BANCO DE MEXICO

CIRCULAR 12/2023 dirigida a los participantes del Sistema de Pagos Electrónicos Interbancarios y demás interesados en actuar con tal carácter, relativa a las 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).

Al margen un logotipo, que dice: Banco de México.- "2023, Año de Francisco Villa, el revolucionario del pueblo".

CIRCULAR 12/2023

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, ha resuelto modificar los marcos de ciberseguridad aplicables a las Reglas del Sistema de Pagos Electrónicos Interbancarios (SPEI), con el propósito de dotar de mayor claridad respecto al elemento de infraestructura tecnológica sobre el cual se debe observar el cumplimiento de los referidos marcos y precisar los elementos obligacionales que los participantes en el 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 y de ciberresiliencia de los participantes del SPEI.

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, 4, párrafo primero, 8, párrafos cuarto y octavo, 10, párrafo primero, 15 Bis 1, párrafo primero, en relación con el 28 Bis 1, fracción IX, 17, fracción I, 20 Quáter, fracción IV y 29 Bis, fracción VIII, del Reglamento Interior del Banco de México, que le otorgan la atribución de expedir disposiciones a través de la Dirección General de Tecnologías de la Información, la Dirección de Disposiciones de Banca Central, la Dirección de Política y Estudios de Sistemas de Pagos e Infraestructuras de Mercados y la Dirección de Ciberseguridad, respectivamente, así como Segundo, fracciones II, IX, X y XVII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, ha resuelto **modificar** la definición "Infraestructura Tecnológica", contenida en la **2a.**, la **46a.**, párrafos octavo y noveno, la **58a.**, fracción I, apartado A, párrafo primero, así como los incisos a), b) y sus numerales 1, 2, 3, 4, 5 y 6, d) y sus numerales 1, 2 y 3, e) y sus numerales 1, 2, 3, f) y su numeral 1, fracción II, inciso b), numeral 3, así como la fracción IV, apartado B, inciso g); **adicionar** las definiciones "Centro de Datos", "Ciberresiliencia", "Infraestructura de Cómputo" e "Infraestructura de Telecomunicaciones" a la **2a.**, los numerales 2 bis, 4 bis y 5 bis al inciso b), los numerales 3, 4, 5, 6, 7, 8, 9 y 10 al inciso f), el inciso g), y los párrafos segundo y tercero, del apartado A de la fracción I de la **58a.**, así como **derogar** el inciso a Bis) y el numeral 6 del inciso d) del apartado A de la fracción I de la **58a.**, de las "Reglas del Sistema de Pagos Electrónicos Interbancarios", emitidas mediante la Circular 14/2017, para quedar en los términos siguientes:

REGLAS DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS

"**2a. Definiciones.-** …

…

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

…

VII Bis. Ciberresiliencia:	a 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. Lo anterior, a través de la implementación de herramientas tecnológicas, controles, estructuras, estrategias, políticas, procesos y prácticas.

…

XXVII Quáter. Infraestructura de Cómputo:	a 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 Infraestructura de Cómputo, Infraestructura de Telecomunicaciones y aplicaciones que utilizan los Participantes para interconectarse y operar con el SPEI.

…"

"**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 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, los Participantes a 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.

…"

"**58a. Requisitos para la admisión como Participante.-** …

I. Requisitos de seguridad informática:

A. En la Infraestructura Tecnológica.

El interesado deberá contar con políticas y procedimientos documentados e implementados que, al menos, incluyan lo siguiente:

a) Tener en su estructura organizacional un área designada como responsable de que la seguridad informática en la Infraestructura Tecnológica se 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) Se deroga.

b) Establecer y mantener controles de seguridad informática, así como de Ciberresiliencia en la Infraestructura Tecnológica que, al menos, incorporen lo siguiente:

1. 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. Utilizar herramientas 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. 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. Utilizar herramientas tecnológicas y contar con procedimientos para la detección y gestión de vulnerabilidades informáticas en la Infraestructura de Cómputo. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

4. Inhibir tanto la activación de cualquier servicio, así como la instalación de aplicaciones o software en la Infraestructura de Cómputo, que no sean indispensables para la operación con el SPEI. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

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. Detectar y gestionar incidentes de seguridad informática en la Infraestructura Tecnológica, así como en aquella otra infraestructura tecnológica utilizada por el Participante que pudiera derivar en una afectación a su operación en el 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. 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. La periodicidad de las pruebas de penetración, los reportes y planes de trabajo que se deben emitir con motivo de las mismas, así como las características que deben reunir las personas que ejecuten las mencionadas pruebas de penetración, serán aquellas especificadas en el Apéndice M del Manual.

c) **...**

d) 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 quede referido, al menos, lo siguiente:

1. Utilizar herramientas tecnológicas para borrar la información de forma segura en la Infraestructura de Cómputo y en la Infraestructura de Telecomunicaciones. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

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

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

4. y 5. **...**

6. Se deroga.

e) Implementar controles de acceso a la Infraestructura Tecnológica, que sean robustos y seguros, de acuerdo con sus políticas y procedimientos, en los que quede referido, al menos, lo siguiente:

1. Controlar el acceso lógico a la Infraestructura de Cómputo de acuerdo con sus procedimientos. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

2. 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. Bloquear de manera manual y automática la Infraestructura de Cómputo al registrar inactividad. Lo anterior, conforme a lo especificado en el Apéndice M del Manual;

4. y 5. **...**

f) Documentar e implementar 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. Inhibir a través de mecanismos lógicos el acceso a internet desde la Infraestructura 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;

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

   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) Implementar controles y políticas que se obliguen a seguir respecto de la Infraestructura Tecnológica, que deberán establecer, conforme a lo especificado en el Apéndice M del Manual, lo siguiente:

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. Sistemas electromecánicos y de protección contra incendios del Centro de Datos;

4. Proceso de mantenimiento de la Infraestructura de Cómputo;

5. Proceso de gestión del acceso físico a los medios usados para el respaldo de información, y

6. Proceso de gestión del acceso remoto.

El Administrador podrá autorizar el uso de mecanismos de control alternos a los referidos en los numerales 2, 2 bis, 3, 4 bis, y 5 bis, del inciso b), 1 y 2 del inciso d), así como 1 del inciso f), correspondientes a la fracción I, apartado A, de la presente Regla 58a., y cuyas características son establecidas en el Apéndice M del Manual.

Para efecto de lo señalado en el párrafo anterior, el Participante de que se trate deberá enviar previamente una comunicación, con las características previstas en el Anexo C del Apéndice M del Manual, a la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, en términos de la **98a.** de estas Reglas, que acredite que los mecanismos de control alternos que pretende implementar permiten producir condiciones de seguridad equivalentes o mayores a aquellas producidas por los elementos descritos en los numerales 2, 2 bis, 3, 4 bis y 5 bis del inciso b), 1 y 2 del inciso d), así como 1 del inciso f), correspondientes a la fracción I, apartado A, de la presente Regla **58a.**, y se encuentran alineados con las mejores prácticas

establecidas sobre la materia por parte de entidades de reconocido prestigio en dicha materia en el país u otras jurisdicciones, tales como el Instituto Nacional de Estándares y Tecnología de los Estados Unidos de América o de la Organización de Estándares Internacionales (NIST e ISO por sus siglas en inglés, respectivamente), así como aquellos que el propio Banco de México determine como equivalentes.

…

II. **…**

a) **…**

b) **…**

1. y 2. **…**

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 Centros de Datos que alojan a la Infraestructura Tecnológica dispuesta para operar con el SPEI.

c) **…**

III. **…**

IV. **…**

A. **…**

B. **…**

a) a f) **…**

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 diez segundos a partir de la ocurrencia de los siguientes eventos:

…"

TRANSITORIAS

PRIMERA.- Lo dispuesto en la presente Circular entrará en vigor el 19 de diciembre de 2023, con excepción a lo señalado en las reglas transitorias siguientes.

SEGUNDA.- Las modificaciones al inciso b) y sus numerales 1 y 4, al inciso d) y su numeral 2, al inciso e) y sus numerales 1 y 3, al inciso f) y su numeral 1, del apartado A de la fracción I de la **58a.**, así como las adiciones de los numerales 3, 4, 5, 6, 7, 8, 9 y 10 al inciso f) del apartado A de la fracción I de la **58a.**, entrarán en vigor el 19 de diciembre de 2024.

TERCERA.- Las modificaciones al inciso a), a los numerales 2, 3, 5 y 6 del inciso b), a los numerales 1 y 3 del inciso d) y al 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 el 19 de diciembre de 2025.

CUARTA.- 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, emitidas mediante la Circular 14/2017 del Banco de México, a partir del 20 de noviembre de 2024. 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 el 19 de mayo de 2025.

QUINTA.- Las derogaciones del inciso a) Bis y el numeral 6 del inciso d) del apartado A de la fracción I de la **58a.**, entrarán en vigor el 19 de diciembre de 2025.

Ciudad de México, a 9 de noviembre de 2023.- BANCO DE MÉXICO: Director General de Tecnologías de la Información, **Octavio Bergés Bastida**.- Rúbrica.- Directora de Disposiciones de Banca Central, **María Teresa Muñoz Arámburu**.- Rúbrica.- Director de Política y Estudios de Sistemas de Pagos e Infraestructuras de Mercados, **Othón Martino Moreno González**.- Rúbrica.- Director de Ciberseguridad, **Alejandro de los Santos Santos**.- Rúbrica.

Para cualquier consulta sobre el contenido de la presente Circular, el Banco de México se pone a su disposición a través de la Dirección de Autorizaciones y Sanciones de Banca Central al teléfono (55) 5237-2000 extensión 3200.