REPORTE DE COMENTARIOS A LA CONSULTA PÚBLICA DEL PROYECTO DE DISPOSICIONES PARA MODIFICAR LAS REGLAS DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS, EMITIDAS MEDIANTE LA CIRCULAR 14/2017, EN MATERIA DE CIBERSEGURIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN

Fecha de elaboración: 30 de enero de 2024

Periodo de consulta: del 3 de agosto de 2023 al 30 de agosto de 2023.

El presente reporte contiene el análisis que el Banco de México ha realizado acerca de los comentarios al proyecto de disposiciones para modificar las "Reglas del Sistema de Pagos Electrónicos Interbancarios", emitidas mediante la Circular 14/2017, en materia de ciberseguridad y tecnologías de la información. Dichos comentarios fueron recibidos como parte del proceso de consulta pública referido, que el propio Banco llevó a cabo del 3 de agosto de 2023 al 30 de agosto del 2023. A este respecto, el contenido de este reporte en ningún caso constituye una decisión o postura oficial definitiva del Banco de México y, por lo tanto, no se deberá considerar como un documento que produzca efectos vinculatorios, genere derechos u obligaciones o fije aspectos de política pública.

Este reporte tiene por objeto exponer el análisis realizado por el Banco de México y dar a conocer su opinión sobre los comentarios y la información presentada por los participantes en la consulta pública llevada a cabo del 3 de agosto de 2023 al 30 de agosto del 2023, respecto del proyecto de disposiciones para modificar las "Reglas del Sistema de Pagos Electrónicos Interbancarios" (en adelante las "Reglas"), emitidas mediante la Circular 14/2017, en materia de ciberseguridad y tecnologías de la información, para modificar el marco regulatorio de ciberseguridad aplicable al Sistema de Pagos Electrónicos Interbancarios (SPEI), con el propósito de: i) dotar de mayor claridad al elemento de infraestructura tecnológica sobre el cual se debe observar el cumplimiento del referido marco legal y ii) precisar, así como actualizar los elementos obligacionales que los participantes del SPEI deben cumplir respecto a los requisitos de seguridad informática actualmente incluidos en las Reglas. Asimismo, se incluyen elementos adicionales que permiten reforzar el marco de ciberseguridad de los participantes del SPEI.

De conformidad con lo establecido en las Políticas para la consulta pública de las disposiciones de carácter general que emita el Banco de México, emitidas por la Junta de Gobierno de este Instituto Central, se pone a disposición del público el presente reporte de comentarios.

Durante el periodo de la consulta, el Banco de México recibió a través del micrositio establecido en su portal de internet para estos efectos (https://www.banxico.org.mx/ConsultaRegulacionWeb/details.jsp?id=4063), comentarios de trece participantes, presentados a nombre de: 1) David Vicente Jiménez, 2) Bank of America México, 3) Oscar German Gutiérrez Torres, 4) Asociación Mexicana de Instituciones Bursátiles, 5) Asociación Mexicana de Internet, 6) Banco Nacional de México, 7) Asociación Fintech México, 8) Banco Azteca, 9) MUFG Bank México, 10) Banco JP Morgan, 11) Asociación de Bancos de México, 12) CIBanco y 13) SD. Indeval. (Cuadro 1). Los mencionados comentarios se encuentran a disposición del público en el micrositio referido.

Cuadro 1: Relación de los participantes en la consulta pública

	Participantes	Fecha de recepción
1	David Vicente Jiménez	22/08/2023
2	Bank of America México	24/08/2023
3	Oscar German Gutiérrez Torres	29/08/2023
4	Asociación Mexicana de Instituciones Bursátiles	29/08/2023
5	Asociación Mexicana de Internet	29/08/2023
6	Banco Nacional de México	29/08/2023
7	Asociación Fintech México	30/08/2023
8	Banco Azteca	30/08/2023
9	MUFG Bank México	30/08/2023
10	Banco JP Morgan	30/08/2023
11	Asociación de Bancos de México	30/08/2023
12	CIBanco	30/08/2023
13	SD. Indeval	30/08/2023

Objetivos de la consulta pública

El proyecto de disposiciones tiene por objeto robustecer y mantener actualizado el marco de ciberseguridad aplicable a los participantes del SPEI conforme a las mejores prácticas y estándares internacionales, detallando las medidas de protección específicas para la infraestructura de cómputo y la infraestructura de telecomunicaciones que utilizan los participantes para conectarse con el SPEI. Por otra parte, se propuso establecer la obligación a cargo de aquellos participantes del SPEI que tengan el carácter de institución para el depósito de valores, de implementar procedimientos de contingencia que les permitan mantener su conexión al SPEI mediante el uso de una tecnología diferente a la empleada normalmente en su infraestructura tecnológica, en términos similares a como al día de hoy se contempla para otro tipo de participantes.

I. Comentarios que derivaron en modificaciones a las disposiciones

i. Definiciones

Se recibieron comentarios a la definición propuesta de “Centro de Datos”. Asimismo, diversos participantes de la consulta sugirieron adicionar la definición de “Ciberresiliencia”.

Opinión del Banco de México

Se ajustó la definición de "Centro de Datos" para acotarla a aquellos sitios de alojamiento físico utilizados por el participante para operar en el SPEI.

Adicionalmente, con el objetivo de aclarar el alcance del término "Ciberresiliencia", se agregó su definición; entendida como la capacidad del participante de prevenir, adaptar, responder o recuperar su operación en el SPEI ante ciberataques o incidentes que puedan afectar a la confidencialidad, integridad, disponibilidad o continuidad operativa de la infraestructura tecnológica, así como de la información que esta utilice.

ii. Sobre el uso de distintas soluciones que permitan a los participantes dar cumplimiento a lo solicitado dentro de los requisitos de seguridad informática

Diversos comentarios recibidos externaron preocupaciones sobre la posibilidad de que el proyecto de disposiciones pudiera no contemplar las posibles soluciones con las cuales se pudiera dar cumplimiento a lo solicitado.

Opinión del Banco de México

Se incluyó un apartado para prever que el Banco de México pueda autorizar el uso de mecanismos de control alternos para algunos de los requisitos establecidos. Cabe reiterar que, si los participantes del SPEI contratan a un tercero para la provisión de algún producto o servicio necesario para operar con el sistema, la obligación de demostrar el cumplimiento a la normatividad aplicable la mantiene el participante del SPEI.

iii. Plazos de implementación previstos en los transitorios

Diversas entidades consideraron que los plazos establecidos podrían ser insuficientes para completar los desarrollos y ajustes solicitados.

Opinión del Banco de México

En atención a los comentarios y a la evaluación realizada por el Banco de México, se determinó procedente ajustar los plazos de implementación previstos en las reglas transitorias, a periodos de doce y veinticuatro meses en los casos respectivos.

Cabe señalar que, en su mayoría, los ajustes corresponden a la reorganización y precisión de ciertos elementos de los requisitos, por lo que los participantes deben estar en posibilidad de dar cumplimiento dentro de los plazos transitorios establecidos. Para los nuevos requisitos que se incluyeron se establecieron plazos de implementación de veinticuatro meses.

iv. Acotación de diversos términos

En términos del numeral 5 del inciso b) del apartado A de la fracción I de la 58a. del proyecto de modificaciones a las Reglas, se prevé que los participantes deben considerar el detectar y gestionar incidentes de seguridad informática en la infraestructura tecnológica del SPEI, así como en otras infraestructuras. Como resultado de lo anterior, se recibieron algunas inquietudes respecto al alcance del término "otras infraestructuras".

Asimismo, se recibieron comentarios relativos a especificar a qué medios se refiere el término "medios extraíbles de almacenamiento de información" previsto en el numeral 5 del inciso g) del apartado A de la fracción I de la 58a. del proyecto de modificaciones a las Reglas.

Finalmente, se recibieron comentarios respecto a las políticas de filtrado de datos de las infraestructuras de cómputo y telecomunicaciones.

Opinión del Banco de México

Se ajustó el numeral 5 del inciso b) del apartado A de la fracción I de la 58a. de las Reglas con la finalidad de aclarar que el término "otras infraestructuras" se refiere a aquellas infraestructuras utilizadas por la propia institución cuya falla pudiera derivar en una afectación a su operación en el SPEI.

Por lo que respecta a los medios extraíbles de almacenamiento de información, se aclaró que estos se refieren a aquellos relacionados con el respaldo de información del SPEI.

Adicionalmente, se realizaron ajustes al numeral 6 del inciso f) del apartado A de la fracción I de la 58a. de las Reglas para dar mayor claridad respecto al elemento regulatorio aplicable a generar e implementar las políticas de filtrado de datos dentro de las señaladas infraestructuras.

II. Comentarios que no derivaron en ajustes a las disposiciones

i. Operación con el SPEI utilizando infraestructuras tecnológicas en la nube

Un grupo de participantes de la consulta realizaron diversos comentarios respecto a la operación en el SPEI utilizando infraestructuras tecnológicas en la nube.

Opinión del Banco de México

Se considera necesario precisar que los requisitos para operar en el SPEI siguen el principio de neutralidad tecnológica, por lo que los participantes pueden definir la arquitectura o tecnología particular a utilizar para operar en el SPEI, siempre y cuando esta dé cumplimiento a los requisitos previstos en la normatividad correspondiente. La normativa aplicable al sistema no restringe la implementación de un tipo de infraestructura en particular, manteniendo una postura neutral.

Cabe reiterar que, si los participantes del SPEI contratan a un tercero para la provisión de algún producto o servicio necesario para operar con el sistema, incluyendo los servicios de infraestructura tecnológica en la nube, la obligación de demostrar el cumplimiento a la normatividad aplicable la mantiene el participante del SPEI.

ii. Implementación del mecanismo de contingencia previsto en el párrafo octavo de la 46a. de las Reglas del SPEI para instituciones para el depósito de valores

El proyecto estableció la obligación a las instituciones de depósito de valores que participan en el SPEI de implementar el mecanismo de contingencia previsto en el párrafo octavo de la 46a. de las Reglas del SPEI. Por lo anterior, un participante de la consulta pública solicitó aclarar si es aplicable el plazo de trescientos sesenta y cinco días para la implementación del referido mecanismo para las instituciones de depósito de valores que tuvieran dicho carácter, previo a la emisión de las modificaciones.

Opinión del Banco de México

Para el caso de instituciones de depósito de valores que ya cuenten con el carácter de participante en el SPEI, a la entrada en vigor de las Reglas, la CUARTA transitoria del proyecto de modificaciones prevé un periodo de implementación de trescientos sesenta y cinco días hábiles posteriores a la publicación de la Circular correspondiente, siendo el 20 de noviembre de 2024 la fecha de implementación del mecanismo de contingencia señalado.

iii. Área responsable de la seguridad informática en la infraestructura tecnológica

Diversas entidades consultaron al Banco Central si el oficial de seguridad de la información del SPEI debe formar parte del área responsable de seguridad informática en la infraestructura tecnológica a que refiere el inciso a) del apartado A de la fracción I de la 58a. de las Reglas.

Opinión del Banco de México

No existe la obligación de que el oficial de seguridad de la información del SPEI deba formar parte del área señalada en el párrafo anterior, por lo que esta será una determinación del participante. El participante debe verificar el cumplimiento, tanto de los requisitos establecidos para el área responsable de la seguridad informática, como de las funciones y responsabilidades del oficial de seguridad de la información del SPEI.

iv. Diversas precisiones a términos y elementos que demuestran el cumplimiento de los requisitos

Se recibió una duda respecto al uso del término "cuentas del sistema operativo", contenido en el numeral 3 del inciso d) del apartado A de la fracción I de la 58a. de las Reglas del SPEI. También se recibió un comentario en el que se solicita que el Banco de México defina o

indique herramientas o proveedores sugeridos para realizar la implementación de diversos requisitos.

Opinión del Banco de México

Por lo que respecta al uso del término "cuentas del sistema operativo", el mismo se refiere a las cuentas de administración o de usuario en el sistema operativo implementado dentro de las infraestructuras.

Adicionalmente, se estima conveniente reiterar que el Banco de México mantiene el principio de neutralidad tecnológica en las infraestructuras tecnológicas utilizadas para operar en el SPEI; por lo que no tiene previsto recomendar o establecer herramientas o proveedores específicos para el cumplimiento de la regulación que pudieran derivar en la limitación de las herramientas y mecanismos tecnológicos implementados por los participantes en el SPEI y que pudieran generar riesgos en la operación de estos con el sistema.

III. Comentarios relacionados con elementos previstos en el Manual de operación del SPEI

A continuación, se enlistan algunos de los aspectos previstos en el apartado A de la fracción I de la 58a. de las Reglas, respecto de los cuales se recibieron comentarios en los que se solicita al Banco de México especificar aspectos técnicos del cumplimiento:

1. Segmentación física o lógica, la red de la infraestructura de telecomunicaciones en distintos dominios y subredes, previsto en el numeral 3 del inciso f).

2. Descripción del área responsable de seguridad informática, conforme a lo establecido en el inciso a).

3. Protocolos y servicios no seguros, conforme a lo establecido en el numeral 1 del inciso b).

4. Alcance del monitoreo de la integridad de la información, conforme a lo establecido en el numeral 2 bis del inciso b).

5. Características de los archivos no autorizados, conforme a lo establecido en el numeral 4 bis del inciso b).

6. Borrado seguro en las infraestructuras de cómputo y telecomunicaciones, conforme a lo establecido en el numeral 1 del inciso d).

7. Características de las pruebas de penetración y de los informes correspondientes, así como del periodo de ejecución, conforme a lo establecido en el numeral 6 del inciso b).

8. Documentación de los componentes que conforman la infraestructura de cómputo y de telecomunicaciones que detalla el numeral 4 del inciso f).

9. Proceso para la implementación del aplicativo SPEI, utilizado por los participantes para conectarse con el sistema, conforme a lo establecido en el inciso c).

10. Procedimientos para detectar la alteración o falsificación de la información contenida en el aplicativo SPEI, conforme al numeral 4 del inciso d).

11. Controles y políticas al proceso de gestión de entrada y salida de equipos de cómputo y telecomunicaciones al centro de datos, detallados en el numeral 2 del inciso g).

12. Controles y políticas relacionados con los sistemas electromecánicos y de protección contra incendios, contenidos en el numeral 3 del inciso g).

13. Proceso de mantenimiento de la infraestructura de cómputo, conforme a lo establecido en el numeral 4 del inciso g).

14. Proceso de gestión del acceso físico a los medios usados para el respaldo de información, incluido en el numeral 5 del inciso g).

15. Controles y políticas del proceso de gestión del acceso remoto, conforme al contenido del numeral 6 del inciso g).

16. Periodo de resguardo de bitácoras de eventos de auditoría de las cuentas del sistema operativo, conforme a lo establecido en el numeral 3 del inciso d).

17. Periodo de resguardo de bitácoras de componentes de la infraestructura tecnológica, conforme a lo establecido en el numeral 5 bis del inciso b).

18. Definición de patrones anómalos, conforme a lo establecido en el numeral 5 bis del inciso b).

Opinión del Banco de México

Diversos comentarios recibidos durante la consulta pública abordan aspectos técnicos específicos de tratamiento sensible y reservado, cuya respuesta se ubica en el Manual de operación del SPEI que se encuentra disponible para los participantes del sistema.