REPORTE DE COMENTARIOS A LA CONSULTA PÚBLICA DEL PROYECTO DE DISPOSICIONES PARA MODIFICAR LAS REGLAS DEL SISTEMA DE PAGOS INTERBANCARIOS EN DÓLARES, EMITIDAS MEDIANTE LA CIRCULAR 4/2016, 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 Interbancarios en Dólares", emitidas mediante la Circular 4/2016, 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 Interbancarios en Dólares" (en adelante las "Reglas"), emitidas mediante la Circular 4/2016, en materia de ciberseguridad y tecnologías de la información, para modificar el marco regulatorio de ciberseguridad aplicable al Sistema de Pagos Interbancarios en Dólares (SPID), 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 SPID 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 SPID.

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=4064), comentarios de ocho

participantes, presentados a nombre de 1) Bank of America México, 2) David Vicente Jiménez, 3) Asociación Mexicana de Instituciones Bursátiles, 4) Banco Nacional de México, 5) CIBanco, 6) Asociación de Bancos de México, 7) Banco JP Morgan y 8) Banco Azteca (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	Bank of America México	21/08/2023 y 24/08/2023
2	David Vicente Jiménez	22/08/2023
3	Asociación Mexicana de Instituciones Bursátiles	29/08/2023
4	Banco Nacional de México	29/08/2023
5	CIBanco	30/08/2023
6	Asociación de Bancos de México	30/08/2023
7	Banco JP Morgan	30/08/2023
8	Banco Azteca	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 SPID, 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 al SPID.

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 con el SPID.

Adicionalmente, con el objetivo de aclarar el alcance del término “Ciberresiliencia”, se agregó la definición; entendida como la capacidad del participante de prevenir, adaptar, responder o recuperar su operación en el SPID 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. Oficial de seguridad de la información

En relación con el inciso a) de la fracción I de la 42a. del proyecto de disposiciones, en la que se establece que los participantes deben contar con un área designada como responsable de la seguridad informática, se recibieron comentarios respecto de la necesidad de designar a un oficial de seguridad de la información para el SPID.

Opinión del Banco de México

Derivado de los comentarios recibidos, se hicieron los ajustes pertinentes para incluir la figura del oficial de seguridad de la información en el SPID, en los mismos términos de la regulación aplicable del Sistema de Pagos Electrónicos Interbancarios, a fin de asegurar que los participantes del SPID cuenten con personal especializado, disponible y con la capacidad de tomar decisiones en temas de ciberseguridad del SPID.

iii. 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 SPID 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 SPID.

iv. 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.

v. Acotación de diversos términos

En términos del numeral 6 del inciso b) de la fracción I de la 42a.de las reglas del proyecto de disposiciones, los participantes deben considerar el detectar y gestionar incidentes de seguridad informática en la infraestructura tecnológica del SPID, así como en otras infraestructuras. Como resultado de lo anterior, se recibieron algunas inquietudes respecto al alcance de la referencia a "otras infraestructuras".

Asimismo, se recibieron comentarios referentes a especificar a qué medios refiere el término "medios extraíbles de almacenamiento de información" previsto en el numeral 5 del inciso f) de la fracción I de la 42a. 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 6 del inciso b) de la fracción I de la 42a. de las Reglas, con el objeto de aclarar que el término "otras infraestructuras" se refiere a infraestructuras utilizadas por la propia institución cuya falla pudiera derivar en una afectación a su operación en el SPID.

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 SPID.

Adicionalmente, se realizaron ajustes al numeral 7 del inciso e) de la fracción I de la 42a., 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. Área responsable de la seguridad informática en la infraestructura tecnológica

Se recibieron dudas referentes a la posible pertenencia del oficial de seguridad de la información del SPID al área responsable de seguridad informática en la infraestructura tecnológica a que refiere el inciso a) de la fracción I de la 42a. de las Reglas.

Opinión del Banco de México

Al respecto, no existe la obligación de que el oficial de seguridad de la información del SPID 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 SPID.

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

A continuación, se enlistan algunos de los aspectos previstos en la fracción I de la 42a. de las Reglas del SPID, sobre los cuales se recibieron comentarios en los que se solicita al Banco de México especificar aspectos técnicos del cumplimiento:

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

2. Utilización de protocolos seguros de comunicación, conforme a lo establecido en el numeral 1 del inciso b).

3. Herramientas para monitoreo de la integridad de la información, conforme a lo establecido en el numeral 2 Bis del inciso b).

4. Impedir la ejecución de archivos no autorizados, conforme a lo establecido en el numeral 4 Bis del inciso b).

5. Herramientas tecnológicas para el registro centralizado de bitácoras, conforme a lo establecido en el numeral 6 Bis del inciso b).

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

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

8. Generación y resguardo de bitácoras de eventos de auditoría, conforme a lo establecido en el numeral 3 del inciso c).

9. Segmentación física o lógica, la red de la infraestructura de telecomunicaciones en distintos dominios y subredes, de conformidad con el numeral 3 del inciso e).

10. Infraestructura de telecomunicaciones, así como la interconexión entre ellos, como lo son diagramas de red, esquemas o mapas, referidos en el numeral 4 del inciso e).

11. Implementación y almacenamiento de las bitácoras de los eventos generados por la infraestructura de telecomunicaciones, referidas en el numeral 5 del inciso e).

12. Generar y almacenar los respaldos de la configuración de la infraestructura de telecomunicaciones, mediante una o más herramientas de las contempladas en el numeral 7 del inciso e).

13. Monitorizar la infraestructura de telecomunicaciones mediante herramientas y protocolos específicos para dicha función, de conformidad con el numeral 10 del inciso e).

14. Gestión de entrada y salida de equipos de cómputo y telecomunicaciones al centro de datos, conforme a lo establecido por el numeral 2 del en el inciso f).

15. Sistemas electromecánicos y de protección contra incendios, a los que refiere el numeral 3 del inciso f).

16. Proceso de mantenimiento de los componentes de cómputo, considerados en el numeral 4 del inciso f).

17. Proceso de gestión del acceso físico a los medios usados para el respaldo de información, referido en el numeral 5 del inciso f).

18. Proceso de gestión del acceso remoto, señalado en el numeral 6 del inciso f).

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 SPID que se encuentra disponible para los participantes del sistema.