BORRADOR	3 de agosto de 2023

El presente documento refleja ciertos aspectos que el Banco de México contempla, en ejercicio de sus facultades, de manera preliminar para la emisión de las disposiciones de carácter general que en él se contienen. En razón de lo anterior, el contenido de este documento, en ningún caso, constituye una decisión o postura, oficial o definitiva, del Banco de México y, por lo tanto, no debe considerarse como un documento que produzca efectos vinculatorios, genere derechos u obligaciones o determine aspectos de política pública.

CIRCULAR **/2023

Ciudad de México, a ** de **** de 2023

A LOS PARTICIPANTES DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS Y DEMÁS INTERESADOS EN ACTUAR CON TAL CARÁCTER:

ASUNTO: MODIFICACIONES A LA CIRCULAR 14/2017 (FORTALECIMIENTO DE LAS DISPOSICIONES EN MATERIA DE CIBERSEGURIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS)

El Banco de México, con el propósito de continuar promoviendo el sano desarrollo del sistema financiero, proteger los intereses del público y propiciar el buen funcionamiento de los sistemas de pagos _____

Por lo anterior, con fundamento en los artículos 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, 2, fracciones I, IV y VIII, y 6 de la Ley de Sistemas de Pagos, 22 de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, ___ del Reglamento Interior del Banco de México, que le otorgan la atribución de expedir disposiciones a través de la ____, respectivamente, así como _____, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, ha resuelto _____ de las "Reglas del Sistema de Pagos Electrónicos Interbancarios", emitidas mediante la Circular 14/2017, para quedar en los términos siguientes:

CIRCULAR 14/2017

REGLAS DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS (SPEI)

CAPÍTULO I
Disposiciones preliminares

…

2a. Definiciones.- Para los efectos de estas Reglas, sin perjuicio del alcance o definiciones que cualquier otra normativa dé a los términos indicados a continuación, se entenderá por:

…

VI Bis. Centro de Datos:	al sitio de alojamiento físico de equipos de cómputo, telecomunicaciones y almacenamiento de información empleados por el Participante.

…

XXVII Quáter. Infraestructura de Cómputo:	los elementos de cómputo, ya sean físicos o virtuales, cuya finalidad sea el procesamiento y almacenamiento de datos utilizados por los Participantes para operar con el SPEI.
XXVII Quinquies. Infraestructura de Telecomunicaciones:	a los elementos de red físicos o lógicos, los cuales brindan el servicio de conectividad y transportan los datos de los diferentes programas de cómputo, y que son utilizados por los Participantes para interconectarse y operar con el SPEI.
XXVIII. Infraestructura Tecnológica:	a la ~~l~~Infraestructura de C~~c~~ómputo, Infraestructura de ~~t~~Telecomunicaciones~~,~~ y aplicaciones que utilizan los Participantes para interconectarse y operar con el SPEI.

…

CAPÍTULO III
Operación

…

Sección XI
Contingencias

…

46a. Contingencias de los Participantes. - …

…

El Participante que, de conformidad con la **90a.** de las presentes Reglas, al cierre del Periodo de Cálculo anterior a aquel en que se encuentre, haya observado un porcentaje de participación relativa, determinado conforme a dicha Regla, mayor al tres por ciento, ~~o bien, sea una institución para el depósito de valores,~~ con el fin de que pueda enfrentar un evento que afecte el procesamiento de Órdenes de Transferencia, deberá ejecutar procedimientos de contingencia conforme a las especificaciones previstas en el Apéndice AI del Manual, a partir de los trescientos

sesenta y cinco días naturales contados a partir del día inmediato posterior a aquel en el que se ubique en el supuesto señalado en el presente párrafo. De igual manera, el Participante que tenga el carácter de institución para el depósito de valores, deberá ejecutar los procedimientos de contingencia antes mencionados, a partir de los trescientos sesenta y cinco días naturales contados a partir del día inmediato posterior a aquél en el que haya sido admitido como Participante.

Adicionalmente, losel Participantes al que se refiere el párrafo precedente deberán entregar al Administrador, dentro de los ciento ochenta días naturales siguientes al vencimiento del plazo de trescientos sesenta y cinco días naturales señalado en ese mismo párrafo, un informe con las características previstas en la **74a.** de las presentes Reglas, que acredite el cumplimiento de los requisitos de seguridad informática, gestión del riesgo operacional y certificación establecidos en las fracciones I, II y III de la **58a**. de las presentes Reglas, aplicables a la infraestructura utilizada por el Participante de que se trate, para ejecutar los procedimientos de contingencia que se establezcan de conformidad con el párrafo anterior.

Quedarán exceptuados de lo establecido en los dos párrafos inmediatos anteriores el Banco de México, actuando en nombre y por cuenta propia o en su carácter de fiduciario en cualquier fideicomiso, y el operador de un sistema internacional de liquidación de operaciones cambiarias que incluyan a la moneda nacional entre las monedas participantes.

…

CAPÍTULO VI
Proceso de admisión para actuar como Participante

Sección I
Requisitos de admisión

…

58a. Requisitos para la admisión como Participante.- El interesado en actuar como Participante que presente una solicitud de admisión de conformidad con la **57a.** de las presentes Reglas deberá acreditar, a satisfacción del Administrador, que cumple con los requisitos que se indican a continuación, en términos de las especificaciones incluidas en el Apéndice M del Manual.

I. Requisitos de seguridad informática:

A. En la Infraestructura Tecnológica.

El interesado deberá contarcuente con una políticas y procedimientos documentados e implementados que se obligue a seguir en materia de seguridad informática que, al menos, incluyan lo siguiente:

a) Contar con Tener en su estructura organizacional un área designada, como responsable de que la seguridad informática que verifique que la administración de en la Infraestructura Tecnológica se lleva a cabo conforme a las políticas y procedimientos de seguridad informática

~~establecidos~~lleve a cabo de conformidad con las Normas Internas del SPEI, así como que dicha área realice el seguimiento al cumplimiento de las citadas Normas Internas.

a Bis) ~~Las medidas y acciones que deberá adoptar, conforme a lo establecido en el Manual, para la atención e incidentes de seguridad de la información en su Infraestructura Tecnológica o en la infraestructura tecnológica de cualquier tercero que pudiera tener una afectación en la operación o en la Infraestructura Tecnológica del interesado.~~Se deroga.

b) ~~Contar con una política escrita que deberá procurar y mantener~~Establecer y mantener controles de~~la~~ ~~solidez~~seguridad informática, así como de ciberresiliencia en~~de~~ la Infraestructura Tecnológica ~~,~~que, ~~queden referidos~~al menos, incorporen~~,~~ ~~a~~ lo~~s~~ siguiente~~s aspectos~~:

1. ~~Procedimientos para evaluar los~~Utilizar en la Infraestructura de Cómputo protocolos seguros de comunicación utilizados en la Infraestructura Tecnológica y prescindir de aquellos que se consideren inseguros, conforme a lo especificado en el Apéndice M del Manual;

2. ~~Procedimientos que contemplen el uso obligatorio de~~Utilizar herramientas ~~que permitan detectar~~tecnológicas y contar con procedimientos para llevar a cabo la detección de virus informáticos y códigos maliciosos en la Infraestructura de Cómputo, así como mantener actualizadas dichas herramientas y procedimientos.~~Tecnológica, así como procedimientos que permitan su actualización periódica~~ Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

2 bis. Utilizar herramientas para el monitoreo de la integridad de la información en la Infraestructura de Cómputo, conforme a lo especificado en el Apéndice M del Manual;

3. ~~Procedimientos que permitan administrar las~~ Utilizar herramientas tecnológicas y contar con procedimientos para la detección y gestión de vulnerabilidades ~~de seguridad informática derivadas de, entre otros factores, cambios, actualizaciones o errores~~informáticas en la Infraestructura ~~Tecnológica;~~de Cómputo. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

4. ~~Procedimientos para inhibir~~Inhibir tanto la activación de cualquier servicio, así como la instalación de ~~cualquier servicio, aplicación~~aplicaciones ~~y/~~o software en la Infraestructura de Cómputo, que no ~~sea indispensable~~sean indispensables para la

operación con el SPEI. Lo anterior, conforme a lo especificado en el Apéndice M del Manual ~~en la Infraestructura Tecnológica~~;

4 bis. Impedir la ejecución de archivos no autorizados en la Infraestructura de Cómputo a través de herramientas tecnológicas. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

5. ~~Procedimientos para detectar~~Detectar y gestionar incidentes de seguridad informática en la Infraestructura Tecnológica~~, que aseguren su identificación, contención y la adecuada recolección y resguardo de evidencia de seguridad informática para su notificación a la alta dirección, y~~ del SPEI, así como en otras infraestructuras que pudieran afectar a la seguridad informática de las operaciones que se van a gestionar a través del SPEI. Lo anterior, de conformidad con lo especificado en el Apéndice M del Manual;

5 bis. Utilizar herramientas tecnológicas que lleven a cabo el registro centralizado de bitácoras de los diferentes componentes de la Infraestructura Tecnológica, así como que identifiquen patrones anómalos y detecten incidentes de seguridad informática. Lo anterior, de conformidad con lo especificado en el Apéndice M del Manual, y

6. ~~Procedimientos para evaluar y/o auditar, al menos cada dos años, la seguridad informática de la Infraestructura Tecnológica, que incluyan la realización de pruebas de penetración por un auditor externo independiente especializado en dicho tipo de pruebas. Además, entre los trabajos de dicha evaluación o auditoría, se deberá prever la presentación de un reporte que establezca un nivel de riesgo informático para la Infraestructura Tecnológica, así como la conformación de un plan de trabajo documentado para atender los riesgos de criticidad alta y media referidos en dicha evaluación o auditoría~~Realizar pruebas de penetración a la Infraestructura Tecnológica, así como elaborar los planes de trabajo y reportes que deriven de los resultados de dichas pruebas. Lo anterior, de conformidad con lo especificado en el Apéndice M del Manual.

c) Política para la implementación del Aplicativo SPEI, ya sea por parte del Participante o por medio de una empresa externa especializada en el desarrollo de programas de cómputo (software) contratada por aquel, que contengan los procedimientos siguientes:

1. Procedimientos que aseguren que se sigue un proceso de desarrollo formal y documentado para la implementación de su

Aplicativo SPEI. El proceso de desarrollo deberá considerar, al menos, las siguientes etapas:

i. Diseño del Aplicativo SPEI.

ii. Desarrollo del Aplicativo SPEI conforme al diseño anterior.

iii. Validación de funcionalidades, propósito, capacidad y calidad del Aplicativo SPEI.

iv. Implantación del Aplicativo SPEI.

v. Seguimiento formal a cambios en el Aplicativo SPEI.

2. Procedimientos que aseguren que la seguridad informática sea considerada durante las diferentes etapas de su proceso de desarrollo;

3. Procedimientos que aseguren que los componentes o mecanismos que brindan seguridad a su Aplicativo SPEI se encuentren vigentes y que se revise su vigencia conforme a lo especificado en el Apéndice M del Manual;

4. Procedimientos que aseguren que la seguridad del Aplicativo SPEI sea revisada de forma estática y dinámica;

5. Procedimientos que permitan vigilar, auditar y rastrear los accesos y actividades realizadas por los diferentes usuarios del Aplicativo SPEI con independencia del nivel de privilegios que se establezca para su acceso y el medio o protocolo de comunicación de acceso. Estos procedimientos deberán considerar el resguardo de la información recabada por un periodo de al menos seis meses, y

6. Procedimientos que permitan vigilar, auditar y rastrear todas las operaciones realizadas en el Aplicativo SPEI. Estos procedimientos deberán considerar el resguardo de la información recabada por un periodo de al menos seis meses.

d) ~~Contar con~~políticas ~~que se obligue a seguir para un~~ Establecer y mantener controles de acuerdo con sus políticas y procedimientos para el manejo seguro de la información electrónica, a las que refiere el Apéndice M del Manual y~~,~~ en los que ~~contengan~~quede referido, al menos, lo~~s~~ ~~procedimientos~~ siguiente~~s~~:

1. ~~Procedimientos que aseguren que al desechar o dar~~ Utilizar herramientas tecnológicas para borrar la información de ~~baja componentes o~~forma segura en ~~dispositivos físicos (hardware) de~~

la Infraestructura ~~Tecnológica la información contenida en estos sea irrecuperable~~de Cómputo y en la Infraestructura de Telecomunicaciones. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

2. ~~Procedimientos para restringir~~Inhibir, a través de mecanismos lógicos, el acceso a los puertos físicos de conexión ~~y~~, así como el uso de dispositivos de almacenamiento extraíbles y periféricos de la Infraestructura ~~Tecnológica~~de Cómputo. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

3. ~~Procedimientos~~ Generar y resguardar bitácoras ~~para el resguardo~~de los eventos de auditoría~~información~~ referentes a la actividad de las cuentas del sistema operativo de la Infraestructura ~~Tecnológica y operativa~~de Cómputo, de acuerdo con sus procedimientos. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

4. Procedimientos que permitan detectar la alteración o falsificación de la información contenida en el Aplicativo SPEI;

5. Procedimientos que permitan cifrar la información sensible en el Aplicativo SPEI, y

6. ~~Procedimientos que permitan contar con un inventario de la Infraestructura Tecnológica con la que se cuente conforme a lo especificado en el Apéndice M del Manual.~~Se deroga.

e) ~~Contar con políticas que se obligue a seguir para implementar mecanismos de control~~Implementar controles de acceso a la Infraestructura Tecnológica, ~~con base en criterios que establezcan para determinar que dichos mecanismos~~ que sean robustos y seguros, de acuerdo con sus políticas y procedimientos, ~~que incluyan~~en los ~~procedimientos~~que quede referido, al menos, lo siguiente~~s~~:

1. ~~Procedimientos que permitan implementar mecanismos y controles robustos de~~Controlar el acceso lógico a la Infraestructura ~~Tecnológica~~de Cómputo de acuerdo con sus procedimientos. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

2. ~~Procedimientos para una gestión~~Gestionar el acceso a las cuentas de usuarios de la Infraestructura de Cómputo y sus contraseñas, de acuerdo con sus procedimientos. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

3. ~~Procedimientos que permitan realizar bloqueo~~Bloquear de manera manual y ~~automático de~~ automática la Infraestructura ~~Tecnológica~~

~~para asegurar que los equipos solo puedan ser utilizados por personal autorizado~~de Cómputo al registrar inactividad. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

4. Procedimientos para la gestión de privilegios de acceso al Aplicativo SPEI, y

5. Procedimientos que permitan vigilar y auditar los accesos y actividades realizadas por los usuarios del Aplicativo SPEI. Estos procedimientos deberán considerar el resguardo de la información recabada por un periodo de, al menos, seis meses, así como la atención y seguimiento a los posibles eventos de fraude relacionados con transferencias.

f) Documentar e implementar ~~Contar con políticas que deberá seguir~~ los controles de la Infraestructura de Cómputo y de la Infraestructura de Telecomunicaciones siguientes, en términos de las especificaciones establecidas en el Apéndice M del Manual:

1. ~~Procedimientos para restringir~~Inhibir a través de mecanismos lógicos el acceso a internet desde la Infraestructura ~~Tecnológica, y~~de Cómputo de acuerdo con sus procedimientos. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

2. Procedimientos para la gestión de una red de telecomunicaciones que permita la comunicación con el Banco de México de una manera eficiente y segura~~.~~;

3. Segmentar física o lógicamente, la red de la Infraestructura de Telecomunicaciones en distintos dominios y subredes;

4. Contar con la documentación que muestre los componentes que conforman la Infraestructura de Cómputo y la Infraestructura de Telecomunicaciones, así como la interconexión entre ellos, como son diagramas de red, esquemas o mapas. Lo anterior, conforme a la información con la que cada componente de la Infraestructura de Telecomunicaciones cuenta para determinar el flujo de los paquetes de datos;

5. Implementar y almacenar las bitácoras de los eventos generados por la Infraestructura de Telecomunicaciones. Dichas bitácoras deberán contener la estampa de tiempo del reloj de los componentes de la Infraestructura de Telecomunicaciones, el cual debe estar sincronizado contra una referencia de tiempo externa;

6. Generar las políticas de filtrado de datos en la Infraestructura de Telecomunicaciones para controlar y especificar los flujos de

información e implementar las listas de control de acceso de conformidad con dichas políticas de filtrado de datos.

En caso de requerirse la implementación de protocolos de reasignación de direccionamiento IP en uno o varios componentes de la Infraestructura de Telecomunicaciones, éstos deberán configurarse en un formato de uno a uno;

7. Generar y almacenar los respaldos de la configuración de la Infraestructura de Telecomunicaciones mediante una o más herramientas;

8. Administrar la Infraestructura de Telecomunicaciones mediante protocolos y mecanismos que permitan controlar, autenticar, autorizar y registrar las actividades de los administradores;

9. Asegurar la información que se transmite por los enlaces de interconexión de la Infraestructura de Telecomunicaciones mediante protocolos y algoritmos de cifrado de datos, y

10. Monitorizar la Infraestructura de Telecomunicaciones mediante herramientas y protocolos específicos para dicha función.

g) Contar con controles y políticas que se obliguen a seguir respecto de la Infraestructura Tecnológica, que deberán establecer:

1. Procedimientos que permitan contar con un inventario de la Infraestructura Tecnológica con la que se cuente conforme a lo especificado en el Apéndice M del Manual;

2. Proceso de gestión de entrada y salida de equipos de cómputo y telecomunicaciones al Centro de Datos;

3. Proceso de gestión y protección del acceso físico a los componentes de cómputo y telecomunicaciones;

4. Sistemas electromecánicos para la continuidad operativa y de protección contra incendios en la instalación donde reside la Infraestructura de Cómputo;

5. Proceso de mantenimiento a los componentes de cómputo;

6. Proceso de gestión del acceso físico a los medios extraíbles de almacenamiento de información, y

7. Proceso de gestión del acceso remoto.

B. En los Canales Electrónicos.

Los interesados que ofrezcan a sus Clientes Emisores Canales Electrónicos deberán contar con procesos y/o sistemas debidamente documentados que consideren al menos:

a) Contar con una estructura organizacional que permita la separación de actividades y roles, diferenciando entre las áreas responsables del desarrollo y operación de los Canales Electrónicos.

b) Procedimientos que permitan administrar las vulnerabilidades de seguridad informática derivadas de, entre otros factores, cambios, actualizaciones o errores en los Canales Electrónicos.

c) Contar con un proceso de desarrollo de software formal y documentado que contemple al menos el seguimiento y control de versiones del software de los Canales Electrónicos.

d) Procedimientos que permitan el resguardo de bitácoras detalladas sobre la operación de los Clientes Emisores en los Canales Electrónicos, incluyendo las incidencias. Las bitácoras deben ser resguardadas por un periodo de al menos un año.

e) Procedimientos que establezcan controles para el acceso a las bitácoras.

f) Procedimientos que contemplen el uso obligatorio de herramientas que permitan detectar virus informáticos y códigos maliciosos en los Canales Electrónicos, así como procedimientos que permitan su actualización periódica.

g) Las medidas y acciones que deberá adoptar, conforme a lo establecido en el Manual, para la atención de incidentes de seguridad de la información en sus Canales Electrónicos.

Además de lo anteriormente establecido en esta fracción, el interesado en actuar como Participante deberá contar con una política y procedimientos documentados que se obligue a seguir en materia de pruebas de confianza e integridad que deba aplicar a aquellos miembros de su personal, así como de los terceros que provean servicios en materia de tecnologías de la información y comunicación, que tengan acceso a información y sistemas relevantes en la operación con el SPEI. Lo dispuesto en la presente Regla no será aplicable al caso en que el Participante sea el Banco de México, en su carácter de fiduciario de cualquier fideicomiso sin estructura orgánica o un operador de un sistema internacional de liquidación de operaciones cambiarias que incluyan al peso como una de las divisas participantes.

II. Requisitos de gestión del riesgo operacional

a) El interesado cuente con políticas y procedimientos documentados que se obligue a seguir para la administración de riesgos operacionales, que incluyan lo siguiente:

1. Una metodología para la administración del riesgo operacional relacionada con la operación con el SPEI que considere la identificación, evaluación, monitoreo y mitigación de los riesgos identificados, así como los roles y responsabilidades definidos para su ejecución, revisión y actualización;

2. Una metodología para el análisis de impactos al negocio, que considere al menos:

   i. Identificar los procesos críticos relacionados con su operación con el SPEI;

   ii. Identificar y clasificar los impactos en el tiempo en el que se encuentra disponible el sistema al materializarse los riesgos operacionales identificados, conforme a la metodología de gestión del riesgo operacional definida;

   iii. Definir un tiempo objetivo de recuperación para cada proceso crítico relacionado con su operación con el SPEI, el cual deberá ser menor o igual a dos horas;

   iv. Definir un punto objetivo de recuperación ante la interrupción de su operación con el SPEI, que considere procedimientos de conciliación para recuperar la operación en un estado consistente de la información hasta antes de la interrupción;

   v. Identificar a las contrapartes críticas internas y externas relacionadas con su operación con el SPEI, y

   vi. Identificar los recursos materiales y humanos críticos para realizar la operación con el SPEI;

3. 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

4. Manuales de procedimientos y de operación que describan las actividades requeridas para realizar su operación con el SPEI y el personal responsable de la ejecución de dichas actividades de forma que se asegure que exista una segregación de funciones en los procesos críticos que se realicen para la operación del SPEI y una definición precisa de responsabilidades.

b) El interesado establezca al menos las siguientes medidas de mitigación de los riesgos:

1. Contar con un listado de los riesgos operacionales identificados, que indique la clasificación del riesgo y el resultado de su evaluación, así como los controles asociados para la operación con el SPEI, incluyendo los tecnológicos y aquellos asociados a proveedores externos;

2. Contar con un análisis de capacidad sobre los recursos tecnológicos, humanos y materiales dispuestos para la operación con el SPEI para asegurar que cuente con los recursos suficientes para manejar volúmenes altos de operación y cumplir con sus objetivos de nivel de servicio, y

3. Contar con políticas y lineamientos para la gestión de privilegios de acceso físico a los sitios operativos desde donde se realiza la operación con el SPEI y a los ~~c~~Centros de ~~d~~Datos que alojan a la Infraestructura Tecnológica dispuesta para operar con el SPEI.

c) El interesado establezca procedimientos documentados que deberá seguir para la recuperación y restauración de la operación con el SPEI ante la materialización de alguno de los riesgos a que se refiere esta fracción, que incluyan:

1. Una política de continuidad, así como las estrategias y procedimientos que el interesado deberá seguir como Participante para que, ante la materialización de los escenarios de contingencia identificados en el análisis de riesgos, pueda continuar con la operación con el SPEI en un nivel mínimo aceptable;

2. Las acciones que deberá seguir para la atención de incidentes que causen una afectación en la operación normal con el SPEI que contemple las fases de identificación, diagnóstico, atención, recuperación, restauración y documentación e indique los roles y responsabilidades correspondientes;

3. Las actividades que deberá realizar para dar respuesta a emergencias ante la ocurrencia de algún incidente que afecte la operación normal con el SPEI en el que se considere la activación de las estrategias y procedimientos de continuidad implementados y se indiquen los roles y responsabilidades, los niveles y tiempo de escalamiento, el protocolo y los medios de comunicación interna y externa disponibles;

4. Las acciones que deberá seguir para el restablecimiento de la operación normal, una vez que se active alguna estrategia o se ejecute algún procedimiento de continuidad derivado de la ocurrencia de un incidente relacionado con la operación con el SPEI, y

5. Un plan de pruebas al que deberá dar seguimiento para evaluar las estrategias y procedimientos de continuidad implementados relacionados

con la operación con el SPEI indicando los lineamientos, tipo de pruebas a realizar y periodicidad de las mismas.

III. Requisitos de certificación de los Aplicativos SPEI.

El interesado lleve a cabo, de conformidad con las especificaciones incluidas en el Apéndice O del Manual, lo siguiente:

a) Acreditar que, en caso de que se utilice un Aplicativo SPEI único para interactuar con las Instancias del SPEI, este cumpla con el protocolo de comunicación de cada una de las Instancias del SPEI respectivas, de conformidad con las especificaciones indicadas en la sección 7 del Manual y, en caso de que se utilice más de un Aplicativo SPEI para interactuar con las distintas Instancias del SPEI, acreditar que cada uno de dichos Aplicativos SPEI cumple con el protocolo de comunicación de la Instancia del SPEI para la cual se utilizará, de conformidad con las especificaciones indicadas en la citada sección 7 del Manual;

b) Acreditar que cada uno de los Aplicativos SPEI a utilizarse procesan adecuadamente los tipos de Órdenes de Transferencia que deban procesar de conformidad con estas Reglas, incluso cuando se presente un alto volumen de ellas en un periodo corto;

c) Acreditar que cuenta con la capacidad para cumplir con la Regla **20a.** para la generación y envío de la Confirmación de Abono;

d) Validar que pueda operar con la infraestructura secundaria que el Administrador haya instrumentado para el SPEI en casos de contingencia, y

e) Acreditar que podrá continuar con su operación ante la activación del "Procedimiento de Operación Alterno SPEI" (POA-SPEI), así como operar mediante el procedimiento de contingencia denominado "Cliente de Operación Alterno SPEI" (COA-SPEI). Se exceptúan del requisito establecido en este inciso los Participantes a que se refiere la **56a.** fracción IV, de las presentes Reglas.

IV. Requisitos de protección a los Clientes Emisores de los interesados.

A. El interesado cuente con sistemas y medidas de control que aseguren, al menos, lo siguiente:

a) Que el procesamiento de las Órdenes de Transferencia de los Clientes Emisores será completamente automatizado y que no contemplen procesos manuales entre las presentaciones de las Solicitudes de Envío del Cliente Emisor en los Canales Electrónicos y su envío al SPEI.

b) Que el interesado podrá ofrecer la posibilidad de realizar Órdenes de Transferencia a nombre y por cuenta de sus Clientes Emisores en un

esquema no automatizado exclusivamente en situaciones de contingencia, siempre y cuando cumpla con las siguientes condiciones:

1. Contar con mecanismos para certificar y validar la identidad del Cliente Emisor;

2. Poner a disposición de sus Clientes Emisores la información sobre los medios y procesos de comunicación en caso de contingencia, y

3. Contar con un esquema para la instrucción de Órdenes de Transferencia que consideren la autorización de al menos dos funcionarios que ocupen un cargo de cuando menos dos jerarquías inmediatas inferiores al director general del interesado.

B. Tratándose de aquellos interesados distintos a Instituciones de Crédito, que ofrezcan a sus Clientes Emisores Canales Electrónicos, deberán cumplir con los siguientes requerimientos:

a) Establecer, de manera clara y precisa, en el contrato para la celebración de operaciones a través de Canales Electrónicos que suscriban con los Clientes Emisores de manera clara y precisa, al menos, lo siguiente:

1. las operaciones y servicios que podrá realizar el Cliente Emisor a través de los Canales Electrónicos;

2. los mecanismos y procedimientos de identificación de los Clientes Emisores, así como los elementos de verificación de identidad;

3. los mecanismos, medios y procedimientos para la notificación a los Clientes Emisores de las operaciones realizadas en Canales Electrónicos;

4. los límites de los montos individuales y agregados diarios correspondientes a las operaciones que los Clientes Emisores puedan realizar a través de Canales Electrónicos, en caso de que existan;

5. los mecanismos para reportar el extravío o robo de algún elemento de verificación de identidad utilizado por el Cliente Emisor para autenticarse con el fin de que el interesado impida el acceso a Canales Electrónicos, así como para reportar operaciones no reconocidas;

6. los mecanismos y procedimientos de cancelación de la contratación de los Canales Electrónicos, y

7. las responsabilidades del interesado respecto los servicios que ofrezcan a través de Canales Electrónicos.

b) Contar con mecanismos y controles que aseguren el resguardo seguro y robusto de los elementos de verificación de identidad e identificadores de Clientes Emisores;

c) Generar una huella digital que compruebe la autenticidad de cada Solicitud de Envío de sus Clientes Emisores, de acuerdo al Apéndice Y del Manual;

d) Además de lo previsto en la fracción I, literal B, inciso d), de la presente Regla, contar con bitácoras detalladas de toda la actividad relacionada con Órdenes de Transferencia y Solicitudes de Envío instruidas por su Cliente Emisor a través de los Canales Electrónicos del interesado. Los interesados deberán almacenar al menos la siguiente información:

1. Canal Electrónico utilizado;

2. Fecha y hora de acceso y finalización de la sesión en el Canal Electrónico;

3. Elementos de verificación de identidad utilizados por los Clientes;

4. Fecha y hora de presentación de las Solicitudes de Envío;

5. Para el caso de Órdenes de Transferencia Aceptadas por SPEI, la información referida en la **83a.** de estas Reglas;

6. La generada conforme al inciso c) del presente literal;

e) Contar con procedimientos para revisar, al menos cada año, las bitácoras mencionadas en el inciso d) anterior y para que en caso que se detecte algún evento inusual se notifique al comité de auditoría interna, en caso que cuente con dicho comité, o si el interesado no cuenta con un comité de auditoría, la notificación se deberá presentar al director general o equivalente;

f) Contar con procedimientos que permitan a sus Clientes Emisores realizar a través de los Canales Electrónicos, con excepción de cajeros automáticos, los actos siguientes:

1. Establecer límites a los montos de las Órdenes de Transferencia para el monto agregado en un día, el monto de cualquier Orden de Transferencia y el monto transferido en un día a una Cuenta del Cliente correspondiente al Cliente Beneficiario;

2. Pre registrar Cuentas de Clientes Beneficiarios, siempre y cuando la regulación aplicable al interesado lo permita, y

3. Establecer el monto máximo para el pre-registro de Cuentas de Clientes Beneficiarios.

g) Contar con procedimientos que permitan entregar a sus Clientes Emisores, a través de los medios que establezcan para tal efecto, notificaciones sin costo para los Clientes Emisores y en un lapso no mayor a ~~10~~diez segundos a partir de la ocurrencia de los siguientes eventos:

1. Operaciones enviadas y recibidas;

2. Cambio de elementos de verificación de identidad, y

3. Cambio en el canal de recepción de notificaciones (al nuevo y al que se esté reemplazando).

h) Procesos que permitan monitorear los patrones de comportamiento transaccional de Clientes Emisores y contar con procedimientos documentados de las acciones que realizará el interesado ante indicativos de fraude;

i) Contar con mecanismos y procedimientos para que los Clientes Emisores puedan:

1. Reportar el extravío o robo de algún elemento de verificación de identidad para que el interesado impida el acceso a Canales Electrónicos, y

2. Reportar y dar seguimiento a operaciones no reconocidas por los Clientes Emisores realizadas a través de Canales Electrónicos.

j) Contar con procesos y mecanismos automáticos para bloquear el acceso a los Canales Electrónicos cuando se trate de acceder a los Canales Electrónicos con información incorrecta en a lo más cinco ocasiones consecutivas, y

k) Contar con procedimientos y mecanismos que permitan al interesado dar por terminada la sesión en Canales Electrónicos cuando exista inactividad por máximo veinte minutos o cuando en el curso de una sesión el interesado identifique cambios relevantes en los parámetros de comunicación del Canal Electrónico, tales como identificación del dispositivo de acceso, rango de direcciones de los protocolos de comunicación, o ubicación geográfica.

C. Los interesados deberán haber celebrado el Convenio de Colaboración para la Protección del Cliente Emisor autorizado por el Administrador, de conformidad con lo previsto en la **43a.** de estas Reglas, sujeto a la condición de que obtengan la autorización para ser admitido como Participante conforme a las presentes Reglas.

V. Requisitos en materia de Riesgos Adicionales para la admisión como Participante.

Los interesados que estén sujetos a regulación y supervisión en materia de prevención y detección de actos, omisiones u operaciones que pudieran favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión de cualquiera de los delitos previstos en los artículos 139 y 148 Bis del Código Penal Federal o que pudieran ubicarse en los supuestos del artículo 400 Bis del mismo Código deberán satisfacer los siguientes requisitos:

a) No deberán haber sido sujetos a la imposición de una sanción firme por infracciones a dicha regulación al menos en los últimos tres años previos a la fecha en que soliciten su admisión como participantes al SPEI.

b) En caso de haber sido sancionados conforme al inciso a) anterior, deberán acreditar ante el Administrador que han realizado las acciones necesarias para corregir las causas que hubieran dado origen a las infracciones respectivas. Dicha acreditación podría solventarse mediante el resultado de la visita de seguimiento que la comisión supervisora competente hubiere realizado para verificar tal situación, o bien, mediante la presentación de un informe elaborado por un Auditor Externo Independiente.

c) En el evento de que la entidad de que se trate haya sido notificada por la respectiva comisión supervisora sobre una posible o presunta infracción a la regulación referida en esta fracción V, dicha entidad deberá informar sobre esta situación al Administrador y presentar un informe de un Auditor Externo Independiente sobre las causas que hayan dado lugar a dicha notificación, así como sobre la viabilidad del plan de corrección que deba presentar para tales efectos, en el supuesto de que se lo hubiera requerido la comisión supervisora.

d) En caso de entidades que tengan el carácter de Institución de Crédito y que no hubieren sido sujetos a la supervisión e inspección por la autoridad competente en la materia a que se refiere la presente fracción durante los dos años inmediatos anteriores a la fecha de su solicitud, deberán acreditar, por medio de un informe elaborado por un Auditor Externo Independiente, que cuentan con la capacidad para dar cumplimiento a la regulación contemplada en esta misma fracción que les resulten aplicables.

Las entidades que no tengan el carácter de Institución de Crédito deberán obtener la acreditación prevista en el párrafo anterior con independencia de la supervisión a la que hayan sido objeto en la materia referida en esta fracción.

Además de lo anteriormente establecido en esta fracción, el interesado en actuar como Participante deberá contar con una política y procedimientos documentados que se obligue a seguir en la materia indicada en el segundo párrafo de la presente fracción, en la cual incluya, al menos, las actividades que realizará para identificar Cuentas de Clientes correspondientes a sujetos distintos a entidades financieras que ofrezcan de manera habitual y profesional, intercambios o compraventas de activos virtuales a que se refiere el artículo 17, fracción XVI, de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita.

VI. Requisitos de interoperabilidad.

Los interesados que tengan el carácter de Cámara de Compensación de Transferencias a Través de Dispositivos Móviles deberán ofrecer sus servicios a sus Clientes independientemente de las compañías de telecomunicaciones con que tengan contratados sus servicios estos Clientes.

…

TRANSITORIAS

PRIMERA.- Lo dispuesto en la presente Circular entrará en vigor a los veinte días hábiles contados a partir de su publicación en el Diario Oficial de la Federación, con excepción a lo señalado en las reglas transitorias siguientes.

SEGUNDA.- Las modificaciones al numeral 2 del inciso d), numeral 3 del inciso e) y a los numerales 1 y 2 del inciso f) del apartado A de la fracción I de la **58a.**, así como las adiciones de los numerales 4 y 6 al inciso f) del apartado A de la fracción I de la **58a.**, entrarán en vigor a los seis meses contados a partir de la fecha de entrada en vigor de la presente Circular.

TERCERA.- Las modificaciones a los numerales 1 y 4 del inciso b) y al numeral 1 del inciso e) del apartado A de la fracción I de la **58a.**, así como la adición del numeral 8 al inciso f) del apartado A de la fracción I de la **58a.**, entrarán en vigor a los doce meses contados a partir de la fecha de entrada en vigor de la presente Circular.

CUARTA.- Las modificaciones al numeral 5 del inciso b) y al numeral 1 del inciso d) del apartado A de la fracción I de la **58a.**, así como la adición del numeral 3 al inciso f) del apartado A de la fracción I de la **58a.**, entrarán en vigor a los dieciocho meses contados a partir de la fecha de entrada en vigor de la presente Circular.

QUINTA.- Las modificaciones al inciso a), a los numerales 2, 3 y 6 del inciso b), numeral 3 del inciso d) y numeral 2 del inciso e) del apartado A de la fracción I de la **58a.**, así como las adiciones de los numerales 2 bis, 4 bis y 5 bis al inciso b) y del inciso g) al apartado A de la fracción I de la **58a.**,

entrarán en vigor a los veinticuatro meses contados a partir de la fecha de entrada en vigor de la presente Circular.

SEXTA.- Las instituciones para el depósito de valores que a la entrada en vigor de la presente Circular hayan sido admitidas como Participantes, deberán ejecutar los procedimientos de contingencia a que refiere el octavo párrafo de la **46a.** de las Reglas del Sistema de Pagos Electrónicos Interbancarios (SPEI), emitidas mediante la Circular 14/2017 del Banco de México, a partir de los trescientos sesenta y cinco días naturales contados a partir del día inmediato posterior a la publicación de la presente Circular en el Diario Oficial de la Federación. Asimismo, deberán entregar al Administrador un informe, con las características previstas en la **74a.** de las presentes Reglas, mediante el cual se verifique el cumplimiento de los requisitos de seguridad informática, gestión del riesgo operacional y certificación establecidos en las fracciones I, II y III de la **58a.** de las presentes Reglas, de únicamente la infraestructura que hayan implementado para ejecutar los procedimientos de contingencia a que refiere el presente párrafo, a más tardar a los quinientos cuarenta y cinco días naturales contados a partir del día inmediato posterior a la publicación de la presente Circular en el Diario Oficial de la Federación.