sus proveedores de servicios y aplicaciones cumplen con niveles de seguridad de la información conforme a las políticas que defina su órgano de gobierno de la seguridad de la información.

7. **Políticas de protección a la infraestructura**: los centros de datos, así como la infraestructura de cómputo y de telecomunicaciones deberá ser gestionada conforme a las mejores prácticas y estándares de seguridad de la industria; y en apego a las políticas que defina el órgano de gobierno de la seguridad de la información de la entidad.

8. **Políticas de protección a los sistemas**: las aplicaciones, bases de datos y sistemas informáticos con que cuente la entidad deberán estar protegidos y gestionados de forma segura, conforme a las mejores prácticas y estándares internacionales, y en apego a las reglas que defina el órgano de seguridad de la información.

9. **Programa de capacitación y de fomento de una cultura de la seguridad informática**: el personal deberá estar capacitado y ser consciente de que la protección de la información es responsabilidad de cada empleado; las áreas de tecnología, seguridad de la información

o de políticas de seguridad de la información, proveen herramientas o lineamientos, pero es responsabilidad de cada individuo conocer la criticidad de la información que maneja y protegerla concordancia.

10. **Programas de educación y fomento de una cultura de seguridad informática para el uso que hacen los clientes de los servicios financieros:** Las entidades deberán redoblar sus esfuerzos para promover entre sus clientes un pleno conocimiento de sus aplicativos y las prácticas de seguridad que deben de seguir.

VIII. Consideraciones finales

En abril y mayo del presente año se registraron una serie de incidentes cibernéticos en los aplicativos e infraestructura que usan algunas instituciones financieras para preparar y mandar órdenes de transferencia a través del SPEI. La regulación del SPEI contiene requerimientos de seguridad informática enfocados a mitigar el riesgo de este tipo de incidentes. No obstante lo anterior, existen indicios que podrían llevar a presumir que el nivel de cumplimiento de estos requisitos por parte de los participantes es heterogéneo y en algunos casos deficiente. El Banco de México está realizando acciones de supervisión para verificar el cumplimiento de la regulación del SPEI, que son adicionales a las incluidas en su programa anual de supervisión.

Los incidentes observados dieron como resultado afectaciones en las cuentas transaccionales de las instituciones participantes en el SPEI (bancos, casas de bolsa, etc.), y no afectaron las cuentas ni los recursos de los clientes. No obstante, para salvaguardar la seguridad del sistema de pagos, tanto a los participantes vulnerados como a los que se identificaron con un alto riesgo de poder ser vulnerados se les instruyó la migración de sus operaciones del SPEI a una red alterna y segura. Sin embargo, al tratarse de un sistema alterno y semiautomático, los tiempos de servicio de las instituciones que migraron al sistema alterno se vieron afectados. En este sentido, algunos clientes tuvieron afectaciones por la ralentización de las transferencias asociadas a operaciones en las que participa alguna de las instituciones que fueron afectadas o que migraron su operación al esquema alterno para el envío de órdenes de transferencias a través del SPEI. Esta ralentización se normalizará gradualmente conforme este conjunto de instituciones realice las correcciones necesarias para adecuar sus sistemas e infraestructura y prevenir incidentes como los que se presentaron.

El SPEI sigue procesando órdenes de transferencia entre los participantes con seguridad, aunque en algunos casos con retrasos en los tiempos de servicio. Las instituciones participantes que han sido afectadas han venido mejorando su nivel de operación en el SPEI, en la medida que se han estabilizado los procesos contingentes.

La seguridad de la información es un tema fundamental para la confianza de los usuarios en el sistema financiero. Aunado a esto, los niveles elevados de interconexión de los participantes pueden generar problemas como la toma de decisiones que no consideren los

impactos que las mismas tienen sobre todo el sistema y que sean las adecuadas para lograr los mayores beneficios de la operación del sistema financiero. Un ejemplo de esto es que la seguridad de la información de una red, depende del eslabón más vulnerable de la cadena, por lo que un ataque sin el adecuado tratamiento puede convertirse de un tema individual en uno sistémico. Es por ello que los requerimientos mínimos en seguridad de la información son indispensables y se reforzarán tanto las normas como su supervisión.

Existe una coordinación y comunicación entre autoridades financieras competentes con el fin de dar un seguimiento a los hechos. Más aún, se han establecido las bases para que los eventos de seguridad de la información sean tratados de forma integral entre las autoridades e instituciones financieras. Es necesario contar con mecanismos para lograr que las entidades consideren los costos para el sistema de posibles ataques al momento de tomar sus decisiones de inversión y, para ello, es necesario que las autoridades establezcan reglas claras y procesos de supervisión y sanción que permitan que las decisiones de inversión logren alcanzar al niveles consistentes con el buen funcionamiento del sistema, así como una adecuada coordinación entre dichas autoridades. Al respecto destaca la firma de las bases de coordinación en materia de seguridad de la información entre autoridades y representantes del sistema financiero.

El Banco de México analizará los diagnósticos de los análisis forenses de las instituciones vulneradas y comunicará en su página de internet las acciones adoptadas, recomendaciones y pasos a seguir. A través de su participación en el Grupo de Respuesta a Incidentes, que establecen las Bases de Coordinación en materia de seguridad de la información, este Instituto Central impulsará protocolos de respuesta y comunicación oportuna entre instituciones y autoridades.

Sin otro asunto que tratar, reiteramos a usted las seguridades de nuestra atenta y distinguida consideración.

A t e n t a m e n t e,

BANCO DE MÉXICO

Mtro. José Jaime Cortina Morfin
Director General de Operaciones y Sistemas de Pagos

Mtro. Luis Urrutia Corral
Director General Jurídico.

Anexo 1.

Disposiciones emitidas para mitigar las afectaciones por los incidentes de seguridad informática

Mediante las modificaciones a las "Disposiciones generales aplicables a los participantes en los sistemas de pagos administrados por el Banco de México y a los demás interesados en actuar con tal carácter", contenidas en la Circular 4/2018, publicada en el Diario Oficial de la Federación del 17 de mayo de 2018, se impuso a 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.

Por otra parte, mediante modificaciones a las Reglas SPEI contenidas en la Circular 5/2018, publicada en el Diario Oficial de la Federación del 17 de mayo de 2018, se permite a los participantes del SPEI 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 $50,000 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). 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. A la fecha de emisión de este reporte, ningún participante ha solicitado la autorización antes referida.