Anexo 1

Anexo Técnico

I. Introducción

El Banco Nacional de Obras y Servicios Públicos (Banobras) es una Institución de Banca de Desarrollo que se tipifica como empresa pública con participación estatal mayoritaria, cuenta con personalidad jurídica y patrimonio propios.

Banobras como parte del Sistema Financiero Mexicano, está obligado al cumplimiento de la normativa emitida por las Autoridades Financieras.

Derivado de lo anterior y con fundamento en la circular 13/2017 y Fracción III Disposición 62ª de la Circular 14/2017 del Banco de México; dirigida a los participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI) y demás interesados en actuar con tal carácter, relativa a las Reglas del Sistema de Pagos Electrónicos Interbancarios (SPEI); se formula el presente Anexo Técnico con la finalidad de que se realice una revisión por un auditor externo independiente en la que se indique el nivel de cumplimiento por parte de la Institución de los requisitos que solicitan las Disposiciones 8ª de la Circular 13/2017 y 58ª de la Circular 14/2017 del Banco de México.

II. Solicitud

El presente documento se elabora con el propósito de integrar los requerimientos para que un auditor externo independiente lleve a cabo la revisión de cumplimiento de los requisitos de las Disposiciones 8ª de la Circular 13/2017 y 58ª de la Circular 14/2017 del Banco de México.

III. Objetivo del servicio

Llevar a cabo una Auditoría por parte de un auditor externo independiente, con el propósito de que éste lleve a cabo una revisión de las reglas del SPEI conforme a los requisitos establecidos en las Disposiciones 8ª de la Circular 13/2017 y 58ª fracciones I, II, IV, V y VI, de la Circular 14/2017 del Banco de México, referentes a Seguridad Informática, Gestión del Riesgo Operacional, Protección a los Clientes Emisores y la Gestión de Riesgos Adicionales; considerando lo señalado en el Anexo M del Manual de Operación del SPEI versión 5.0.

IV. Datos, universo y alcance

Para llevar a cabo el servicio solicitado, es necesario considerar los siguientes elementos:

1. La revisión deberá ser sobre el cumplimiento de las obligaciones que les serán aplicables a Banobras a partir del 31 de enero de 2018.

2. El universo a evaluar deberá ser sobre el cumplimiento a lo establecido en las Disposiciones 8ª de la Circular 13/2017 y 58ª fracciones I, II, IV, V y VI de la Circular 14/2017 del Banco de México; considerando lo señalado en el Anexo M del Manual de Operación del SPEI versión 5.0.

V. Procedimientos

La auditoría deberá contemplar por lo menos los aspectos de las Disposiciones 8ª de la Circular 13/2017 y 58ª fracciones I, II, IV, V y VI de la Circular 14/2017 del Banco de México, considerando lo señalado en el Anexo M del Manual de Operación del SPEI versión 5.0., y de acuerdo a los procedimientos que se numeran a continuación:

V.I Prestación de servicios por parte de terceros:

1. Validar que en caso de que la Institución haya pactado con terceros, se les haya proporcionado una interface que les permita conectarse con el Sistema de Pagos en el que tenga el carácter de Participante o en el que pretenda participar de conformidad con lo dispuesto en las Disposiciones, o algún otro servicio que resulte esencial para el procesamiento de Órdenes de Transferencia, siempre y cuando cumplan con los requisitos y condiciones establecidos en la Circular, verificar que la Institución presente una solicitud de autorización al Banco de México, por conducto de la Gerencia de Operación y Continuidad de Negocio de los Sistemas de Pagos.

2. Verificar que junto con la solicitud, se haya proporcionado la documentación e información que se señala a continuación:

   I. Proyecto de contrato o instrumento jurídico que pretenda celebrar con el tercero. El referido contrato o instrumento deberá señalar expresamente la voluntad del tercero, respecto de los servicios materia de contratación, a sujetarse incondicionalmente a las Disposiciones y a las Normas Internas, así como a todas aquellas obligaciones a las que se sujeta la Institución que lo haya contratado, incluyendo de manera enunciativa y no limitativa a las siguientes:

      a. Permitir que el Banco de México realice visitas para verificar el cumplimiento de los requisitos aplicables a que se refieren las presentes Disposiciones y las Normas Internas;

      b. Proporcionar la información que el Banco de México solicite en los plazos que éste indique;

      c. Permitir que la Institución o el interesado que lo haya contratado y un auditor externo independiente de la citada Institución o del interesado tengan acceso a sus

Mera

instalaciones, documentos, equipos e información en general, y que realicen auditorías;

d. Entregar al auditor externo independiente de la Institución o del interesado los libros, códigos de sistemas, registros, manuales y documentos en general, relacionados con la prestación del servicio;

e. Guardar confidencialidad respecto de la información relativa a los aspectos técnicos del funcionamiento del Sistema de Pagos, así como de la información de las operaciones que conforme a la legislación aplicable esté definida como datos personales y que recabe como parte de las actividades que realice al amparo del contrato o instrumento jurídico que celebre con la Institución o el referido interesado;

f. Contar, en su caso, con lineamientos de seguridad y planes de continuidad de negocio que se ajusten a lo establecido en las Normas Internas, y

g. Establecer la prohibición para que el tercero subcontrate la prestación de los servicios que preste a la Institución o al interesado;

II. Aprobación del consejo de administración u órgano equivalente que tenga bajo su responsabilidad las funciones de administración de la Institución en actuar como tal, en la cual deberá constar que:

a) La contratación no pone en riesgo el cumplimiento de las disposiciones aplicables a la Institución respecto su operación en el Sistema de Pagos, y

b) Las prácticas de negocio del tercero son consistentes con la operación del Participante o del interesado;

III. Documentos que acrediten la experiencia, capacidad técnica y suficiencia de recursos humanos del tercero respecto de los servicios materia de contratación;

IV. El procedimiento que ofrezca el tercero a la Institución para identificar, medir, vigilar, limitar, controlar, informar y revelar los riesgos que puedan derivarse de la prestación de sus servicios;

V. Los mecanismos para la solución de controversias pactados entre a la Institución y el tercero, relativas al contrato o instrumento jurídico que hayan celebrado;

MRGN

VI. El procedimiento para evaluar el desempeño del tercero en la prestación de los servicios, el cumplimiento de sus obligaciones contractuales y la periodicidad de la evaluación;

VII. El documento que describa las acciones que se llevarán a cabo para la terminación ordenada del mismo, en el evento de que se suspenda la prestación del servicio a través del tercero y no sea posible sustituir inmediatamente al tercero en dicha prestación, y

VIII. Aquella documentación, información y certificaciones que adicionalmente el Banco de México le solicite.

V.II Seguridad Informática-Infraestructura Tecnológica:

Verificar que la Institución cuente con políticas y procedimientos en materia de Seguridad de la Información; las cuales realicen, lo siguiente:

3. Verificar que se cuente con un área responsable de la seguridad de la información y que ésta verifique que la administración de la Infraestructura Tecnológica se lleva a cabo conforme a las políticas y procedimientos de seguridad informática establecidos.

4. Validar que la política establecida procure y mantenga la solidez de la Infraestructura Tecnológica, que queden referidos, al menos, a los siguientes aspectos:

   a. Procedimientos para evaluar los protocolos 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 de Operación del SPEI versión 5.0.

   b. Procedimientos que contemplen el uso obligatorio de herramientas que permitan detectar virus informáticos y códigos maliciosos en la Infraestructura Tecnológica, así como procedimientos que permitan su actualización periódica conforme a lo especificado en el Apéndice M del Manual de Operación del SPEI versión 5.0.

   c. Procedimientos que permitan administrar las vulnerabilidades de seguridad informática derivadas de, entre otros factores, cambios, actualizaciones o errores en la Infraestructura Tecnológica.

   d. Procedimientos para inhibir la instalación de cualquier servicio, aplicación y/o software que no sea indispensable para la operación con el SPEI en la Infraestructura Tecnológica.

MRIOV

e. Procedimientos para 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.

f. 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.

5. Verificar que se cuenta con una política para la implementación de los sistemas informáticos, ya sea por parte de la Institución o por medio de una empresa externa contratada por ésta, especializada en el desarrollo de programas de cómputo (software), y que contengan los procedimientos siguientes:

   a. Procedimientos que aseguren que se sigue un proceso de desarrollo formal y documentado para la implementación de sus sistemas informáticos. El proceso de desarrollo deberá considerar, al menos, las siguientes etapas:

      i. Diseño del sistema informático.
      ii. Desarrollo del sistema informático conforme al diseño anterior.
      iii. Validación de funcionalidades, propósito, capacidad y calidad del sistema informático.
      iv. Liberación y/o instalación del sistema informático.
      v. Seguimiento formal a cambios en el sistema informático.

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

   c. Procedimientos que aseguren que los componentes que brindan seguridad a sus sistemas informáticos se encuentren vigentes y que se revise su vigencia conforme a lo especificado en el Apéndice M del Manual de Operación del SPEI versión 5.0.

   d. Procedimientos que aseguren que la seguridad del sistema informático sea revisada de forma estática y dinámica.

MRGV

e. Procedimientos que permitan vigilar, auditar y rastrear los accesos y actividades realizadas por los diferentes usuarios de los servicios informáticos 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 período de al menos seis meses.

f. Procedimientos que permitan vigilar, auditar y rastrear todas las operaciones realizadas por los sistemas informáticos. Estos procedimientos deberán considerar el resguardo de la información recabada por un período de al menos seis meses.

6. Corroborar que se cuenten con políticas del manejo seguro de la información electrónica, que incluyan:

   a. Procedimientos que aseguren que al desechar o dar de baja componentes o dispositivos físicos (hardware) de la Infraestructura Tecnológica la información contenida en estos sea irrecuperable.

   b. Procedimientos para restringir el acceso a los puertos físicos de conexión y dispositivos periféricos de la Infraestructura Tecnológica.

   c. Procedimientos para el resguardo de información de la Infraestructura Tecnológica y Operativa.

   d. Procedimientos que permitan detectar la alteración o falsificación de la información contenida en la Infraestructura Tecnológica.

   e. Procedimientos que permitan cifrar la información sensible en la Infraestructura Tecnológica.

7. Contar con políticas que se obligue a seguir para implementar mecanismos de control de acceso a la Infraestructura Tecnológica, con base en criterios establecidos para determinar que dichos mecanismos sean robustos y seguros, que incluyan:

   a. Procedimientos que permitan implementar mecanismos y controles robustos de acceso lógico a la Infraestructura Tecnológica.

   b. Procedimientos para una gestión de usuarios y contraseñas.

   c. Procedimientos que permitan realizar bloqueo manual y automático de la Infraestructura Tecnológica para asegurar que los equipos solo puedan ser utilizados por personal autorizado.

MRAV

d. Procedimientos para la gestión de privilegios de acceso a la Infraestructura Tecnológica.

e. Procedimientos que permitan vigilar y auditar los accesos y actividades realizadas por los usuarios de la Infraestructura Tecnológica. Estos procedimientos deberán considerar el resguardo de la información recabada por un período de al menos seis meses. Así como la atención y seguimiento a los posibles eventos de fraude relacionados con transferencias.

8. Validar que se cuenten con políticas que deban seguir para la comunicación con el Banco de México, que incluyan:

   a. Procedimientos para restringir el acceso a internet desde la Infraestructura Tecnológica.

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

Canales Electrónicos

9. Validar que los interesados que ofrezcan a sus Clientes Emisores Canales Electrónicos cuenten con procesos y/o sistemas debidamente documentados que consideren al menos lo siguiente:

   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.

MEW

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 período 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.

V.III Riesgo Operacional

10. Validar que se cuente con políticas y procedimientos para la administración de riesgos operacionales, que incluyan lo siguiente:

a. 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.

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

c. 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.

d. Manuales de procedimientos y de operación que describan las actividades requeridas

MRVA

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 realiza para la operación del SPEI y una definición precisa de responsabilidades.

11. Validar el establecimiento de medidas de mitigación de los riesgos, que cuenten con:

    a. 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.

    b. 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.

    c. 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.

12. Validar el establecimiento de procedimientos para la recuperación y restauración de la operación con el SPEI ante la materialización de riesgos operacionales, que incluyan:

    a. 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 SPEI en un nivel mínimo aceptable.

    b. 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.

    c. 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.

d. 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.

e. Un plan de pruebas al que deberá dar seguimiento para evaluar las estrategias y procedimientos de continuidad implementados relacionados con la operación del SPEI indicando los lineamientos, tipo de pruebas a realizar y periodicidad de las mismas.

V. V Protección a los Clientes Emisores

13. Verificar que se cuenten 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:

        i. Contar con mecanismos para certificar y validar la identidad del Cliente Emisor.
        ii. Poner a disposición de sus Clientes Emisores la información sobre los medios y procesos de comunicación en caso de contingencia.
        iii. 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.

14. Validar que cuando 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:

mevo

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 garanticen 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 el numeral V.II, punto 9, inciso d), del presente Anexo técnico, 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. La Institución deberá 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;

MRM

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. Preregistrar 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 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.

MRN

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 a la Institución 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.

V. VI Gestión de Riesgos Adicionales

15. Validar el cumplimiento a regulaciones y supervisiones 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, debiendo satisfacer los siguientes requisitos:

a. Que la Institución no haya sido sujeta a la imposición de una sanción firme por infracciones a dicha regulación al menos en los últimos tres años.

b. En caso de que la Institución haya sido sancionada conforme al inciso a) anterior, verificar que se haya elaborado por un auditor externo independiente un informe para acreditar ante el Banco de México, que la Institución ha realizado las acciones necesarias para corregir las causas que hubieran dado origen a las infracciones respectivas.

c. En el evento de que la Institución haya sido notificada una posible o presunta infracción a la regulación referida en esta fracción, elaborar por un auditor externo independiente un informe 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.

d. En caso de que no ser sujeto 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, elaborar por un despacho externo independiente un informe que acredite que la Institución cuenta con la capacidad para dar

mcpr

cumplimiento a la regulación contemplada en esta misma fracción que les resulten aplicables.

V.VII. Requisitos de interoperabilidad

16. Validar que 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.

VI. Requisitos del Auditor

El auditor externo deberá cumplir con los requisitos generales, los requisitos de independencia, y requisitos técnicos.

VI.I Requisitos Generales

1. Declaración bajo protesta de decir verdad firmada por el representante legal de no haber sido sentenciado por delitos patrimoniales.

2. Declaración bajo protesta de decir verdad firmada por el representante legal de no estar inhabilitado para ejercer el comercio o para desempeñar un empleo, cargo o comisión en el servicio público, o en el sistema financiero mexicano, así como no haber sido concursado en los términos de la Ley relativa o declarado como quebrado sin que haya sido rehabilitado.

3. Declaración bajo protesta de decir verdad firmada por el representante legal de no tener litigios pendientes con Banobras.

4. Declaración bajo protesta de decir verdad firmada por el representante legal donde indique que los miembros del equipo de auditoría no deberán ser subcontratados y deberán haberse incorporado al despacho al menos 180 días naturales antes de la suscripción del contrato para evaluar el cumplimiento de los requisitos.

VI.II Requisitos de Independencia

El auditor externo no se considerará independiente cuando la persona o despacho de que se trate se ubique en alguno de los supuestos señalados en el artículo 189 fracciones I a IV, IX y X de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito y en los siguientes:

5. El auditor, el despacho en el que labore o algún socio o empleado del mismo proporcione servicios de consultoría sobre la elaboración de los procesos, procedimientos, políticas y criterios, así como los sistemas con que el interesado o participante deba contar para dar cumplimiento a los requisitos a que se refieren la Disposición 58ª de la Circular 14/2017 del Banco de México.

6. El auditor, el despacho en el que labore o algún socio o empleado del mismo proporcione servicios de operación, directa o indirecta, de los sistemas de información financiera del interesado o Participante, respectivamente, o bien, administración de su red local.

7. El auditor, el despacho en el que labore o algún socio o empleado del mismo proporcione supervisión de, diseño o implementación de los sistemas informáticos (*hardware y software*) de la entidad, que lleven a cabo actividades para las operaciones que el interesado o el Participante realicen a través del SPEI.

8. El auditor, el despacho en el que labore o algún socio o empleado del mismo proporcione servicios de administración, temporal o permanente; y en las decisiones de la Institución.

9. El auditor, el despacho en el que labore o algún socio o empleado del mismo, realice actividades de Auditoría interna relativa a la evaluación del nivel de cumplimiento de los requisitos a que se refieren las Reglas del SPEI.

10. El auditor, el despacho en el que labore o algún socio o empleado del mismo proporcione servicios de reclutamiento y selección de personal de la Institución para que ocupen cargos de director general o de los dos niveles inmediatos inferiores al de este último.

11. Cualquier otro que implique o pudiera implicar conflictos de interés respecto al trabajo de auditoría externa.

12. Los ingresos que el Auditor Externo Independiente perciba o vaya a percibir por llevar a cabo la evaluación del interesado o Participante, dependan del resultado de la propia evaluación o del éxito de cualquier operación realizada por el propio interesado o Participante que tenga como sustento la certificación del Auditor Externo Independiente.

Para dar cumplimiento a los numerales 5 a 12, del presente apartado, el Auditor Experto Independiente deberá integrar una declaración bajo protesta de decir verdad firmada por el representante legal, que cumpla con los requisitos de independencia.

mrm

VI.III Requisitos Técnicos

Seguridad de la Información

13. Proporcionar curriculum donde se plasme su experiencia en materia de consultoría en seguridad de la información y seguridad informática en el sector financiero de por lo menos 5 años.

14. Contar con al menos 2 Auditores Externos Independientes, titulados, en materia de seguridad informática, que se encuentren dentro del equipo de trabajo y cumplan con todas las características generales y de seguridad informática mencionadas en el presente apartado.

15. Los Auditores Externos Independientes involucrados en el proyecto deberán contar con al menos alguna de las siguientes certificaciones: CISSP (Certified Information System Security Professional), CISA (Certified Information Systems Auditor) o CISM (Certified Information Security Manager) o sus equivalentes que cumplan con las siguientes características:

    - Ser reconocidas a nivel mundial como estándar en seguridad informática, aceptación de un código de ética, un mínimo de experiencia en estas áreas, actualización continua sobre los conocimientos en el tema; así como, la atestiguación de un colega del medio que sustente la certificación.

16. Los Auditores Externos Independientes involucrados en el proyecto deberán haber participado en actividades o proyectos relacionados con seguridad de información y seguridad informática en los últimos 24 meses.

Gestión de Riesgo Operacional

17. Experiencia en consultoría en gestión del riesgo en el sector financiero de por lo menos 5 años.

18. Contar con al menos 1 Auditor Independiente que se encuentre dentro del equipo de trabajo, titulado, en materia de gestión del riesgo.

19. El Auditor Externo Independiente involucrado en el proyecto deberán contar con al menos dos de las siguientes certificaciones: ISO 31000, ISO 22301, Basilea II y COSO II o sus equivalentes.

MRW

20. Los Auditores Externos Independientes involucrados en el proyecto deberán demostrar experiencia en auditoría de gestión del riesgo y de gestión de continuidad de negocio en el sector financiero de por lo menos 2 años.

Para dar cumplimiento a los numerales 13 a 20, del presente apartado, el despacho deberá integrar al curriculum referencias de las Auditorías en materia de Seguridad de la Información, Plan de Continuidad de Negocio, y Administración de Riesgos Operacionales, en los últimos 5 años, para lo cual deberán incorporar en el curriculum la siguiente información: ente auditado, fecha, nombre del contacto, dirección, domicilio, teléfono, un extracto apropiado del contrato de prestación de servicios. Asimismo, se solicita evidencia de que los miembros del equipo de auditoría cuenten con sus certificados vigentes.

VII. Vigencia

La duración de la auditoría no deberá exceder de 50 días hábiles a partir del día siguiente al fallo, considerando la revisión de la documentación en sitio, entrevistas presenciales, elaboración de productos entregables, revisión de contratos, entre otras actividades.

VIII. Forma de pago

La forma de pago a la entrega y aceptación de los siguientes entregables, a partir del inicio de la vigencia del contrato:

	Entregable	Período	Porcentaje del Pago
1.	Plan de Trabajo y Metodología de Evaluación	A más tardar el día hábil 7	5%
2.	Observaciones y/o recomendaciones	A más tardar el día hábil 40	30%
3.	Proyecto de Informe y papeles de trabajo	A más tardar el día hábil 40	30%
4.	Informe Final	A más tardar el día hábil 50	35%

IX. Entregables

Derivado de las necesidades y de los beneficios que la Institución espera recibir con la contratación de este servicio, deberá considerarse la entrega de los siguientes documentos con las características que se señalan a continuación:

MRM

- Plan de trabajo de la Auditoría y Metodología de Evaluación deberá considerar la fecha compromiso de la conclusión de cada procedimiento del apartado V Requisitos del Auditor de este anexo, así como fecha de emisión de observaciones, de emisión del proyecto de informe, de entrega de papeles de trabajo y del informe final, respectivamente. Asimismo, se debe incluir la metodología de evaluación.

- Presentaciones semanales de avances de la auditoría para vigilar que se cumplan con los tiempos establecidos en el plan de trabajo.

- En caso de existir observaciones y/o recomendaciones se deberá asentar por cada una, un documento que describa la situación encontrada, el fundamento legal que determina el incumplimiento o referencia de mejor practica en caso de recomendaciones, el plan de acción sugerido para corregir o implementarla, así como la clasificación interna de su importancia en alto, medio, bajo o recomendación:

  - Alto: Son observaciones que representan un hecho pasado que causaron: Daño patrimonial, Robo o Fraude y Riesgo de Reputación.
  - Medio: Son observaciones que representan un hecho pasado, que ponen en riesgo el patrimonio de la Institución.
  - Bajo: Son observaciones que representan un hecho pasado, cuya materialización no pone en riesgo el patrimonio de la Institución:
  - Recomendación: Son sugerencias de Auditoría Interna que tienen propósito de mejorar el ambiente de control actual.

- Proyecto de informe, y papeles de trabajo deberá contener lo siguiente:

  - Objetivo de la auditoría.
  - Alcance de la auditoría.
  - Criterios, procedimientos y metodología de evaluación, que debe incluir lo siguiente:

    - El nivel de cumplimiento de cada requisito, indicando si: i) se cumple totalmente, ii) se cumple parcialmente, o iii) no se cumple
    - Metodología que especifique el procedimiento de evaluación utilizado.

MRN

- Validación del cumplimiento de los procedimientos establecidos en la planeación, contratación y ejecución en el apartado V de este anexo en el cual se describan:

    - Nivel de cumplimiento.
    - Justificación del nivel de cumplimiento especificado en cada requisito.
    - Situación encontrada de las debilidades.
    - Observaciones y/o recomendaciones indicando el fundamento legal.
    - Planes de remediación sugeridos para mitigar los hallazgos.
    - Conclusiones y opinión sobre el estado actual considerando los elementos evaluados.

- Papeles de trabajo, deberán estar integrados: por los documentos de análisis elaborados por los auditores, los cuales deberán describir el trabajo desarrollado de cada procedimiento del apartado V de este anexo, por la información soporte entregada por las diferentes áreas de la Institución, y por las observaciones e informe final. Los documentos que integren los papeles de trabajo deberán estar debidamente indexados y referenciados al informe final y documentación soporte.

- Informe final que contenga los requisitos del Banco de México, así como lo siguiente:

    - Objetivo de la auditoría
    - Alcance de la auditoría.
    - Criterios, procedimientos y metodología de evaluación, que debe incluir lo siguiente:
        - El nivel de cumplimiento de cada requisito, indicando si: i) se cumple totalmente, ii) se cumple parcialmente, o iii) no se cumple
        - Metodología que especifique el procedimiento de evaluación utilizado.
    - Validación del cumplimiento de los procedimientos establecidos en la planeación, contratación y ejecución en el apartado V de este anexo en el cual se describan:
        - Debilidades y brechas respecto de lo dispuesto en la Circular 13/2017 y 14/2017.
        - Conclusiones y opinión sobre el estado actual considerando los elementos evaluados.
        - Recomendaciones y/o Medidas de Corrección sugeridas para que Banobras logre el cumplimiento de las Disposiciones.
        - Planes de remediación en proceso.

Las observaciones y recomendaciones del informe final, deberán estar referenciados, con índices, marcas y fuente de información, respecto de los documentos de análisis elaborados por los auditores y la información soporte.

El informe deberá de ser entregado en papel membretado por la empresa con la que se firmará el contrato y firmado por el Auditor externo independiente en original y tres tantos.

MCW

Es importante mencionar que los informes y documentación generada son para uso interno; en su caso se podrán fotocopiar y turnar a las Entidades Fiscalizadoras y a las Autoridades Financieras que lo soliciten, sin requerir autorización del despacho ganador.

Los documentos deberán ser entregados en papel membretado por la empresa con el que se firmará el contrato y firmados por el Auditor responsable de la Auditoría.

X. Penalizaciones y Deductivas

Penas

En caso de que los entregables no se reciban por el Banco en las fechas establecidas, este se hará acreedor de la siguiente penalización:

a) 2% del valor del entregable por día de retraso.

Deductivas

En los términos de lo previsto por el artículo 53 bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento; Banobras aplicará al licitante que resulte ganador una deductiva del 2% del valor del entregable por cumplimiento parcial o deficiente de los mismos por cada día de atraso de las fechas establecidas en el plan de trabajo, a entera satisfacción de la Dirección de Auditoría Interna, de acuerdo a las características señaladas en el apartado X de éste anexo.

MRM