BANCO DE MÉXICO

16 de mayo de 2018

Resumen de requerimientos en materia de seguridad informática y continuidad operativa a los participantes del SPEI

De acuerdo con las Reglas del SPEI (Circular 14/2017 emitida por el Banco de México), los participantes de este sistema tienen las siguientes obligaciones:

En materia de seguridad informática:

En el aplicativo que los participantes utilizan para conectarse al SPEI:

- *[Regla 58a., fracción I, literal A, inciso a)]* "Contar con un área designada, responsable de la seguridad informática que verifique que la administración de la Infraestructura Tecnológica se lleva a cabo conforme a las políticas y procedimientos de seguridad informática establecidos".
- *[Regla 58a., fracción I, literal A, inciso b)]* "Contar con una política escrita que deberá procurar y mantener la solidez de la Infraestructura Tecnológica, que queden referidos, al menos, a los siguientes aspectos:

  1. 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;
  2. 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;
  3. Procedimientos que permitan administrar las vulnerabilidades de seguridad informática derivadas de, entre otros factores, cambios, actualizaciones o errores en la Infraestructura Tecnológica;
  4. 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;
  5. 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, 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"

- *[Regla 58a., fracción I, literal A, inciso c)]* "Política para la implementación de sus sistemas informáticos, 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. 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.
  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 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;
  4. Procedimientos que aseguren que la seguridad del sistema informático sea revisada de forma estática y dinámica;
  5. 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 periodo de al menos seis meses, y
  6. 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 periodo de al menos seis meses."
- *[Regla 58a., fracción I, literal A, inciso d)]* "Contar con políticas que se obligue a seguir para un manejo seguro de la información electrónica, que contengan los procedimientos siguientes:
  1. 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;
  2. Procedimientos para restringir el acceso a los puertos físicos de conexión y dispositivos periféricos de la Infraestructura Tecnológica;
  3. Procedimientos para el resguardo de información de la Infraestructura Tecnológica y operativa;
  4. Procedimientos que permitan detectar la alteración o falsificación de la información contenida en la Infraestructura Tecnológica, y
  5. Procedimientos que permitan cifrar la información sensible en la Infraestructura Tecnológica."

- *[Regla 58a., fracción I, literal A, inciso e)]* "Contar con políticas que se obligue a seguir para implementar mecanismos de control de acceso a la Infraestructura Tecnológica, con base en criterios que establezcan para determinar que dichos mecanismos sean robustos y seguros, que incluyan los procedimientos siguientes:
  1. Procedimientos que permitan implementar mecanismos y controles robustos de acceso lógico a la Infraestructura Tecnológica;
  2. Procedimientos para una gestión de usuarios y contraseñas;
  3. Procedimientos que permitan realizar bloqueo manual y automático de la Infraestructura Tecnológica para asegurar que los equipos solo puedan ser utilizados por personal autorizado;
  4. Procedimientos para la gestión de privilegios de acceso a la Infraestructura Tecnológica, y
  5. 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 periodo de al menos seis meses. Así como la atención y seguimiento a los posibles eventos de fraude relacionados con transferencias. "
- *[Regla 58a., fracción I, literal A, inciso f)]* "Contar con políticas que deberá seguir para la comunicación con el Banco de México, que incluyan los procedimientos siguientes:
  1. Procedimientos para restringir el acceso a internet desde la Infraestructura Tecnológica, y
  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."

En el aplicativo que los participantes ponen a disposición de sus clientes para que estos puedan instruir transferencias a través del SPEI:

- *[Regla 58a., fracción I, literal B]* "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."

- *[Regla 71a.]* "Los Participantes distintos a Instituciones de Crédito que ofrezcan a sus Clientes Emisores el servicio de transferencias electrónicas por medio del SPEI, a través de Canales Electrónicos, deberán cumplir con los requerimientos previstos en la presente Regla.

  I. Deberán requerir y proporcionar a sus Clientes Emisores elementos de verificación de identidad para la realización de operaciones a través de los Canales Electrónicos. Estos elementos deberán ser los siguientes:

  a) Basados en datos que solo conoce el Cliente. Se componen de datos del Cliente recopilados por el Participante que son solo del conocimiento del Cliente, entre los que se incluyen información biográfica y contraseñas. Las contraseñas deberán tener una longitud mínima de: i) cuatro caracteres para operaciones instruidas a través cajeros automáticos; y de ii) ocho caracteres para operaciones instruidas a través de internet;

  b) Basados en objetos que solo posee el Cliente. Se componen por información obtenida de, por ejemplo, dispositivos generadores de contraseñas dinámicas de un solo uso, del chip de una tarjeta o de dispositivos móviles pre-registrados con el Participante. En caso de que los Participantes decidan utilizar estos elementos de verificación de identidad a través de dispositivos cuya principal función sea la generación de contraseñas dinámicas de un solo uso, éstos deberán proporcionar dichos dispositivos a los Clientes con los cuales acuerden la realización de Órdenes de Transferencia a través de Canales Electrónicos;

  c) Basados en las características inherentes del Cliente: Se componen por información derivada de las propias características (biométricas) del Cliente, como podrían ser escaneo de retinas vivas, escaneo de huellas dactilares vivas, reconocimiento facial, entre otros.

  II. Para permitir el inicio de una sesión en Canales Electrónicos, los Participantes distintos a las Instituciones de Crédito deberán solicitar y validar, al menos: i. el identificador del Cliente Emisor, el cual deberá ser único para cada Cliente Emisor y tener una longitud mínima de 6 caracteres, en el caso de la presentación de Órdenes de Transferencia a través de cajeros automáticos, el identificador de Cliente podrá ser la tarjeta de débito entregada por el Participante al Cliente Emisor; y ii. al menos un elemento de verificación de los comprendidos en los incisos a), b) o c) de la fracción I de la presente Regla.

  III. Los Participantes deben impedir la lectura en pantalla de los elementos de verificación de identidad usados por el Cliente en los Canales Electrónicos.

IV. En cada ocasión que el Cliente Emisor pretenda realizar la instrucción de una Solicitud de Envío, se les deberá solicitar un segundo elemento de verificación de identidad correspondiente a los previstos en la fracción I anterior, adicional a los utilizados para el inicio de sesión en los Canales Electrónicos, con excepción de instrucciones de Solicitudes de Envío por un monto de hasta ocho mil pesos, en las que el Participante podrá no requerir a sus Clientes Emisores utilizar un segundo elemento de verificación."

En materia de continuidad operativa:

- *[Regla 58a., fracción II, inciso 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."

- *[Regla 58a., fracción II, inciso 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 centros de datos que alojan a la Infraestructura Tecnológica dispuesta para operar con el SPEI."

- *[Regla 58a., fracción II, inciso 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 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;
    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.

- *[Regla 58a., fracción III, inciso e)]* "El interesado lleve a cabo, de conformidad con las especificaciones incluidas en el Apéndice O del Manual, lo siguiente:

    …

    e) Acreditar que pueden 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), en caso de tratarse de Instituciones de Crédito o instituciones para el depósito de valores."