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 EN EL SISTEMA DE PAGOS INTERBANCARIOS EN DÓLARES:

ASUNTO: MODIFICACIONES A LA CIRCULAR 4/2016 (FORTALECIMIENTO DE LAS DISPOSICIONES EN MATERIA DE CIBERSEGURIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN DEL SISTEMA DE PAGOS INTERBANCARIOS EN DÓLARES)

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 Interbancarios en Dólares", emitidas mediante la Circular 4/2016, para quedar en los términos siguientes:

CIRCULAR 4/2016

REGLAS DEL SISTEMA DE PAGOS INTERBANCARIOS EN DÓLARES (SPID)

CAPÍTULO I
Disposiciones preliminares

…

2a. Definiciones.- Para efectos de estas Reglas, se entenderá por:

…

I Bis. Aplicativo SPID:	al programa de cómputo que usan los Participantes para interactuar con el SPID y que forma parte de la Infraestructura Tecnológica.

…

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

…

XIX Bis. 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 SPID.
XIX Ter. 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.
XX. Infraestructura Tecnológica:	A la ~~i~~Infraestructura de Cc~~o~~mputo, Infraestructura de ~~t~~Telecomunicaciones~~, software~~ y aplicaciones que utilizan los Participantes para interconectarse y operar con el SPID.

…

CAPÍTULO IV
Proceso de admisión para actuar como Participante

…

Sección I
Requisitos de admisión

…

42a. Requisitos para la admisión como Participante. - La Institución de Crédito que presente una solicitud de admisión en términos de la Regla anterior 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 E, Anexo C, del Manual.

I. Requisitos de seguridad informática:

En la Infraestructura Tecnológica, ~~l~~La Institución de Crédito ~~debe elaborar~~ deberá contar con~~y documentar una~~ política~~s~~ y procedimientos documentados que~~que se obligue a seguir en materia de seguridad informática que~~, al menos, incluya~~n~~ lo siguiente:

a) ~~Contar con~~ Tener en su estructura organizacional un área designada~~,~~ como responsable de que la seguridad informática en ~~que verifique que la administración de~~ la Infraestructura Tecnológica se lleve a cabo de conformidad con las Normas Internas del SPID~~;~~, así como que dicha área realice el seguimiento al cumplimiento de las citadas Normas Internas. ~~se lleva a cabo conforme a las políticas y procedimientos de seguridad informática establecidos;~~

b) ~~Contar con una política escrita que se obligue a seguir para procurar y mantener la solidez~~ Establecer y mantener controles de seguridad informática, así como de ciberresiliencia ~~de~~ en la Infraestructura Tecnológica, que ~~quede referida,~~ al menos incorporen~~, a~~ lo~~s~~ siguiente~~s aspectos~~:

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

2. ~~Procedimientos que contemplen el uso obligatorio de~~Utilizar herramientas tecnológicas y contar con procedimientos para llevar a cabo la detección de ~~que permitan detectar~~ 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 E, Anexo C, 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; Utilizar herramientas para el monitoreo de la integridad de la información en la Infraestructura de Cómputo, conforme a lo especificado en el Apéndice E, Anexo C, del Manual;

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

4. ~~Procedimientos para inhibir~~ Inhibir tanto la activación de cualquier servicio, así como la instalación de aplicaciones ~~de cualquier servicio, aplicación y/~~o software en la Infraestructura de Cómputo, que no sean indispensables para la operación con el SPID. Lo anterior, conforme a lo especificado en el Apéndice E, Anexo C, del Manual ~~SPID en la Infraestructura Tecnológica~~;

BORRADOR

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 E, Anexo C, del Manual;

5. (Derogado por Circular 11/2016).

6. ~~Procedimientos para detectar~~ Detectar y gestionar incidentes de seguridad informática ~~–~~en la Infraestructura Tecnológica del SPID, así como en otras infraestructuras que pudieran afectar a la seguridad informática de las operaciones que se van a gestionar a través del SPID. Lo anterior, de conformidad con lo especificado en el Apéndice E, Anexo C, del Manual;~~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~~

6 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 E, Anexo C del Manual, y

7. ~~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 el propio Participante o 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 22 riesgos de criticidad alta y media referidos en dicha evaluación o auditoriae~~ 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 E, Anexo C, del Manual;

b Bis) Contar con una política ~~que se obligue a seguir~~ para la implementación del ~~sus sistemas informáticos~~ Aplicativo SPID, 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 ~~sus sistemas informáticos~~su Aplicativo SPID. El proceso de desarrollo deberá considerar, al menos, las siguientes etapas:

   i. Diseño del ~~sistema informático~~ Aplicativo SPID.

ii. Desarrollo del ~~sistema informático~~ Aplicativo SPID conforme al diseño anterior.

iii. Validación de funcionalidades, propósito, capacidad y calidad del ~~sistema informático~~ Aplicativo SPID.

iv. ~~Liberación y/o instalación~~ Implantación del ~~sistema informático~~Aplicativo SPID.

v. Seguimiento formal a cambios en el ~~sistema informático~~Aplicativo SPID.

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 sus ~~sistemas informáticos~~ Aplicativo SPID se encuentren vigentes y que se revise su vigencia en los términos y plazos indicados en el Apéndice E, Anexo C, del Manual;

4. Procedimientos que aseguren que la seguridad del ~~sistema informático~~ Aplicativo SPID 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 ~~los servicios informáticos~~ Aplicativo SPID 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 ~~6~~ seis meses~~;~~, y

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

c) ~~Contar conpolíticas 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~~ de forma segura en ~~o dispositivos físicos (hardware) de~~ la Infraestructura de Cómputo y en la Infraestructura de Telecomunicaciones ~~Tecnológica la información contenida en estos sea borrada de manera segura~~. Lo anterior, conforme a lo especificado en el Apéndice E, Anexo C, del Manual;

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

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

4. Procedimientos que permitan detectar la alteración o falsificación de la información contenida en el Aplicativo SPID;~~la Infraestructura Tecnológica, y~~

5. Procedimientos que permitan cifrar la información sensible en ~~la Infraestructura Tecnológica~~el Aplicativo SPID~~.~~, y

d) ~~Contar con políticas que deberá seguir para implementar mecanismos robustos y seguros de control~~ Implementar controles de acceso a la Infraestructura Tecnológica, que sean robustos y seguros, de acuerdo con sus políticas y procedimientos, en los que queden referidos, al menos, ~~incluyan los procedimientos~~ 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 E, Anexo C, 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 E, Anexo C, del Manual;

3. ~~Procedimientos que permitan realizar bloqueo~~ Bloquear de manera manual y automática~~a~~ ~~de~~ la Infraestructura de Cómputo al registrar inactividad. Lo anterior, conforme a lo especificado en el Apéndice E, Anexo C, del Manual~~. Tecnológica para asegurar que los equipos solo puedan ser utilizados por personal autorizado, y Procedimientos para la gestión de privilegios de acceso a la Infraestructura Tecnológica~~;

4. Procedimientos para la gestión de privilegios de acceso a~~l la Infraestructura Tecnológica~~ Aplicativo SPID, y

5. Procedimientos que permitan vigilar y auditar los accesos y actividades realizadas por los usuarios del ~~la Infraestructura Tecnológica~~ Aplicativo SPID. Estos procedimientos deberán considerar el resguardo de la información recabada por un periodo de al menos ~~6~~ seis meses, así como la atención y seguimiento a los posibles eventos de fraude relacionados con transferencias;

e) ~~Contar con políticas que deberá~~ 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 E, Anexo C, del Manual~~seguir para la gestión de una red de telecomunicaciones que permita la comunicación segura y eficiente con el Banco de México, que incluyan los procedimientos siguientes~~:

1. ~~Procedimientos para restringir~~ 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 E, Anexo C, del Manual ~~Tecnológica, y~~;

2. Procedimientos para la gestión de una red de T~~t~~elecomunicaciones 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 lo 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

BORRADOR

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.

f) 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 E, Anexo C, 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.

II. Requisitos de gestión del riesgo operacional

a) La Institución de Crédito debe contar con políticas y procedimientos documentados que deberá seguir para la gestión de riesgos operacionales, que incluyan lo siguiente:

1. Una metodología de gestión del riesgo operacional relacionada con la operación con el SPID que considere la identificación y evaluación de riesgos, así como la

implementación de controles que permitan la mitigación de los riesgos identificados;

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 SPID;

   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 SPID, 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 SPID, 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 SPID, y

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

3. Procedimientos de contratación y capacitación que aseguren que el personal relacionado con la operación del SPID, cuente con las habilidades, competencias y conocimientos requeridos para el puesto que desempeña, y

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

b) La Institución de Crédito debe asegurar que se establezcan medidas de mitigación de los riesgos a que se refiere esta fracción, que consideren lo siguiente:

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

2. Contar con un análisis de capacidad sobre los recursos tecnológicos, humanos y materiales dispuestos para la operación con el SPID 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 a los sitios operativos desde donde se realiza la operación con el SPID y a los Ce~~c~~entros de D~~d~~atos que alojan a la Infraestructura Tecnológica dispuesta para operar en SPID, y

c) La Institución de Crédito deberá contar con procedimientos que deberá seguir para la recuperación y restauración de la operación ante la materialización de un riesgo, que incluyan:

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

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

3. Documentar las actividades que deberá realizar para dar respuesta a emergencias ante la ocurrencia de algún evento que afecte la operación normal con el SPID 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;

4. Documentar las acciones que deberá seguir para el regreso a 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 SPID, 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 SPID indicando los lineamientos, tipo de pruebas a realizar y periodicidad de las mismas;

III. Requisitos de certificación del aplicativo que utilizarán para conectarse al SPID La Institución de Crédito debe llevar a cabo, de conformidad con el Apéndice F del Manual, lo siguiente:

a) Acreditar que el aplicativo cumple con el protocolo de comunicación del SPID;

b) Acreditar que el aplicativo procesa adecuadamente las Órdenes de Transferencia, incluso cuando se presenta un alto volumen de ellas en un periodo corto de tiempo, y

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

IV. Requisitos de gestión de Riesgos Adicionales

La Institución de Crédito deberá satisfacer lo siguiente:

a) Contar con procesos, sistemas y personal adecuados para recabar, verificar y conservar la información de identificación de sus Clientes Emisores y Clientes Beneficiarios, según sea el caso, referida en la fracción I de la **50a.** de las presentes Reglas, así como aquella sobre conocimiento de las características de dichos clientes que permita evaluar el riesgo que pueden representar en la materia a que se refiere dicha Regla;

b) Contar con procesos que deberá seguir, así como sistemas y personal adecuados, para llevar a cabo la verificación a que se refiere la fracción IV de la **50a.** de las presentes Reglas;

c) Contar con procesos que deberá seguir, así como personal adecuado, para monitorear las transferencias realizadas por medio del SPID a través de los sistemas automatizados con que cuente, con el fin de detectar inusualidades en dichas transferencias o inconsistencias de estas con la información que sea del conocimiento de la Institución de Crédito de que se trate y tomar las acciones que procedan para aclarar tales observaciones;

d) Elaborar y documentar las políticas y procedimientos que deberá seguir para evaluar y mitigar los riesgos que la Institución de Crédito podría asumir ante la realización de transferencias por medio del SPID relacionadas con actos presuntamente ilícitos o con recursos de origen indeterminado, las cuales podrán formar parte de aquellas políticas y procedimientos con que cuente la Institución de Crédito en materia de riesgos similares, y

e) Contar con un modelo de evaluación de Riesgos Adicionales, que se obligue a aplicar a todos sus clientes que sean titulares de cuentas de depósitos de dinero en Dólares y que, por lo tanto, sean susceptibles de quedar como Clientes Beneficiarios de Órdenes de Transferencias que la Institución de Crédito de que se trata reciba a partir de su admisión al SPID, así como de sus Clientes Emisores con quienes llegue a convenir la tramitación de Solicitudes de Envío. Dicho modelo de Riesgos Adicionales deberá cumplir con las características establecidas en el **Anexo 2** de las presentes Reglas y deberá ser aprobado por el Comité de Riesgos con base en la propuesta que, al efecto, haga el Comité de Comunicación y Control que el Participante deba establecer de conformidad con las disposiciones aplicables, lo cual deberá ser informado por dicho Comité de Riesgos al Consejo de

Administración o Consejo Directivo de la Institución de Crédito, según corresponda. Asimismo, la Institución de Crédito deberá enviar al Banco de México, por conducto de la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, a más tardar a los 30 Días Hábiles Bancarios posteriores a aquel en que el modelo de Riesgos Adicionales referido se haya informado al Consejo de Administración o Consejo Directivo de que se trate, un documento que lo describa y que incluya al menos los aspectos indicados en el **Anexo 2**.

…

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 c), numeral 3 del inciso d) y numerales 1 y 2 del inciso e) de la fracción I de la **42a.**, así como las adiciones de los numerales 4 y 6 al inciso e) de la fracción I de la **42a.**, 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 numeral 1 del inciso d) de la fracción I de la **42a.**, así como la adición del numeral 8 al inciso e) de la fracción I de la **42a.**, 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 6 del inciso b), numeral 1 del inciso c) de la fracción I de la **42a.**, así como la adición del numeral 3 al inciso e) de la fracción I de la **42a.**, 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 7 del inciso b), numeral 3 del inciso c), numeral 2 del inciso d) de la fracción I de la **42a.**, así como las adiciones de los numerales 2 Bis, 4 Bis y 6 Bis al inciso b) y del inciso f) a la fracción I de la **42a.**, entrarán en vigor a los veinticuatro meses contados a partir de la fecha de entrada en vigor de la presente Circular.

BORRADOR