Comisión Nacional Bancaria y de Valores

Auditoría de Ciberseguridad a la Banca Electrónica y Medios de Pago del Sistema Financiero del Gobierno Mexicano

Auditoría Combinada de Cumplimiento y Desempeño: 2018-5-06B00-21-0054-2019

54-GB

Criterios de Selección

Esta auditoría se seleccionó con base en los criterios establecidos por la Auditoría Superior de la Federación para la integración del Programa Anual de Auditorías para la Fiscalización Superior de la Cuenta Pública 2018 considerando lo dispuesto en el Plan Estratégico de la ASF.

Objetivo

Llevar a cabo la revisión de la ciberseguridad de la banca electrónica y sistemas de pago de las entidades del gobierno mexicano, verificando el marco normativo y regulatorio, la eficacia y eficiencia de las entidades a cargo de la regulación, supervisión y vigilancia del cumplimiento de los mecanismos de ciberseguridad, así como la aplicación de controles, en recursos humanos, procesos y tecnologías en las entidades gubernamentales que utilizan la banca electrónica y los sistemas de pago.

Consideraciones para el seguimiento

Los resultados, observaciones y acciones contenidos en el presente informe individual de auditoría se comunicarán a la entidad fiscalizada, en términos de los artículos 79 de la Constitución Política de los Estados Unidos Mexicanos y 39 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, para que en un plazo de 30 días hábiles presente la información y realice las consideraciones que estime pertinentes.

En tal virtud, las recomendaciones y acciones que se presentan en este informe individual de auditoría se encuentran sujetas al proceso de seguimiento, por lo que en razón de la información y consideraciones que en su caso proporcione la entidad fiscalizada, podrán confirmarse, solventarse, aclararse o modificarse.

Alcance

El universo seleccionado abarcó a la Comisión Nacional Bancaria y de Valores (CNBV) y al Banco de México (BANXICO) como organismos reguladores, así como a 7 participantes de la Banca de Desarrollo: Banco Nacional de Comercio Exterior, S.N.C. (BANCOMEXT), Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. (BANJÉRCITO), Banco Nacional de Obras y Servicios Públicos, S.N.C. (BANOBRAS), Financiera Nacional de Desarrollo

Agropecuario, Rural, Forestal y Pesquero (FND), Nacional Financiera, S.N.C. (NAFIN), Banco del Bienestar, S.N.C. (antes BANSEFI) y Sociedad Hipotecaria Federal, S.N.C. (SHF).

Antecedentes

Las Tecnologías de la Información y Comunicaciones (TIC), han transformado la forma de relacionarnos en la sociedad; las organizaciones públicas y privadas se encuentran en constante desarrollo de nuevos modelos de servicio que dependen cada vez más de las TIC. Esta transformación digital conlleva a grandes retos, entre los más complejos de contener, están los riesgos cibernéticos.

De acuerdo con el Informe Global de Riesgos 2019 del Foro Económico Mundial, los riesgos cibernéticos se mantienen dentro del cuadrante de alto impacto y alta probabilidad del panorama de riesgos mundiales. Esta encuesta identificó 43 tipos de riesgos, de los que destaca el "fraude y robo de datos masivo" ubicándose en el lugar número cuatro y los "ataques cibernéticos" situados en el número cinco.

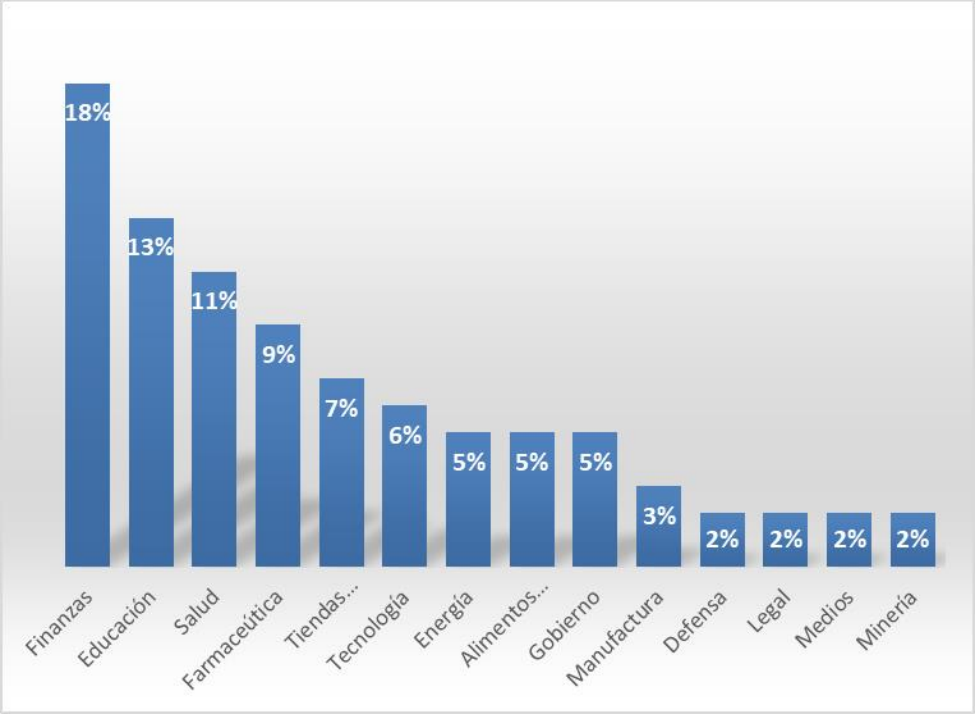
Acorde con el “Reporte Oficial de Cibercrimen 2020” de Grupo Herjavec[1], el costo mundial del cibercrimen en 2021 será de 6 trillones de dólares americanos, siendo que en 2015 fue de 3 trillones.

El sector financiero ha sido de los más intensivos en el uso de las TIC; sin embargo, es uno de los que mayores ataques cibernéticos recibe, de acuerdo con el reporte anual de 2019 sobre amenazas cibernéticas[2], este sector lo encabeza con un 18.0% del total, seguido por el educativo con un 13.0% y salud con un 11.0%.

1 Empresas especializadas en consultoría y servicios administrados de ciberseguridad.

2 Emitido por la empresa FireEye (especializada en análisis de ciberseguridad).

Reporte anual de 2019 sobre amenazas cibernéticas



Fuente: Desarrollo de la ASF con base en el reporte anual de amenazas cibernéticas 2019 de FireEye.

Dentro de los sistemas por donde fluye la mayor cantidad de transacciones y montos en el sector financiero, se encuentran los Sistemas de Pago.

Sistemas de Pago

Un Sistema de Pago es un conjunto de instrumentos, procedimientos y reglas para la transferencia de fondos entre dos o más participantes. El sistema incluye a los participantes y a la entidad que opera el mecanismo.

Los Sistemas de Pago se basan en los fundamentos emitidos por el Banco de Pagos Internacionales (BIS por sus siglas en inglés) [3], entre ellos, los "Principios aplicables a las infraestructuras del mercado financiero", dentro de los cuales se mencionan los siguientes:

- **Infraestructuras de los Mercados Financieros (IMF).** Son sistemas multilaterales entre instituciones participantes, incluyendo al operador del sistema, que permiten la compensación, liquidación o el registro de transacciones financieras. Las IMF se

[3] Es una institución internacional financiera propiedad de numerosos bancos centrales con sede en Basilea.

conforman de los Sistemas de Pagos, los depósitos centrales de valores, los sistemas de liquidación de operaciones con valores, las contrapartes centrales y los repositorios de operaciones. Las IMF suelen establecer un conjunto de reglas y procedimientos comunes para todos los participantes, una infraestructura tecnológica y un marco especializado de gestión del riesgo que es adecuado para los riesgos a los que están expuestas.

- **Los participantes**. Pueden ser las Administradoras de Fondos para el Retiro; Casas de Bolsa; Casas de Cambio; Instituciones de Crédito; Instituciones de Seguros; Sociedades Distribuidoras de Acciones de Sociedades de Inversión; Sociedades Financieras de Objeto Limitado, y Sociedades Operadoras de Sociedades de Inversión.

Los Sistemas de Pago tradicionalmente se clasifican en dos grupos, los de alto valor y los de bajo valor.

- Los Sistemas de Pago de alto valor, generalmente se liquidan el mismo día y la práctica general es que los pagos se liquiden tan pronto sea posible como es el caso del Sistema de Pagos Electrónicos Interbancarios (SPEI) en México, el cual es administrado por Banco de México (BANXICO).

- Los de bajo valor se liquidan en sistemas con esquemas de liquidación diferida. Las empresas usan estos sistemas para pagos comerciales, pagar nóminas y otros pagos que no son urgentes o que pueden ser programados previamente.

El Banco Mundial menciona que los Sistemas de Pago deben ser eficientes y confiables ya que:

- Soportan la estabilidad financiera, por medio de la mitigación de riesgos relacionados con las transacciones financieras.

- Apoyan la eficiencia de la economía facilitando el flujo de pagos, promoviendo la confianza en los consumidores en el uso de los servicios de pagos.

- Soportan la digitalización de los pagos gubernamentales en áreas como: protección social, e-gobierno y reformas de administración de finanzas públicas, también incluyen el cobro de impuestos, pago de salarios del sector público, adquisiciones públicas y otros pagos de gobierno a personas.

Importancia de los Sistemas de Pago para la Banca de Desarrollo

Las instituciones de la Banca de Desarrollo tienen como objeto fundamental facilitar el acceso al ahorro y financiamiento a personas físicas y morales; las 7 instituciones de la Banca de Desarrollo consideradas en esta revisión contemplan un amplio espectro de sectores a los que atienden: pequeña y mediana empresa, obra pública, apoyo al comercio exterior,

vivienda y promoción del ahorro y crédito al sector militar entre otras. La mayoría de las transacciones que realizan se hacen a través de los Sistemas de Pago como el SPEI.

Durante 2018 y 2019, la Banca de Desarrollo y la Tesorería de la Federación (operada por BANXICO) por medio del SPEI realizaron transacciones por un importe de 52.1 billones de pesos.

Estado de la Ciberseguridad en México

Las ciberamenezas no tienen límites territoriales, cada país debe tomar acciones en diversas áreas, que le permitan prevenir, detectar, responder y recuperarse ante estos ciberataques. Existen diversos estudios que han comparado y evaluado las medidas de ciberdefensa que los países han desarrollado, uno de los indicadores que más se utilizan para comprender el estado de la ciberseguridad de una nación es el Índice Global de Ciberseguridad (GCI por sus siglas en inglés) que ha emitido la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés), este indicador se basa en las mediciones siguientes:

- **Legales.** Basada en la existencia de instituciones y marcos de referencia relacionados con la ciberseguridad y el cibercrimen.

- **Técnicas**. Se basa en la existencia de instituciones y marcos de referencia técnicos relacionados con la ciberseguridad.

- **Organizacionales**. Se basa en la existencia de estrategias y políticas de coordinación de instituciones para el desarrollo de la ciberseguridad a nivel nacional.

- **Construcción de capacidades**. Se basa en la existencia de investigación y desarrollo, programas de entrenamiento y educación, profesionales certificados y entidades del sector público que fomenten el desarrollo de capacidades en ciberseguridad.

- **De cooperación**. Mide la existencia de asociaciones, marcos de cooperación y redes para compartir información relacionada con la ciberseguridad.

En los años que la ITU ha realizado la medición del GCI, México se ha mantenido por arriba de la media; aunque, de 2017 a 2018 descendió 35 posiciones como se observa en la tabla siguiente:

Tabla 1. Resultados del GCI de México

Año	Puntos obtenidos (GCI de un máximo de 1.0)	Total de países en la encuesta	Lugar obtenido por México
2015	0.324	196	18, (cabe aclarar que en este año varios países se podían ubicar en una misma clasificación, por ejemplo, en el lugar 18 se ubicaron 4 países)
2017	0.660	164	28, a partir de esta evaluación cada país se ubicó en un solo lugar.
2018	0.629	175	63

Fuente: Elaborado por la ASF con base en los reportes GCI 2015, 2017, 2018 del ITU.

Ciberseguridad en el Sector Financiero Mexicano

En 2019, la Secretaría General de la Organización de los Estados Americanos (OEA), presentó el estudio "Estado de la Ciberseguridad en el Sector Financiero Mexicano"[4], cuyo propósito fue dar a conocer información sobre eventos y/o incidentes de seguridad de la información (incluyendo los de ciberseguridad) y fraudes ocurridos en medios digitales en las instituciones financieras y su impacto, en dicho estudio se menciona:

- La totalidad de las entidades e instituciones financieras de México manifiestan que identificaron algún tipo de evento (ataques exitosos y ataques no exitosos) de seguridad digital en su contra. Los eventos de seguridad digital más comúnmente identificados durante el año 2018 fueron: i) el código malicioso (malware) (56.0% del total de entidades), ii) el phishing (correo electrónico dirigido para poder obtener información personal con fines maliciosos) (47.0% del total de entidades) y iii) la violación de políticas de escritorio limpio (clear desk) (31.0% del total de entidades). Se destaca que un 19.0% de las entidades e instituciones financieras identifican ocurrencia de eventos de malware diariamente.

- Con los valores obtenidos del estudio, se estimó que el costo total anual de respuesta y de recuperación ante incidentes de seguridad digital de las entidades e instituciones financieras en México en 2018 fue de 107 millones de dólares americanos aproximadamente.

[4] El estudio de la OEA proviene de una base de datos de 240 entidades e instituciones financieras participantes del Sistema Financiero Mexicano, el 15% corresponden a entidades públicas.

Esta revisión contribuye a la mejora de la ciberseguridad en los Sistemas de Pagos en temas regulatorios, de supervisión, vigilancia y condiciones de operación de los participantes y del administrador de estos sistemas.

Resultados

1. Regulación, Supervisión y Vigilancia de los Sistemas de Pago

Sistemas de Pago en el Sistema Financiero Mexicano

En México, existen distintos tipos de Sistemas de Pago; los de alto valor y los de bajo valor.

Sistemas de alto valor

- **Sistema de Pagos Electrónicos Interbancarios (SPEI)**. Es el principal medio por el cual los bancos liquidan transacciones entre ellos y entre sus clientes.

- **DALÍ**. Es el sistema de depósito, administración y liquidación de valores, donde se liquidan todas las operaciones con títulos del mercado de valores.

- **Sistema de Atención a Cuentahabientes (SIAC).** Opera en las cuentas corrientes que los bancos tienen en el Banco Central. Es el medio por el cual el Banco de México provee de liquidez a los bancos.

- **Sistema de Pagos Interbancarios en Dólares (SPID).** Permite el envío, procesamiento y liquidación de Órdenes de Transferencia Interbancarias denominadas en dólares a través de medios electrónicos entre cuentas de depósito a la vista en dólares con o sin chequera pagaderos en la República Mexicana correspondientes a personas morales que tengan su domicilio en territorio nacional.

Los Sistemas de Pago de bajo valor que están constituidos por cheques, transferencias electrónicas de fondos, domiciliaciones y tarjetas bancarias.

Tipos de Riesgo a los que se enfrentan los Sistemas de Pago

Entre los principales riesgos en materia de ciberseguridad a los que se enfrentan los Sistemas de Pago se encuentran:

- **Riesgo sistémico.** De acuerdo con el Banco de Pagos Internacionales, las Infraestructuras de Mercados Financieros (IMF) pueden tener interdependencias complejas al estar vinculadas entre sí o depender unas de otras, compartir participantes, así como prestar servicios a instituciones y mercados que se encuentren interrelacionados. Estas interdependencias pueden constituir una fuente significativa de riesgo sistémico, ya que incrementan la posibilidad de que las perturbaciones se trasladen rápida y ampliamente por los mercados.

- **Riesgo operacional.** Es el riesgo ocasionado por los errores que puedan producirse en los sistemas de información, los procesos internos y el personal o alteraciones provocadas por acontecimientos externos que deriven en la reducción, deterioro o interrupción de los servicios prestados.

La materialización del riesgo operacional puede ocasionar consecuencias reputacionales, legales, deteriorar el entorno sistémico y originar pérdidas financieras.

Funciones del Banco de México (BANXICO) en los Sistemas de Pago

BANXICO desempeña, bajo la Dirección General de Sistemas de Pagos e Infraestructuras de Mercado (DGSPIM) en coordinación con otras direcciones generales, las funciones siguientes:

Regulador

Regulador para todas las IMF del país, en algunos casos, es único y en otros comparte la responsabilidad con alguna otra autoridad. En el desempeño de este papel, el Banco emite circulares, reglas y autoriza las normas internas con base en las cuales deben operar las IMF y sus participantes.

También tiene como objetivo que las IMF cuenten con un esquema robusto de continuidad operativa que garantice un alto nivel de disponibilidad, además de que sean transparentes con los participantes y el público en general con respecto a sus reglas, beneficios y riesgos generados por su uso. [5]

Regulación del SPEI y el SPID

La Ley del Banco de México (Artículo 2) establece como finalidades de BANXICO propiciar el buen funcionamiento de los Sistemas de Pagos y promover el sano desarrollo del sistema financiero del país, para lo cual ha emitido normas internas, reglas de adhesión y funcionamiento para el SPEI y SPID, entre las que se encuentran:

- Circular 17/2010 donde se emiten por primera vez las Reglas del SPEI, define los criterios para actuar como participante, así como para la solicitud y envió de ordenes de transferencia de cuentahabientes, cancelación y liquidación de ordenes de transferencias, acreditación y devolución de ordenes de transferencias aceptadas y los escenarios en caso de alguna contingencia.

- Manual de Operación del SPEI, define la forma de conectarse y operar, los requisitos que deben de cumplir los participantes, entre ellos, los especificados en el apéndice M: requisitos de seguridad informática y de gestión del riesgo operacional.

[5] Información obtenida del documento Política y funciones del Banco de México respecto a las infraestructuras de los mercados financieros. agosto, 2016.

- Circular 4/2016 (Reglas del SPID), en ella se describe el esquema operativo, así como los requerimientos para actuar como participante.

- Circular 13/2017 que regula el procedimiento que deberán seguir los interesados para actuar como Participantes, así como establecer las obligaciones a las que deberán sujetarse.

- Circular 14/2017 (REGLAS DEL SPEI), donde se definen las normas internas del SPEI, describe el esquema operativo, los requisitos para ser admitidos como nuevos participantes o para su permanencia, se incluyen por primera vez los requisitos de seguridad informática y de gestión del riesgo operacional que tienen que cumplir los participantes y la forma en como los participantes dan a conocer su cumplimiento al administrador.

Supervisión y Vigilancia del SPEI y SPID

BANXICO, conforme al artículo 35 bis de la Ley del Banco de México y artículos 2, fracciones IX, XXII y XXIII, 3 y 4 de las reglas de supervisión, programas de autocorrección y del procedimiento sancionador, ejerce las funciones de inspección, supervisión y vigilancia de los participantes (Entidades Supervisadas), para verificar operaciones y revisar los registros y sistemas mediante la realización de visitas a las instalaciones, oficinas, sucursales o equipos automatizados, así como, el análisis y monitoreo de la información que las Entidades Supervisadas suministren al Banco. Lo anterior con la finalidad de comprobar el cumplimiento que den a lo dispuesto por la Ley, las Leyes y las Disposiciones.

Operador

El artículo 2 de la Ley de Sistemas de Pagos define como Administrador del Sistema a la sociedad, entidad o institución financiera que opera un Sistema de Pago, establece sus Normas Internas o, en su caso, lleva a cabo conforme a la normativa aplicable a ese Sistema de Pago, las acciones para coordinar la actuación de los Participantes.

BANXICO tiene la obligación de publicar en el Diario Oficial de la Federación, en el mes de enero de cada año, la lista de los acuerdos o procedimientos que tengan por objeto la compensación o liquidación de obligaciones de pago derivadas de órdenes de transferencia de fondos o valores que hayan reunido los requisitos previstos en el artículo anterior, así como aquellos en los que el Banco de México actúe como Administrador del Sistema.

BANXICO opera los Sistemas de Pago referentes a SPEI, SPID y SIAC.

Usuario

BANXICO es usuario, debido a que realiza mediante el SPEI pagos del Gobierno Federal (Tesorería de la Federación), en calidad de su agente financiero, además de realizar sus propios pagos, como los de nómina y a proveedores.

Rol de los Bancos Centrales en los Sistemas de Pago a Nivel Mundial

El Grupo de Banco Mundial (World Bank Group) realizó, en 2018, una encuesta sobre el alcance de la vigilancia en los Sistemas de Pagos (resumen de resultados de la cuarta encuesta de Sistemas de Pago Mundial), entre sus resultados se destacan los siguientes:

- Fuerte empuje de los bancos centrales hacia un alcance más amplio en la vigilancia de todos los Sistemas de Pago relevantes en un país, con independencia de si es el operador del sistema.

- La separación organizacional entre las funciones de revisión y operación de los bancos centrales ayuda a asegurar la aplicación consistente de las políticas y los estándares. Esta encuesta mostró que más del 85 por ciento de los países encuestados, tienen sus funciones de vigilancia segregadas de las tareas operacionales de los Sistemas de Pago, como se muestra en la tabla siguiente:

Tabla 1. Rol de los bancos centrales en los Sistemas de Pago

Bancos Centrales	La función de vigilancia de los Sistemas de Pago está segregada de las tareas operacionales ya sea en otra organización o por la independencia en la línea de reporte	
	# (cantidad)	% (porcentaje)
Total Mundial (110)	93	85%
Por ingreso		
Alto (43)	39	91%
Alto-medio (32)	24	75%
Bajo-medio (29)	24	83%
Bajo (6)	6	100%
Por Región		
Este de Asia y el Pacífico (14)	13	93%
Europa y Asia Central (11)	11	100%
América Latina y el Caribe (18)	10	56%
Este Medio y Norte de África (9)	7	78%
Sur de Asia (5)	4	80%
África Sub-Sahara (17)	13	76%
Países zona Euro (18)	18	100%
Otros Miembros del EU (8)	8	100%
Otros Países Desarrollados (10)	9	90%
Por tamaño de población		
>30 millones (34)	29	85%
>5 millones, <30 millones (38)	35	92%
<5 millones (38)	29	76%

Fuente: Grupo de Banco Mundial (World Bank Group).

Del análisis de las funciones de Regulador, Operador, Supervisor y Usuario realizadas por BANXICO respecto a los Sistemas de Pago SPEI y SPID se observó lo siguiente:

Segregación de funciones

La DGSPIM realiza las funciones de operador de los Sistemas de Pagos sobre la infraestructura administrada por la DGTI, sin que exista normativa interna, emitida y revisada por un tercero (ajeno a la DGSPIM y la DGTI), lo que no permite una segregación apropiada de funciones.

Como se menciona en la Tabla 1, se identifica que existe una tendencia de que los Bancos Centrales refuercen sus labores de revisión y regulación, y se aseguren que la función de operador esté segregada.

Regulador

- El SPEI inició operación en 2004; en mayo de 2006, emitió la Circular1/2006 donde se informa el ingreso como participantes del SPEI a las afores, casas de bolsa, casas de cambio, aseguradoras, sofoles, sociedades distribuidoras de acciones de sociedades de inversión y sociedades operadoras de fondos de inversión, la cual no contemplaba controles de seguridad de la información.

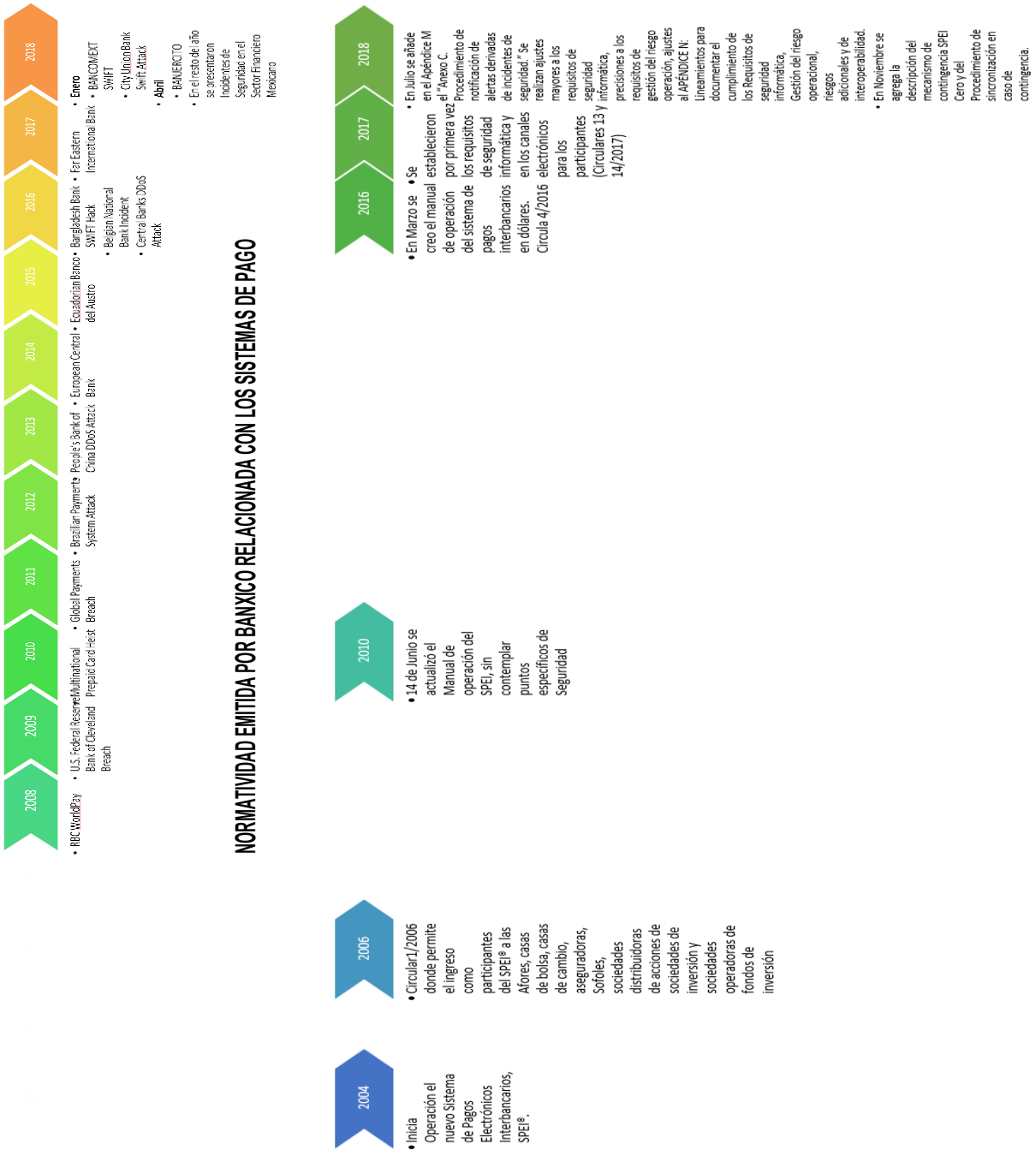
- En marzo de 2016, BANXICO incluyó por primera vez, controles relacionados con la seguridad de la información para el SPID en su Circular 4/2016 y para el SPEI y los canales electrónicos que lo soportan en sus Circulares 13/2017 y 14/2017, ambas publicadas el 4 de julio de 2017; sin embargo, aún no se ha establecido normatividad interna específica de seguridad de la información para su rol como operador de los Sistemas de Pago.

- Para el desarrollo de los 25 requisitos de seguridad informática y de gestión del riesgo operacional del Manual de Operación del SPEI solicitados en la Regla 58a. de la Circular 14/2017 y detallados en el apéndice M, la DGSPIM solicitó la participación de la Dirección General de Tecnologías de Información (DGTI) responsable del soporte y administración de la infraestructura tecnológica del SPEI.

- Entre 2008 y 2017, ocurrieron al menos una docena de ataques cibernéticos relacionados con los Sistemas de Pagos e infraestructura tecnológica de bancos centrales en diferentes partes del mundo, como se muestra en la imagen 1.

- BANXICO, a partir de mayo de 2018, ha fortalecido los mecanismos en materia de seguridad de la información.

Imagen 1. INCIDENTES DE SEGURIDAD RELACIONADOS CON SISTEMAS DE PAGO EN MÉXICO Y EN EL RESTO DEL MUNDO



Fuente: Desarrollado por la ASF.

Revisión del alcance de la normatividad emitida por BANXICO en materia de ciberseguridad

Debido a la complejidad y sofisticación de las amenazas cibernéticas, se han desarrollado distintas disciplinas que diferencian a la seguridad de la información, tales como:

- La Seguridad de la Información[6] es la que "asegura que la información en una organización esté protegida ante, la revelación a usuarios no autorizados (confidencialidad), modificación inapropiada (integridad) y la falta de accesibilidad cuando es requerida (disponibilidad)".

- La ciberseguridad[7] es definida como "la protección de los activos de información, abordando las amenazas a la información procesada, almacenada y transportada por los activos de información interconectados".

Por su parte, el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) menciona que:

- La Ciber resiliencia es "la habilidad de anticiparse, mantenerse, recuperarse y adaptarse ante condiciones adversas, estresantes, ataques o compromisos en sistemas que incluyen ciber recursos".

Existen distintos marcos de referencia internacionales en materia de seguridad de la información, ciberseguridad y ciber resiliencia que contienen las mejores prácticas en la materia y son utilizados en distintas organizaciones y sectores, tales como el financiero, entre los cuales se encuentran los siguientes:

6 Acorde con el manual de fundamentos de Ciberseguridad de la ISACA.

7 Id.

Tabla 2. Marcos de Referencia

Marco de referencia	Organización que lo emite	Enfoque
Information Security Management System (ISMS) – ISO/IEC 27001	Organización Internacional de Normalización (ISO)	Seguridad de la Información
Control Objectives for Information and Related Technology (COBIT)	ISACA	Seguridad de la Información (Gobernabilidad)
Business Continuity Management (BCM) – ISO 22301	ISO	Seguridad de la Información (Continuidad)
ISO 31000 – Risk Management	ISO	Seguridad de la Información (Administración de Riesgos)
ISO 27032 – Cybersecurity	ISO	Ciberseguridad
NIST Cybersecurity Framework (CSF)	Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) de EUA	Ciberseguridad
NIST SP 800 - 53	NIST	Ciberseguridad
FFIEC Cybersecurity Assesssment Tool	Federal Financial Institutions Examination Council (FFIEC)	Ciberseguridad
NIST SP 800 - 160	NIST	Ciber resiliencia
MITRE Cyber resiliency Design Principles	The MITRE Corporation	Ciber resiliencia
CPMI-IOSCO guidance for cyber-resilience of financial market infrastructures	Comité de pagos e Infraestructuras de Mercado (CPM) – Organización Internacional de Comisiones de Valores (IOSCO)	Ciber resiliencia

Fuente: Desarrollado por la ASF.

Se puede entender a la ciberseguridad y ciber resiliencia como partes de la seguridad de la información que aplican una mayor cantidad de controles y mecanismos de protección para las infraestructuras críticas de las organizaciones y con eso contar con mayores herramientas para enfrentar a las ciber amenazas.

La Auditoría Superior de la Federación desarrolló un modelo para evaluar el nivel de madurez de ciberseguridad de la administración y operación de los sistemas SPEI y SPID, basado en el Marco de Referencia de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés), se realizó el análisis de los 25 requisitos de seguridad informática y de gestión del riesgo operacional solicitados en el apéndice M del Manual de Operación del SPEI, del cual se identificaron 62 subcategorías de las 108 que contiene el marco del NIST, algunas de las cuales pudieran ser aplicables en los requisitos solicitados por BANXICO; por otra parte, en las circulares 4/2016, 13/2017 y 14/2017, no se incluyen algunos temas relacionados con ciber resiliencia[8], por lo que se le recomendó evaluar la conveniencia de su inclusión, cabe señalar que, aunque la normatividad referida no las incluye, en la evaluación realizada por la ASF que se presenta en el resultado 3, se observó que las entidades revisadas contemplan dentro de sus controles estas subcategorías.

[8] El Banco de Pagos Internacionales (BIS por sus siglas en inglés), en su publicación *Rango de prácticas de Ciber resiliencia*, menciona que la mayoría de los Banco Centrales en su labor de supervisión en esta materia, utilizan marcos internacionales tales como, el Marco de Referencia de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés).

Operador

En el resultado núm. 3 de este informe se presenta la evaluación del nivel de madurez de ciberseguridad de BANXICO como operador de los Sistemas de Pagos.

Supervisor

La regla 74a. está relacionada con las funciones de supervisión y vigilancia:

"74a. Informe y evaluación periódica. tercer párrafo se indica "El informe y constancia a los que se refiere el párrafo anterior deberán enviarse a través de la Gerencia de Operación y Continuidad de Negocio de los Sistemas de Pagos en términos de lo establecidos en el Apéndice N del Manual, dentro de los sesenta días naturales siguientes al cierre del ejercicio de que se trate".

El artículo donde se definió el plazo en el cual los participantes debían de entregar información del cumplimiento de los 25 requisitos es:

"DÉCIMO Transitorio. Tratándose de aquellas entidades que a la fecha de entrada en vigor de las presentes Reglas tengan el carácter de Participantes del SPEI conforme a las "Reglas del Sistema de Pagos Electrónicos Interbancarios", […] serán consideradas como Participantes en términos de las presentes Reglas hasta que el Administrador emita una resolución. Asimismo, conservarán el carácter de Participante antes referido únicamente aquellas entidades antes indicadas que obtengan la resolución favorable del Administrador sobre su admisión como Participante y celebren el Contrato a que se refieren las presentes Reglas. Para efectos de lo anterior, los Participantes interesados deberán presentar la documentación establecida en la 74a. de estas Reglas, de conformidad con lo establecido en la fracción IV, del Artículo Décimo Primero Transitorio de estas Reglas a más tardar el 28 de febrero de 2018".

Durante la revisión realizada por este organismo fiscalizador a las labores de supervisión que BANXICO llevó a cabo, respecto del informe de cumplimiento de los 25 requisitos solicitados en las reglas 58a y 67a de la Circular 14/2017 que enviaron los participantes de la Banca de Desarrollo: BANJERCITO, BANOBRAS, BANCOMEXT, NAFIN, SHF, se observó lo siguiente:

- Al momento de recibir la información de los participantes (28 de febrero de 2018 como se señala en el artículo DÉCIMO Transitorio), BANXICO no había establecido los procedimientos o manuales referentes a la supervisión de telecomunicaciones y seguridad informática y designado al personal especializado responsable de la evaluación de la información.

- A la fecha de la auditoría (diciembre 2019) no se había establecido formalmente un acuerdo en BANXICO, entre la Dirección General de Asuntos del Sistema Financiero, la Dirección General Jurídica, la Dirección General de Sistemas de Pagos e Infraestructuras

de Mercados, y la Dirección General de Tecnologías de la Información, para la coordinación y delimitación de las labores que llevan a cabo en la admisión, autorización, acceso, evaluación de información proporcionada y supervisión de los participantes en el SPEI y SPID .

- Los manuales de procedimientos de Operación Supervisión de medios de pagos y Proceso de Seguimiento de la Regulación In Situ, se encontraban desactualizados ya que no contemplaban la delimitación formal de las responsabilidades de las nuevas áreas involucradas en la supervisión, de acuerdo con las facultades de cada una de éstas.

- La definición de controles para el registro y seguimiento de la revisión Extra Situ que deben seguir los involucrados, no se encontraba actualizada conforme a los nuevos procesos y responsabilidades de la DGSPIM, con la finalidad de mantener uniformidad en la revisión y en la evidencia documental que se recaba como parte de la revisión citada.

- De las evaluaciones realizadas por la DGSPIM al cumplimiento de los 25 requisitos listados en el apéndice M: requisitos de seguridad informática y de gestión del riesgo operacional para los Bancos que integran la Banca de Desarrollo, se proporcionó un documento sin fecha y firma y sólo se evaluaron 10 de los 25 requisitos.

- En las Circulares 13/2017 y 14/2017, no se estableció un periodo de tiempo para que la Gerencia de Operación y Continuidad de Negocio de los Sistemas de Pagos, ahora, Gerencia de Supervisión de Sistemas de Pagos e Infraestructuras de Mercados de BANXICO, emitiera un pronunciamiento respecto al informe y evidencias proporcionados por los participantes y no se observó que realizara un análisis de riesgo para determinar acciones de mitigación.

- A la fecha de la auditoría (diciembre 2019), la DGSPIM no había emitido pronunciamiento a los participantes de la Banca de Desarrollo, sobre el cumplimiento de los requisitos solicitados en el apéndice M: requisitos de seguridad informática y de gestión del riesgo operacional, acorde con lo solicitado en la regla 74a. de la Circular 14/2017, con excepción de BANJERCITO y BANCOMEXT donde realizó visitas de investigación derivadas de los incidentes de ciberseguridad ocurridos en 2018.

Imposición de multas

En la Circular 14/2017, se menciona la regla 99a. Proporcionar información al Administrador; la cual establece que los participantes deberán proporcionar al Administrador, en los términos y plazos que este indique, la información y documentación relativa a cualquier aspecto relacionado con la operación del SPEI que se les requiera por escrito.

Los Participantes debieron de haber presentado la documentación establecida en la regla 74a. de la Circular 14/2017, a más tardar el 28 de febrero de 2018 (artículo DÉCIMO TRANSITORIO de la Circular 14/2017).

Se observó que Banco del Bienestar, durante 2018, solicitó a BANXICO una prórroga para la entrega de la documentación requerida en la regla 74a. de la Circular 14/2017, mediante un escrito con fecha 28 de febrero; el 1 de marzo BANXICO autorizó dicha prórroga con vencimiento al 18 de mayo, este mismo día, Banco del Bienestar solicitó una segunda prórroga; el 22 de mayo BANXICO le niega la segunda prórroga y agrega que deberá llevar a cabo las acciones correspondientes a fin de entregar el informe de cumplimiento a la brevedad posible. El Banco del Bienestar envió a BANXICO el 15 de octubre, la información requerida del cumplimiento de los requisitos de seguridad informática y de gestión de riesgo operacional.

A la fecha de la auditoría (diciembre 2019) BANXICO no había impuesto multa o sanción al Banco del Bienestar, conforme a la regla 16a. “Supervisión y sanción. El Banco de México supervisará el cumplimiento de cada Participante a lo dispuesto en las presentes Disposiciones y en las Normas Internas y cualquier incumplimiento será sancionado en términos de lo dispuesto en la Ley del Banco de México y demás ordenamientos que resulten aplicables” de la circular 13/2017.

Durante 2020, BANXICO inició el proceso para la imposición de una multa a dicho banco por el incumplimiento del plazo de entrega de la información respecto a la regla 74a. de la Circular 14/2017.

Metodología para la elaboración del plan anual de visitas de inspección

La Dirección de Regulación y Supervisión de BANXICO a partir de 2014, desarrolló una metodología basada en riesgos para priorizar la supervisión en el caso específico del SPEI y del SPID, la DGSPIM en 2018 desarrolló su propia metodología con la cual elabora su plan anual de visitas. Se identificó que, bajo esta metodología, durante 2018 y 2019, ninguna entidad de la Banca de Desarrollo fue sujeta a una visita de inspección por parte de esta dirección para revisar el cumplimiento de las Circulares 4/2016, 13/2017 y 14/2017. Es importante mencionar que, durante estos años, la Banca de Desarrollo operó más de 52 billones de pesos por medio del SPEI. Las únicas visitas que se realizaron fueron derivadas de los incidentes de ciberseguridad reportados por BANJERCITO y BANCOMEXT.

Usuario (participante)

- BANXICO indicó que, mediante los programas de trabajo comunica los niveles de disponibilidad del SPEI, los cuales se asocian a niveles de servicio para aquellos que provee en su carácter de operador del sistema y participante; sin embargo, dichos niveles no se encuentran definidos en el contrato firmado con la TESOFE ni identifica las responsabilidades de BANXICO en caso de incumplir con los mecanismos de seguridad.

Coordinación y comunicación entre BANXICO y la CNBV en las labores de vigilancia y supervisión

La Comisión Nacional Bancaria y de Valores (CNBV), es un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público (SHCP), con facultades en materia de autorización, regulación, supervisión y sanción sobre los diversos sectores y entidades que integran el Sistema Financiero Mexicano, así como sobre aquellas personas físicas y morales que realicen actividades previstas en las leyes relativas al sistema financiero. La Comisión se rige por la Ley de la CNBV.

Acorde con el Convenio de Colaboración en Materia de Supervisión celebrado entre BANXICO y la CNBV el 15 de diciembre de 2017, el intercambio de información sólo aplica para visitas de inspección ordinarias, es decir, BANXICO envía su plan anual de visitas para que la CNBV tenga conocimiento de éste, sin que se comparta más información.

La CNBV firmó en el marco del Foro sobre Ciberseguridad, celebrado en octubre de 2017, los principios para el Fortalecimiento de la Ciberseguridad para la Estabilidad del Sistema Financiero Mexicano.

A raíz de los incidentes de seguridad reportados en el Sistema Financiero Mexicano, el 24 de mayo de 2018 se dio a conocer el documento “Bases de Coordinación en Materia de Seguridad de la Información”.

Los documentos anteriormente mencionados no establecen la colaboración entre BANXICO y la CNBV para compartir los hallazgos y observaciones identificados en las visitas de inspección y vigilancia que efectúen en materia de riesgo tecnológico y seguridad de la información.

La CNBV realizó visitas en 2017 a BANCOMEXT, SHF, Banco del Bienestar, BANJERCITO y en 2018 a BANOBRAS y Banco del Bienestar, donde identificó hallazgos relacionados con temas de riesgo operacional y tecnológico, sin que dichos resultados se compartieran con BANXICO.

Por lo anterior, se recomienda establecer entre BANXICO y la CNBV protocolos para compartir información de forma oportuna de los hallazgos y observaciones que se identifiquen durante las visitas de supervisión y revisión en materia de riesgo tecnológico y seguridad de la información.

2018-0-98001-21-0054-01-001 **Recomendación**

Para que el Banco de México garantice que la normativa interna en materia de seguridad informática y de gestión del riesgo operacional en su rol de operador, sea consistente, en lo que corresponda, con la regulación emitida a los participantes de los Sistemas de Pago y lleve a cabo acciones para que los procesos de revisión relativos a su rol de operador de los Sistemas de Pagos, sean realizados por un tercero independiente de la Dirección General de

Sistemas de Pagos de Infraestructuras de Mercados y la Dirección General de Tecnologías de Información.

2018-0-98001-21-0054-01-002 **Recomendación**

Para que el Banco de México formalice los acuerdos que determinan las funciones y responsabilidades entre las distintas direcciones encargadas de realizar el análisis y monitoreo de la información proporcionada por los participantes de los Sistemas de Pago y se incluyan en los manuales de procedimientos de Operación y Supervisión de medios de pagos y Proceso de Seguimiento de la Regulación In Situ y Extra Situ.

2018-0-98001-21-0054-01-003 **Recomendación**

Para que el Banco de México implemente mecanismos que le permitan determinar el perfil de riesgo de cada participante tomando en cuenta el nivel de cumplimiento de sus controles de seguridad informática y gestión del riesgo operacional, cambios relevantes en su infraestructura, procesos, ciberamenazas, entre otros, que puedan afectar a la infraestructura particular de cada participante o a los Sistemas de Pagos en su conjunto y, con base en ello, pronunciarse con los interesados y, en caso de ser necesario, aplicar acciones de mitigación de los riesgos identificados.

2018-0-98001-21-0054-01-004 **Recomendación**

Para que el Banco de México evalúe la conveniencia de incluir en los requisitos de seguridad de la información del Sistema de Pagos Electrónicos Interbancarios (SPEI) y el Sistema de Pagos Interbancarios en Dólares (SPID), las 62 subcategorías del marco de referencia de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) que no están contempladas en su marco normativo.

2018-5-06B00-21-0054-01-001 **Recomendación**

Para que la Comisión Nacional Bancaria y de Valores establezca protocolos de coordinación con Banco de México, con el objeto de compartir información de forma oportuna de los hallazgos y observaciones en materia de riesgo tecnológico y seguridad de la información que se identifiquen durante las actividades de supervisión y vigilancia que llevan a cabo ambas entidades.

2. Incidentes de Ciberseguridad en el Sistema Financiero Mexicano en 2018

Antecedentes

La Circular 13/2017 “Disposiciones Generales Aplicables a las Instituciones de Crédito y Otras Empresas que Presten de Manera Profesional el Servicio de Transferencias de Fondos, así como a los Participantes en los Sistemas de Pagos Administrados por el Banco De México y a los demás Interesados en actuar con el Carácter de Participante en Dichos Sistemas” y la Circular 14/2017 “ Reglas del Sistema de Pagos Electrónicos Interbancarios”, ambas

publicadas el 4 de julio de 2017 en el Diario Oficial de la Federación (DOF), establecen las obligaciones de los participantes y del administrador, en este caso BANXICO.

Las principales reglas donde se especifican las obligaciones de los participantes se señalan a continuación:

Circular 13/2017

"13a. Obligaciones de los Participantes. - Cada Participante deberá observar en todo momento los requisitos técnicos, operativos, de seguridad informática y de gestión de riesgos operacionales, de protección de clientes emisores, de interoperabilidad y aquellos relacionados con el uso del Sistema de Pagos en la realización de actividades ilícitas, necesarios para propiciar el buen funcionamiento del Sistema de Pagos".

"15a. Obligaciones de los Participantes del SPEI. - Los Participantes del SPEI, además de lo establecido en la 13a. de las presentes Reglas, deberán cumplir con las obligaciones siguientes:

I. […]

XV. Realizar verificaciones periódicas al cumplimiento de los requisitos en materia de: i) seguridad de la información en su infraestructura tecnológica o infraestructura tecnológica de cualquier tercero que pudiera tener una afectación en la operación o en la infraestructura tecnológica del Participante del SPEI, y ii) atención de incidentes de seguridad de la información en sus canales electrónicos".

Circular 14/2017

"56a. Para ser admitidos como Participantes, los interesados deberán cumplir con los requisitos, términos y condiciones establecidos en las presentes Reglas y el Manual, obtener la autorización del Banco de México de conformidad con lo dispuesto en la Circular 13/2017 y, a su vez, ser admitidos por el Administrador de acuerdo con la 64a. de las presentes Reglas, así como celebrar el Contrato mencionado en la 65a. de estas Reglas".

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

"67a. Cumplimiento permanente de los requisitos para la admisión como Participante. - Los Participantes deberán cumplir en todo momento con los requisitos a que se refieren las 58a., 68a., 70a., 71a. y 72a., de las presentes Reglas".

"74a. Informe y evaluación periódica.- Cada Participante deberá verificar el cumplimiento de los requisitos de seguridad informática, de gestión del riesgo operacional y de protección a

los Clientes Emisores del Participante, de Riesgos Adicionales y de interoperabilidad para operar en el SPEI establecidos en la 58a. de estas Reglas, a través de revisiones que realicen cada dos años de manera alternada el titular del área de auditoría interna del propio Participante y el o los Auditores Externos Independientes el periodo de evaluación inmediato siguiente. Dichas revisiones deberán observar lo dispuesto en las fracciones II y III de la 62a. de las presentes Reglas. En caso de que el Participante no cuente con un área de auditoría interna, deberá de realizar las revisiones antes señaladas en todos los casos por Auditores Externos Independientes".

Las principales reglas donde se especifican las obligaciones como administrador, se señalan a continuación:

Circular 13/2017

"6a. Resolución.- Una vez que la solicitud a que se refiere la 4a. de las presentes Disposiciones reúna los requisitos, a que se refieren la 4a. y 5a. de las presentes Disposiciones, el Banco de México con base en la documentación recibida y una vez que haya llevado a cabo las pruebas, revisiones y visitas que, en su caso, considere necesarias a las instalaciones, equipos, documentos o información del interesado de que se trate, determinará si resulta procedente autorizar a dicho interesado como Participante. En caso de que se conceda dicha autorización, el Banco de México informará su decisión al interesado en actuar como Participante a efecto de que celebre el contrato a que se refiere la Disposición siguiente".

Circular 14/2017

"62a. Evaluación de cumplimiento.- El interesado que presente la solicitud de admisión para actuar como Participante, de conformidad con lo previsto en la 57a. de las presentes Reglas, deberá acreditar en dicha solicitud el cumplimiento de los requisitos de seguridad informática, gestión del riesgo operacional, protección a los Clientes Emisores de los interesados, de gestión de Riesgos Adicionales y de interoperabilidad para operar con el SPEI establecidos en las fracciones I, II, IV, V y VI de la Regla 58a., así como en la 68a. de las presentes Reglas".

"63a. Revisión por parte del Administrador. - Para verificar el cumplimiento de los requisitos para operar con el SPEI establecidos en la 58a. de estas Reglas, el Administrador podrá requerir la documentación, información, ejecución de pruebas e informes adicionales, que estime necesarias. Asimismo, el Administrador podrá realizar visitas en las instalaciones y sistemas del interesado de que se trate, con el propósito de verificar el cumplimiento de los citados requisitos".

"64a. Resolución del Administrador.- Una vez que la solicitud a que se refiere la 57a. de estas Reglas reúna la documentación e información a que se refiere el presente Capítulo, que el Administrador haya realizado las pruebas también referidas en este Capítulo y que, en su caso, haya llevado a cabo la visita mencionada en la Regla anterior, dicho Administrador,

con base en la referida documentación e información, así como con los resultados de las pruebas y visitas, determinará si resulta procedente admitir como Participante en el SPEI al solicitante. El Administrador informará su resolución al solicitante a efecto de que celebren el Contrato a que se refiere la Regla siguiente".

En 2018 diversas entidades del Sector Financiero Mexicano sufrieron incidentes de ciberseguridad relacionados con el SPEI, acorde con la información proporcionada por BANXICO, la cronología de los eventos fue la siguiente:

- El 13 de abril, BANXICO tuvo conocimiento de que un participante (Participante 1) detectó operaciones no reconocidas, las cuales reportó como un fraude interno.

- El 17 de abril, el Participante 1 notificó nuevamente que detectó operaciones no reconocidas.

- El 17 de abril, BANXICO envió un comunicado a todos los participantes de los Sistemas de Pagos, mencionando que se identificaron algunas debilidades relacionadas con la seguridad informática de un participante en el SPEI y recomendó la verificación y en su caso la implementación de mecanismos y/o la validación de las configuraciones para garantizar la autenticidad de las operaciones que serían enviadas al Sistema de Pagos.

- El 18 de abril, BANXICO emitió un segundo comunicado a los participantes de los Sistemas de Pago con perfil de riesgo similar al Participante 1, entre ellos BANJERCITO y BANOBRAS, indicando que el participante afectado contaba con un aplicativo desarrollado por el proveedor LGEC, S.A de C.V., (Proveedor A) y que los vectores de ataque estaban dirigidos a componentes de dicho aplicativo y solicitó contactar al proveedor A para implementar los elementos de seguridad que consideraran pertinentes para mitigar las vulnerabilidades en su infraestructura tecnológica.

- El 24 de abril, BANXICO identificó que BANJERCITO (Participante 2) se encontraba desconectado del SPEI. En respuesta BANJERCITO indicó que había detectado una inconsistencia en su saldo y confirmó que tuvo un incidente de ciberseguridad. BANXICO realizó la desconexión de la infraestructura de BANJERCITO.

- El 24 de abril, BANXICO creó la Dirección de Ciberseguridad.

- El 25 de abril, BANXICO inició la visita de investigación a BANJERCITO de los eventos ocurridos.

- El 26 de abril, BANXICO recibió la notificación de que el participante 3 identificó una inconsistencia en su saldo y confirmó un nuevo incidente de ciberseguridad. Ese mismo día BANXICO instruyó al resto de los participantes con el mismo perfil de riesgo (Proveedor B) y a BANJERCITO, a operar por medio del Cliente de Operación Alterna para el SPEI (COA-SPEI), a partir del día siguiente y hasta nuevo aviso. Asimismo, comunicó a las instituciones de crédito que no se encontraban en posibilidad de utilizar

el COA-SPEI, que debían llevar a cabo las acciones necesarias para poder operar de esta forma a partir del 30 de abril de 2018.

- El 27 de abril, BANJERCITO presentó una denuncia ante la Unidad Especializada en Investigación de Delitos Fiscales y Financieros en la Procuraduría General de la República (PGR) ahora Fiscalía General de la República (FGR).

- El 2 de mayo, otro participante (Participante 4), tuvo afectaciones en sus saldos, BANXICO instruyó a los participantes con un perfil de riesgo similar al Participante 4 a operar a través del mecanismo de contingencia COA-SPEI. Cabe señalar que este participante no tenía el mismo perfil de riesgo que los anteriores.

- El 7 de mayo, BANXICO emitió un comunicado indicando a los participantes con el mismo perfil de riesgo del Participante 4 y que utilizaban el aplicativo desarrollado por el Proveedor B que, a partir del 14 de mayo de 2018 y hasta nuevo aviso, deberían de operar a través del procedimiento de contingencia COA-SPEI.

- El 8 de mayo, otro participante (Participante 5) reportó a BANXICO que identificó operaciones no reconocidas, BANXICO envió un comunicado a los participantes con un perfil de riesgo similar al Participante 5 y que utilizaban el aplicativo desarrollado por otro proveedor (Proveedor C); que partir de ese mismo día debían de operar a través del mecanismo de contingencia COA-SPEI.

De las actividades realizadas por BANXICO ante los incidentes de ciberseguridad ocurridos en el sector financiero, se observó lo siguiente:

- BANXICO solicitó a BANJERCITO la imagen forense obtenida posterior al evento; no obstante, a la fecha de la auditoría (diciembre 2019), no había realizado el análisis de dicha imagen y tampoco había sido destruida.

- BANXICO realizó un análisis de bitácoras de su infraestructura para determinar si había sido comprometida, antes o durante los incidentes; sin embargo, no llevó a cabo un análisis forense, mencionó que no lo consideró necesario debido a que la infraestructura del SPEI no se vio afectada.

- El Plan de Respuesta a Incidentes de Ciberseguridad de BANXICO, no considera escenarios de actuación ante eventos de participantes que puedan afectar al operador y otros participantes.

Cumplimiento de BANJERCITO respecto a la Circular 14/2017

- El 27 de febrero de 2018, de manera previa a los incidentes, en cumplimiento con la regla 74a. Informe y evaluación periódica de las reglas del Sistema de Pagos electrónicos interbancarios emitida en la circular 14/2017, BANJERCITO entregó un dictamen a BANXICO, en el cual identificaron diversos incumplimientos, así como su

plan de trabajo para remediarlos. BANXICO no se pronunció respecto a este dictamen, está información la utilizó en la visita de investigación realizada el 25 de abril de 2018.

Incidente de ciberseguridad en BANJERCITO

Como resultado del comunicado emitido por BANXICO el 18 de abril de 2018, BANJERCITO implementó mecanismos de contingencia manuales en la Dirección de Operaciones Bancarias durante los días previos al incidente y tuvo contacto con el proveedor del aplicativo Enlace Financiero SPEI; el 20 de abril de 2018, el proveedor le proporcionó una serie de recomendaciones, entre ellas, la aplicación de una corrección al aplicativo. Sin embargo, BANJERCITO no demostró haber aplicado dicha corrección, ni que el proveedor hubiera realizado los análisis de vulnerabilidades estático[9] y dinámico[10] al código nuevamente, como se establece en el contrato, el cual indica que cada vez que haya cambios en el aplicativo se tienen que volver a realizar. Dicha cronología se puede apreciar en la Tabla 3.

El 24 de abril de 2018, se presentó el incidente de ciberseguridad, que derivó en una extracción de 3,560.5 miles de pesos por medio de 11 transferencias fraudulentas por medio del SPEI, de las cuales se recuperaron 4, resultando una afectación de 2,574.4 miles de pesos.

BANJERCITO contaba con un seguro con cobertura contra los delitos financieros e informáticos, la aseguradora designó al Proveedor D, para realizar la ejecución de un análisis forense digital con la finalidad de poder identificar las causas del evento y poder cumplir con los requisitos necesarios para el cobro del seguro. De las recomendaciones del Proveedor D, BANJERCITO solicitó al Proveedor E, la ejecución de un análisis estático y dinámico de código.

Una de las hipótesis que concluyen tanto el análisis forense como la revisión estática y dinámica del aplicativo, fue que posiblemente el evento consistió en la explotación de una serie de vulnerabilidades existentes en un componente del aplicativo del Enlace Financiero para el Sistema de Pagos Electrónicos Interbancarios (SPEI) del Banco, el cual fue desarrollado por el proveedor LGEC S.A. de C.V.

9 Revisión con base en el análisis del código fuente del aplicativo.

10 Revisión con base en la emulación del comportamiento real del aplicativo.

Tabla 3. Cronología de eventos relacionados con el Incidente de Seguridad ocurrido en BANJERCITO

Fuente: Desarrollado por la ASF.

De la revisión de las actividades realizadas por BANJERCITO para la identificación, contención y mitigación del incidente de ciberseguridad, así como de las investigaciones posteriores, se observó lo siguiente:

- Al momento del incidente, BANJERCITO no contaba con políticas, procedimientos ni protocolos de emergencia para identificar, notificar, contener, atender, solucionar y mitigar incidentes de seguridad.

- Incumplía con algunos requisitos de seguridad informática solicitados en la Circular 14/2017.

- Carece de la documentación relacionada con las actividades de protección y custodia de los componentes de infraestructura comprometidos.

- El Órgano Interno de Control y la Dirección de Auditoría Interna no llevaron a cabo actividades de análisis o investigación respecto del incidente.

Del contrato Número 012/2018 celebrado con LGEC, S.A. de C.V., se identificó lo siguiente:

- La vigencia del contrato fue del 01 de enero al 31 de diciembre de 2018, con el objeto de proveer servicios de soporte y mantenimiento a los sistemas “Enlace Financiero SPEI" y "Enlace Financiero SPID", se realizó el pago por 1,294.7 miles de pesos el 27 de marzo de 2018 por medio de una sola exhibición y 35.1 miles de pesos por concepto de consultoría el 29 de enero de 2019.

- El proveedor no hizo la entrega de los análisis de vulnerabilidades estático y dinámico correspondiente a la última versión que se liberó del Enlace Financiero SPID.

- El reporte de vulnerabilidades realizado por el proveedor el 11 de enero de 2018, que se proporcionó con relación a la ejecución de análisis estático y dinámico para el

aplicativo Enlace Financiero SPEI no consideró todos los componentes relacionados a dicho aplicativo.

- BANJERCITO no gestionó con el proveedor la aplicación de la garantía de cumplimiento conforme a la cláusula OCTAVA del contrato, tras el evento de seguridad informática y de los defectos que presentó el aplicativo de Enlace Financiero SPEI.

- Dado que BANJERCITO ya no utilizó el aplicativo después del incidente de seguridad ni los servicios de soporte y mantenimiento, debió haber realizado la rescisión administrativa del contrato por los incumplimientos mencionados, situación que no sucedió y éste continúo vigente por 8 meses.

- En el contrato, no se establecieron cláusulas de penalización o deductivas al proveedor ante defectos, vicios ocultos, conforme a lo indicado en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Pago del Deducible

- Una vez que BANJERCITO contó con el visto bueno por parte de la aseguradora para la recuperación del daño mediante el rubro de "Otros riesgos no financieros" por la totalidad de los daños dictaminados tras el incidente de ciberseguridad, realizó el pago del deducible por 1,500.0 miles de pesos como se establece en la cláusula 3.8 (Cobertura de delito Informático) del anexo técnico del contrato de la póliza.

Por lo anterior, se identifica que BANJERCITO incumplió con la regla 67a. Cumplimiento Permanente de los Requisitos para la Admisión como Participante de la Circular 14/2017**,** aún y cuando ya contemplaba un plan de trabajo para el cumplimiento, no se realizaron actividades oportunas para solventar los incumplimientos críticos; BANXICO no se pronunció respecto al informe que le envió BANJERCITO el 28 de febrero del 2018 en cumplimiento con la regla 74a. de la misma Circular, está información se utilizó en la visita de investigación realizada el 25 de abril de 2018.

2018-0-98001-21-0054-01-005 **Recomendación**

Para que el Banco de México considere en su plan de respuesta a incidentes de seguridad, escenarios posibles de actuación ante eventos de participantes que puedan afectar al operador y a otros participantes.

2018-9-06G1H-21-0054-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que el Órgano Interno de Control en Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C., o su equivalente realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las

irregularidades de los servidores públicos que, en su gestión, no definieron, documentaron, formalizaron ni publicaron, mecanismos, protocolos, políticas o procedimientos respecto a la identificación, notificación, contención, atención, resolución y mitigación de incidentes de seguridad en sistemas críticos como el Sistema de Pagos Electrónicos Interbancarios(SPEI). No documentaron las actividades del proveedor durante los procesos de contención y mitigación del incidente de seguridad del cual fue objeto el Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. (BANJERCITO) el 24 de abril de 2018, no llevaron a cabo una cadena de custodia que asegurara la integridad de todos los componentes involucrados en el incidente de seguridad referido, toda vez que realizaron actividades de borrado de procesos y reinicio de equipos que comprometieron los resultados del análisis forense y revisión de código estático y dinámico ejecutados posteriormente, no consideraron la custodia de equipos con acceso a la red del banco y tampoco hicieron efectiva la garantía de cumplimiento hacia el proveedor en función de la calidad del servicio, al no realizar la terminación anticipada del contrato número 012/2018, en incumplimiento de las Declaraciones I incisos E, F, y G, Octava, Décima Primera y Décima Quinta del contrato 012/2018 celebrado con el proveedor LGEC S.A. de C.V, Fracción III Subdirección de Tecnología y Seguridad Informática, Objetivo 1, Función1; Dirección de Informática, Objetivo 2 función 3; Gerencia de Computo y Seguridad Función 13, Subdirección de Servicios de Informática Objetivo 1, función 2; Gerencia de Centro de Cómputo y Seguridad Objetivo 1,: Dirección de Operaciones Bancarias, Objetivo 2, Gerencia de Operaciones de Tesorería Objetivo 1; Dirección de Auditoría Interna Funciones 1 y 2; Órgano Interno de Control, Titular del Órgano Interno de Control, Función 1; del Manual General de Organización del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. del 30 de septiembre de 2016: Fracción III. Subdirección de Tecnología y Seguridad Informática Función 7 y 12: Dirección de Informática Función 4 del Manual General de Organización del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. del 30 de abril de 2018 y del 30 de noviembre.

2018-9-06G1H-21-0054-08-002 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que el Órgano Interno de Control en Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C., o su equivalente realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de los servidores públicos que, en su gestión, no aseguraron el cumplimiento del Contrato de Servicio Número 012/2018 respecto de las declaraciones I incisos E, F, y G, cláusula Primera numerales 4.1 y 4.2, Octava y Décimo Primera celebrado con el proveedor LGEC S.A. de C.V., debido a que no revisaron que los entregables de las pruebas estáticas y dinámicas contemplaran todos los componentes relacionados con el aplicativo Sistemas de Pagos Electrónicos Interbancarios (SPEI), para asegurar que no tuviera las vulnerabilidades detectadas en el análisis forense, las cuales pudieron estar relacionadas con que se materializara el incidente de ciberseguridad en el aplicativo Enlace Financiero desarrollado por el LGEC S.A de C.V. Adicionalmente no se entregaron las pruebas estáticas y dinámicas del aplicativo Sistemas de Pagos Electrónicos en Dólares (SPID), en incumplimiento Declaraciones I incisos E, F, y G, Cláusulas Primera numerales 4.1 y 4.2, Décimo Primera del

contrato 012/2018 celebrado con el proveedor LGEC S.A. de C.V, requisito 1.1 fracción ii, Requisito 11 incisos a ,b, c, y d del Apéndice M del Manual de Operación del SPEI versión 5.3.3 del 22 de junio de 2017, Requisito 11 incisos a y b del Anexo C del Manual de Operación del SPID versión 3.1 del 30 de diciembre de 2016, Capitulo III, regla 12a de la circular 13/2017 publicada en el D.O.F. el 04 de julio de 2017, Capitulo III regla 15a, fracción X de la circular 10/2018 de fecha 27 de julio de 2018, Capitulo IV, sección I, regla 56a, fracción I, apartado A, incisos a, a bis, b numeral 3; en el artículo 86, inciso b), numeral 1 y 164 fracción V de las Disposiciones de carácter general aplicables a las instituciones de crédito del 27 de diciembre de 2017, Fracción III Subdirección de Tecnología y Seguridad Informática, Objetivo 1, Función1; Dirección de Informática, Objetivo 2 función 3; Gerencia de Computo y Seguridad Función 13, Subdirección de Servicios de Informática Objetivo 1, función 2; Gerencia de Centro de Cómputo y Seguridad Objetivo 1,: Dirección de Operaciones Bancarias, Objetivo 2, Gerencia de Operaciones de Tesorería Objetivo 1; Dirección de Auditoría Interna Funciones 1 y 2; Órgano Interno de Control, Titular del Órgano Interno de Control, Función 1; del Manual General de Organización del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. del 30 de septiembre de 2016: Fracción III. Subdirección de Tecnología y Seguridad Informática Función 7 y 12: Dirección de Informática Función 4 del Manual General de Organización del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. del 30 de abril de 2018 y del 30 de noviembre.

2018-2-06G1H-21-0054-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 1,500,000.00 pesos (un millón quinientos mil pesos 00/100 M.N.), por concepto del pago del deducible indicado en la Sección V. Deducible del Anexo Técnico de la Póliza que celebró BANJERCITO con Aseguradora Inbursa S.A. Grupo Financiero Inbursa, a raíz del incidente de ciberseguridad que se suscitó el 24 de abril de 2018, ya que se tiene constancia de las vulnerabilidades con las que contaba el aplicativo Enlace Financiero SPEI adquirido en el contrato de servicio número 012/2018 celebrado con LGEC S.A. de C.V., ante lo cual no se gestionó con el proveedor la rescisión del contrato ni que éste respondiera por la calidad de los servicios o en su defecto por los gastos derivados, los cuales fueron asumidos por la institución, en incumplimiento Artículo 66 fracción I, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, última reforma publicada el 30 de marzo de 2016 en el Diario Oficial de la Federación (D.O.F). Declaraciones I incisos E, F, y G, Octava, Décima Primera del contrato 012/2018 celebrado con el proveedor LGEC S.A. de C.V, requisito 1.1 fracción ii, Requisito 11 incisos a ,b, c, y d del Apéndice M del Manual de Operación del SPEI versión 5.3.3 del 22 de junio de 2017, Requisito 11 incisos a y b del Anexo C del Manual de Operación del SPID versión 3.1 del 30 de diciembre de 2016, Capitulo III, regla 12a de la circular 13/2017 publicada en el D.O.F. el 04 de julio de 2017, Capitulo III regla 15a, fracción X de la circular 10/2018 de fecha 27 de julio de 2018, Capitulo IV, sección I, regla 56a, fracción I, apartado A, incisos a, a bis, b numeral 3; en el artículo 86, inciso b), numeral 1 y 164 fracción V de las Disposiciones de carácter general aplicables a las instituciones de crédito del 27 de diciembre de 2017, Fracción III Subdirección de Tecnología y Seguridad Informática, Objetivo 1, Función1; Dirección de Informática, Objetivo 2 función 3; Gerencia de Computo y Seguridad Función 13, Subdirección de Servicios de Informática

Objetivo 1, función 2; Gerencia de Centro de Cómputo y Seguridad Objetivo 1,: Dirección de Operaciones Bancarias, Objetivo 2, Gerencia de Operaciones de Tesorería Objetivo 1; Dirección de Auditoría Interna Funciones 1 y 2; Órgano Interno de Control, Titular del Órgano Interno de Control, Función 1; del Manual General de Organización del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. del 30 de septiembre de 2016: Fracción III. Subdirección de Tecnología y Seguridad Informática Función 7 y 12: Dirección de Informática Función 4 del Manual General de Organización del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. del 30 de abril de 2018 y del 30 de noviembre.

Causa Raíz Probable de la Irregularidad

Se detectaron incumplimientos y deficiencias en el aplicativo Enlace Financiero SPEI, no se gestionó la recisión del contrato ni que el proveedor respondiera por la calidad de los servicios o en su defecto por los gastos derivados, los cuales fueron asumidos por la institución.

3. Evaluación del nivel de madurez de ciberseguridad en los sistemas de pago (Banca de Desarrollo y BANXICO)

Metodología de evaluación

La Auditoría Superior de la Federación desarrolló un modelo para evaluar el nivel de madurez de la ciberseguridad en la administración y operación de los Sistemas de Pago SPEI y SPID. Para su elaboración, se tomó como base el Marco de Referencia de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology), el Apéndice M: Requisitos de Seguridad Informática y de Gestión del Riesgo Operacional del Manual del SPEI (A. En la Infraestructura Tecnológica y B. En los Canales Electrónicos), Apéndice E. Seguridad Informática y Gestión de Riesgo Operacional del Manual SPID versión 1.0 del BANXICO, así como la Resolución que modifica las Disposiciones de Carácter General aplicables a las instituciones de crédito emitida por la Comisión Nacional Bancaria y de Valores.

Como resultado del modelo, se elaboraron 17 cédulas de evaluación que comprenden las 5 funciones y 22 categorías relacionadas con la ciberseguridad que se desarrollan a continuación:

Funciones

1.- Identificar

Se refiere a la comprensión del contexto de la organización, los activos que soportan los procesos críticos de las operaciones y los riesgos asociados. Esta comprensión permite definir los recursos y las inversiones de acuerdo con la estrategia de gestión de riesgos y sus objetivos. Las categorías dentro de esta función son:

Tabla 4. Categorías de la función identificar

ID.AM - Gestión de Activos
ID.BE - Entorno Empresarial
ID. GV - Gobernanza
ID.RA - Evaluación de Riesgos
ID.RM - Estrategia de Gestión de Riesgos
ID.SC - Gestión del Riesgo en la Cadena de Suministro

Fuente: Marco de Referencia de Ciberseguridad NIST.

2.- Proteger

Es una función vinculada a la aplicación de medidas para garantizar la entrega de los servicios críticos. Las categorías dentro de esta función son:

Tabla 5. Categorías de la función proteger

PR.AC - Gestión de Identidad y Control de Acceso
PR.AT - Concienciación y Capacitación
PR.DS - Seguridad de Datos
PR. IP - Procesos y Procedimientos de Protección de la Información
PR.MA - Mantenimiento
PR.PT - Tecnología de Protección

Fuente: Marco de Referencia de Ciberseguridad NIST

3.- Detectar

Es la definición y ejecución de actividades apropiadas para la identificación de los incidentes de ciberseguridad. Las categorías que la componen son:

Tabla 6. Categorías de la función detectar

DE.AE - Anomalías y Eventos
DE.CM - Monitoreo continuo de la seguridad
DE. DP - Procesos de Detección

Fuente: Marco de Referencia de Ciberseguridad NIST

4.- Responder

Se refiere a la definición y ejecución de actividades apropiadas para tomar medidas en caso de detección de un evento de ciberseguridad. El objetivo es reducir el impacto de un potencial incidente de ciberseguridad. Las categorías dentro de esta función son:

Tabla 7. Categorías de la función responder

RS.RP - Planificación de Respuesta
RS.CO - Comunicaciones
RS.AN - Análisis
RS.MI - Mitigación
RS.IM - Mejoras

Fuente: Marco de Referencia de Ciberseguridad NIST

5.- Recuperar

Está vinculada a la definición y ejecución de las actividades dirigidas a la gestión de los planes de resiliencia para restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética. El objetivo es asegurar la resiliencia de los sistemas e instalaciones y, en caso de incidentes, apoyar la recuperación oportuna de las operaciones. Las categorías dentro de esta función son:

Tabla 8. Categorías de la función recuperar

RC.RP - Planificación de recuperación
RC.CO - Comunicaciones

Fuente: Marco de Referencia de Ciberseguridad NIST

Modelo de Madurez

Los niveles de madurez utilizados por la ASF en esta auditoría se definieron con base en el modelo CMMI (Capability Maturity Model Integration) y la Herramienta de evaluación de Ciberseguridad del Federal Financial Institutions Examination Council (FFIEC) de los Estados Unidos de América, de acuerdo con los niveles siguientes:

Tabla 9. Modelo de madurez

Descripción
Incompleto. Se carece de actividades o estas no se llevan a cabo de forma completa por lo que no se cubren los objetivos del proceso.
Inicial. Las actividades se realizan, pero no se logra el cumplimiento de objetivos del proceso.
Administrado. El proceso logra sus propósitos en una forma organizada. Los procesos están bien definidos.
Definido. El proceso logra sus propósitos en una forma organizada y existen estándares y mejores prácticas en toda la organización.
Cuantitativo. El proceso logra su propósito, está bien definido y su desempeño es medido (cuantitativamente).
Optimizado. El proceso logra su propósito, está bien definido, el desempeño es medido y se lleva a cabo la mejora continua.

Fuente: Modelo de madurez desarrollado por la ASF con base en CMMI FFIEC.

De acuerdo al CMMI para alcanzar el siguiente nivel de madurez, es necesario cumplir al menos con el 75.0% del nivel anterior, la Herramienta de Evaluación de Ciberseguridad del FFIEC propone 5 niveles de madurez, el primero considera que se deben cumplir todos los requerimientos legales, así como las guías recomendadas por las entidades de supervisión. Los requerimientos solicitados por el manual del SPEI emitidos por el BANXICO se encuentran incluidos en los niveles de madurez 1 y 2**.**

Agrupación de subcategorías de ciberseguridad del Marco de Referencia de Ciberseguridad NIST

Para el modelo desarrollado por la ASF, se analizaron las 108 subcategorías que contiene el Marco de Referencia de Ciberseguridad NIST con base en los criterios de madurez del CMMI, como resultado se obtuvieron 65 subcategorías que incluyen a los 43 restantes en alguno de sus niveles de madurez.

Resultados de la evaluación

Se llevó a cabo una primera evaluación del nivel de madurez de las 65 subcategorías de ciberseguridad en los Sistemas de Pago a 7 entidades de las 8 consideradas en esta auditoría, la FND decidió dejar de ser participante de los Sistemas de Pago en mayo de 2019 al no poder cumplir con los requisitos solicitados por BANXICO.

De esta evaluación inicial se observó que dos entidades presentaron niveles de madurez en ciberseguridad para los Sistemas de Pago muy bajos y las cinco restantes niveles bajos, de acuerdo con la metodología aplicada por la ASF y la información entregada inicialmente por las entidades auditadas. Es importante indicar que estos bajos niveles de madurez implican incumplimientos de algunos de los controles de seguridad de la información requeridos por la normativa de los Sistemas de Pagos.

Se entregó el resultado del análisis a cada una de las entidades evaluadas mediante un reporte que contiene el detalle de los hallazgos y recomendaciones específicas para que

iniciaran las acciones necesarias, o en su caso presentaran evidencia adicional para incrementar sus niveles de madurez en cada una de las 65 categorías revisadas.

Durante el desarrollo de esta auditoría, la ASF estableció contacto en diversas ocasiones con las entidades auditadas para revisar los avances de las acciones para cada una de las subcategorías evaluadas, con base en esto, las entidades aportaron nueva evidencia, lo que motivó una segunda evaluación por parte de la ASF, de la cual se obtuvieron los resultados siguientes:

Tabla 10. Resultado de la segunda evaluación de madurez de ciberseguridad.

Funciones (Identificar, Proteger, Detectar, Responder)

Función	Categoría	Subcategoría	Ent 1	Ent 2	Ent 3	Ent 4	Ent 5	Ent 6	Ent 7
IDENTIFICAR	ID.AM Gestión de Activos	1							
		2							
		3							
		4							
		5							
	ID.BE Entorno Empresarial	6							
		7							
		8							
	ID. GV Gobernanza	9							
		10							
		11							
	ID.RA Evaluación de Riesgos	12							
		13							
		14							
		15							
		16							
PROTEGER	PR AC Gestión de Identidad	17							
		18							
		19		N/A					
		20							
		21							
		22							
	PR.AT Concienciación y Capacitación	23							
		24							
		25							
		26							
	PR DS Seguridad de los Datos	27							
		28							

Función	Categoría	Subcategoría	Ent 1	Ent 2	Ent 3	Ent 4	Ent 5	Ent 6	Ent 7
		29							
		30							
		31							
		32							
		33							
	PR IP Procesos y Procedimientos de proyección de la información	34							
		35							
		36							
		37							
		38							
		39							
		40							
		41							
		42							
		43							
	PR.MA Mantenimiento	44							
	PR.PT Tecnología de Protección	45							
		46							
		47							
DETECTAR	DE.AE Anomalías y eventos	48							
		49							
	DE.CM Monitoreo Continuo de la Seguridad	50							
		51							
		52							
		53							
		54							
		55							
	DE. DP Procesos de Detección	56							
		57							
RESPONDER	RS.RP Planificación de la Respuesta	58							
	RS.CO Comunicaciones	59							
		60							
		61							
	RS.AN Análisis	62							
		63							
Promedio									

Fuente: Elaborado por la ASF.

De esta evaluación, se observó que una entidad continuó presentando un nivel de madurez muy bajo; 3 entidades, bajo; 1 entidad, medio bajo y 2 entidades, niveles medios de madurez.

La evaluación de la función recuperar se llevó a cabo en tres entidades que habían ejecutado procesos de recuperación de incidentes de ciberseguridad, obteniendo el resultado siguiente:

Tabla 11. Resultado de evaluación de madurez de ciberseguridad inicial (Función Recuperar)

Función	Categoría	Subcategoría	Ent 1	Ent 2	Ent 3
RECUPERAR	RC.CO Comunicaciones	64			
		65			

Fuente: Elaborado por la ASF.

Se agruparon de mayor a menor riesgo las 63 subcategorías, identificando que el 23.8% tienen un nivel de riesgo muy alto y alto, como se muestra a continuación:

- 6.3% con un nivel de riesgo muy alto
- 17.5% con un nivel de riesgo alto
- 20.6% con un nivel de riesgo medio -alto
- 27.0% con un nivel de riesgo medio
- 14.3% con un nivel de riesgo medio – bajo
- 14.3% con un nivel de riesgo bajo

El resultado del análisis de esta segunda evaluación también fue entregado a las entidades auditadas junto con recomendaciones específicas, para que en cada una de las subcategorías que aplique, se logre alcanzar al menos un nivel de madurez 2.

Análisis del resultado de las funciones del modelo de madurez de ciberseguridad

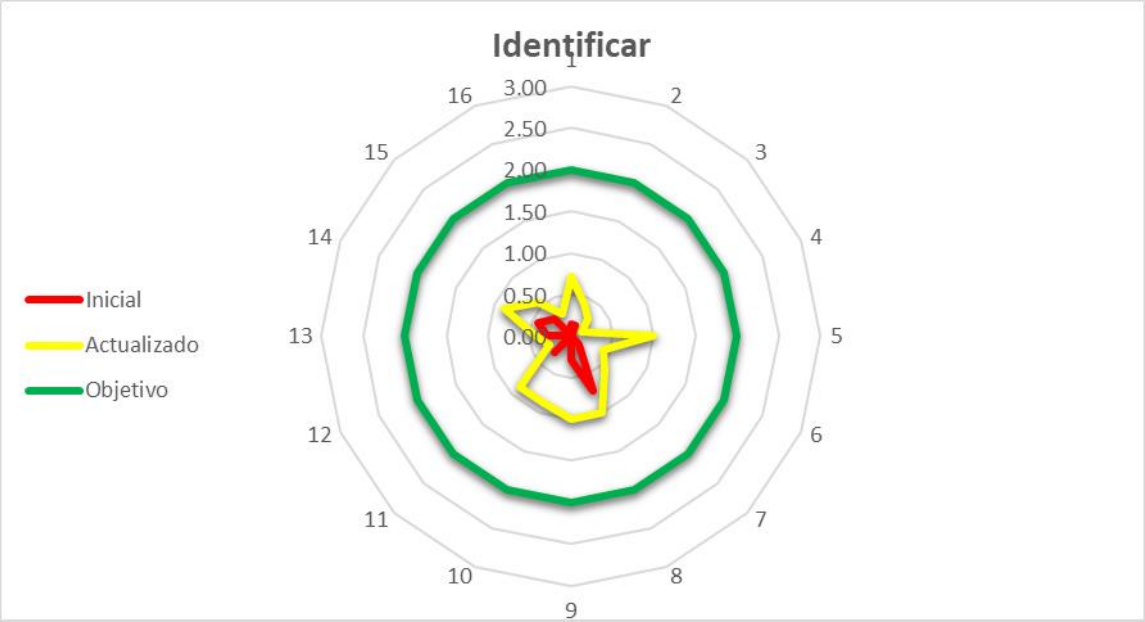
Se llevó a cabo un análisis de la madurez de cada una de las funciones que componen el modelo de evaluación de ciberseguridad correspondientes a: Identificar, Proteger, Detectar y Responder; en el caso de la función Recuperar, no se llevó a cabo el análisis puesto que sólo se contó con información de 3 de las 7 entidades que formaron parte de la revisión.

Las gráficas siguientes representan los niveles de madurez promedio de todas las entidades evaluadas con los resultados: iniciales (primera evaluación), actualizados (de la segunda

evaluación) y el objetivo propuesto, de cada una de las categorías que componen a las funciones Identificar, Proteger, Detectar y Responder.

Identificar

Gráfica 1. Grafica radial, niveles de madurez inicial, actualizado y objetivo de la función identificar.

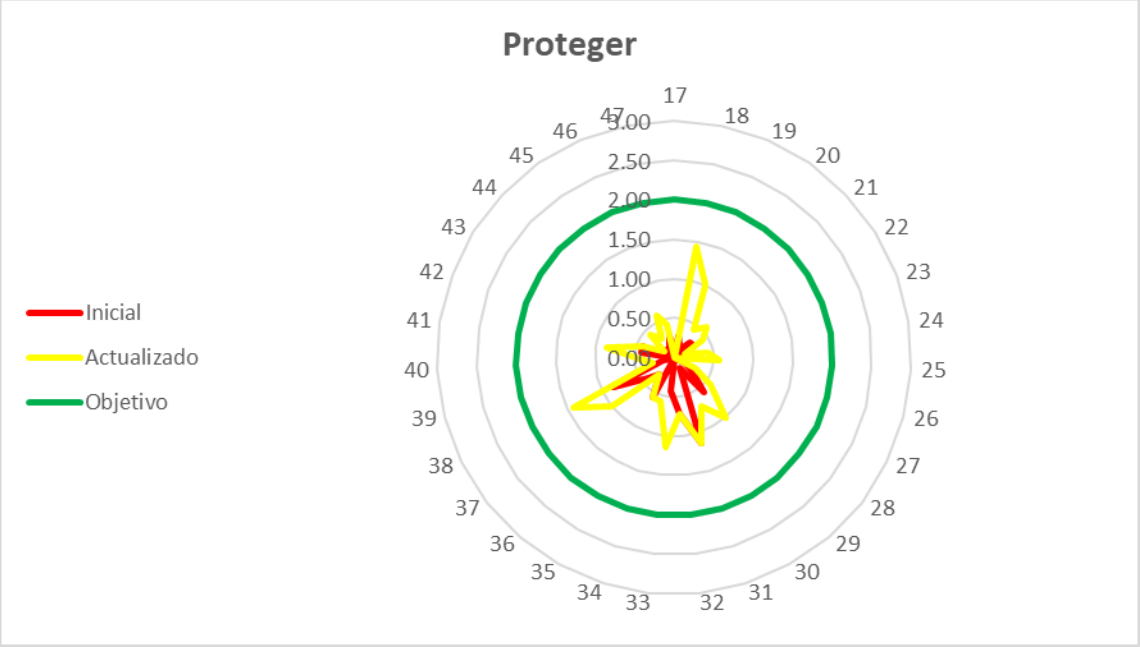


Fuente: Elaborado por la ASF.

La función Identificar presentó un promedio inicial de madurez de 0.17 en la primera revisión, en la segunda evaluación se ubicó en 0.61, lo que indica que se debe continuar con la implementación de acciones que permitan definir los recursos y las inversiones de acuerdo con la estrategia de gestión de riesgos y sus objetivos.

Proteger

Gráfica 2. Gráfica radial, niveles de madurez inicial, actualizado y objetivo de la función proteger.

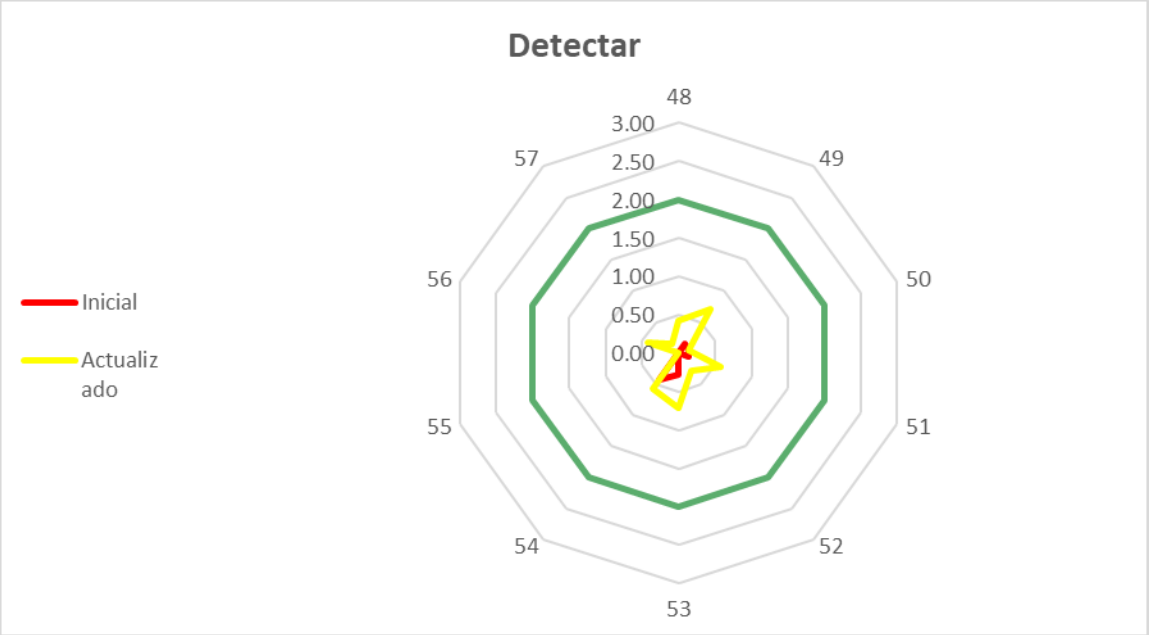


Fuente: Elaborado por la ASF.

La función Proteger presentó un promedio inicial de madurez de 0.28; en la segunda evaluación, se actualizó a 0.59, lo que indica que se tienen que incrementar las medidas para proteger los procesos y los activos de la organización.

Detectar

Gráfica 3. Gráfica radial, niveles de madurez inicial, actualizado y objetivo de la función detectar.

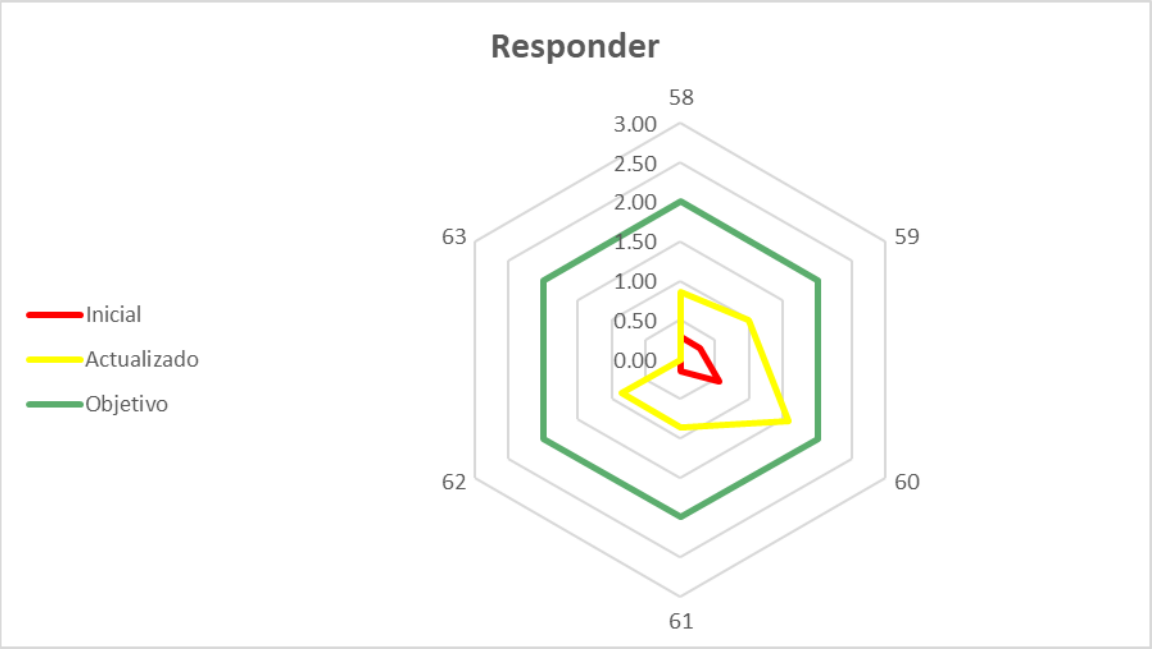


Fuente: Elaborado por la ASF.

La función Detectar presentó un promedio inicial de madurez de 0.11; en la segunda evaluación, se actualizó a 0.40, por lo que se tienen que tomar acciones adicionales para tener una adecuada definición y ejecución de actividades dirigidas a la identificación temprana de los incidentes de seguridad.

Responder

Gráfica 4. Gráfica radial, niveles de madurez inicial, actualizado y objetivo de la función responder



Fuente: Elaborado por la ASF.

La función responder presentó un promedio inicial de madurez de 0.21; en la segunda evaluación, se actualizó a 0.86, que es la función que mayor nivel promedio de madurez obtuvo; no obstante, se tiene que continuar con la definición y ejecución de actividades apropiadas para tomar medidas en caso de detección de un evento de seguridad con el objetivo de reducir el impacto de un potencial incidente de ciberseguridad.

2018-0-98001-21-0054-01-006 **Recomendación**

Para que el Banco de México implemente las acciones necesarias para incrementar el nivel de madurez a un mínimo de 2, de cada una de las 65 subcategorías del modelo de evaluación de ciberseguridad que lo requieran.

2018-2-06G0N-21-0054-01-001 **Recomendación**

Para que el Banco Nacional de Comercio Exterior, S.N.C., implemente las acciones necesarias para incrementar el nivel de madurez a un mínimo de 2, de cada una de las 65 subcategorías del modelo de evaluación de ciberseguridad que lo requieran.

2018-2-06G1C-21-0054-01-001 **Recomendación**

Para que el Banco Nacional de Obras y Servicios Públicos, S.N.C., implemente las acciones necesarias para incrementar el nivel de madurez a un mínimo de 2, de cada una de las 65 subcategorías del modelo de evaluación de ciberseguridad que lo requieran.

2018-2-06G1H-21-0054-01-001 **Recomendación**

Para que el Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C., implemente las acciones necesarias para incrementar el nivel de madurez a un mínimo de 2, de cada una de las 65 subcategorías del modelo de evaluación de ciberseguridad que lo requieran.

2018-2-06HIU-21-0054-01-001 **Recomendación**

Para que Nacional Financiera, S.N.C., implemente las acciones necesarias para incrementar el nivel de madurez a un mínimo de 2, de cada una de las 65 subcategorías del modelo de evaluación de ciberseguridad que lo requieran.

2018-2-06HJO-21-0054-01-001 **Recomendación**

Para que el Banco del Bienestar, S.N.C., implemente las acciones necesarias para incrementar el nivel de madurez a un mínimo de 2, de cada una de las 65 subcategorías del modelo de evaluación de ciberseguridad que lo requieran.

2018-2-06HKI-21-0054-01-001 **Recomendación**

Para que la Sociedad Hipotecaria Federal, S.N.C., implemente las acciones necesarias para incrementar el nivel de madurez a un mínimo de 2, de cada una de las 65 subcategorías del modelo de evaluación de ciberseguridad que lo requieran.

Montos por Aclarar

Se determinaron 1,500,000.00 pesos pendientes por aclarar.

Buen Gobierno

Impacto de lo observado por la ASF para buen gobierno: Liderazgo y dirección y Controles internos.

Resumen de Observaciones y Acciones

Se determinaron 3 resultados, de los cuales, 3 generaron:

13 Recomendaciones, 2 Promociones de Responsabilidad Administrativa Sancionatoria y 1 Pliego de Observaciones.

Dictamen

El presente dictamen se emite el 27 de enero de 2020, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la Comisión Nacional Bancaria y de Valores (CNBV) y el BANXICO (BANXICO) como organismos reguladores, así como de los 7 participantes de la Banca de Desarrollo: Banco Nacional de Comercio exterior, S.N.C. (BANCOMEXT), Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. (BANJÉRCITO), Banco Nacional Obras y Servicios Públicos, S.N.C. (BANOBRAS), Financiera Nacional de Desarrollo Agropecuario, Rural, Forestal y Pesquero (FND), la Nacional Financiera S.N.C. (NAFIN), Banco del Bienestar S.N.C., antes BANSEFI y Sociedad Hipotecaria Federal S.N.C. (SHF) cuyo objetivo consistió en llevar a cabo la revisión de la ciberseguridad de la banca electrónica y Sistemas de Pago de las entidades del gobierno mexicano, verificando el marco normativo y regulatorio, la eficacia y eficiencia de las entidades a cargo de la regulación, supervisión y vigilancia del cumplimiento de los mecanismos de ciberseguridad, así como la aplicación de controles, en recursos humanos, procesos y tecnologías en las entidades gubernamentales que utilizan la banca electrónica y los Sistemas de Pago, se concluye que, en términos generales, cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los resultados descritos en el presente informe de auditoría que arrojaron deficiencias y debilidades que son importantes, entre las que destacan las siguientes:

- Durante 2018 y 2019, la Banca de Desarrollo y la Tesorería de la Federación (operada por BANXICO) a través del SPEI realizaron transacciones por un importe de 52.1 billones de pesos.

- **Regulación en seguridad informática.** El SPEI inició operación en 2004 y, en julio de 2017, se incluyeron, por primera vez en la regulación de los participantes, los controles de seguridad informática y gestión de riesgo operacional, es importante señalar que entre 2008 y 2017 ocurrieron al menos una docena de ataques cibernéticos relacionados con los Sistemas de Pagos e infraestructura tecnológica de bancos centrales en diferentes partes del mundo.

- **Segregación de Funciones.** La encuesta de 2018 del Grupo de Banco Mundial (World Bank Group) sobre el alcance de la vigilancia en los Sistemas de Pagos, menciona que la separación organizacional entre las funciones de revisión y operación de los bancos centrales ayuda a asegurar la aplicación consistente de las políticas y los estándares. Esta encuesta mostró que más del 85 por ciento de los países encuestados, tienen sus funciones de vigilancia segregadas (ya sea en otra organización o por la independencia en la línea de reporte) de las tareas operacionales de los Sistemas de Pagos.

En BANXICO, la Dirección General de Sistemas de Pago e Infraestructuras de Mercados (DGSPIM) realiza las funciones de operador de los Sistemas de Pagos sobre infraestructura administrada por la DGTI, sin que exista normativa interna, emitida y revisada por un tercero (ajeno a la DGSPIM y la DGTI), lo que no permite una segregación apropiada de funciones.

- **Supervisión y Vigilancia.** Se identificó que, bajo la metodología de supervisión y vigilancia de la DGSPIM, durante 2018 y 2019, ninguna entidad de la Banca de Desarrollo fue sujeta a una visita de inspección por parte de esta dirección, para revisar el cumplimiento de los requisitos de seguridad informática y gestión de riesgo operacional en los Sistemas de Pagos.

BANXICO no se pronunció con los participantes de la Banca de Desarrollo, respecto de la información que proporcionaron sobre el cumplimiento de los requisitos de seguridad informática y gestión de riesgo operacional del apéndice M del Manual de operación del SPEI.

- **Coordinación entre reguladores**. Se identificó que no son compartidos los hallazgos en materia de riesgo tecnológico y seguridad de la información entre la CNBV y BANXICO.

- **Incidente de seguridad en BANJERCITO**. El 24 de abril de 2018, se presentó el incidente de seguridad informática, que derivó en una extracción de 3,560.5 miles de pesos, provenientes de 11 transferencias fraudulentas a través del sistema SPEI; de las 11 transacciones se pudieron realizar 3 recuperaciones totales y una parcial por lo que el nuevo monto extraído fue de 2,574.4 miles de pesos:

  - Al momento del incidente, BANJERCITO no contaba con políticas, procedimientos, ni protocolos de emergencia para identificar, notificar, contener, atender, solucionar y mitigar incidentes de ciberseguridad.

  - Incumplía con algunos requisitos de seguridad informática solicitados en la Circular 14/2017.

  - No contó con documentación relacionada con las actividades de protección y custodia de los componentes de infraestructura comprometidos.

  - El Órgano Interno de Control y la Dirección de Auditoría Interna no llevaron a cabo actividades de análisis o investigación respecto del incidente.

- **Niveles de madurez en ciberseguridad.** En la revisión de la madurez de ciberseguridad, se detectó inicialmente que 2 entidades presentaron niveles muy bajos y las 5 restantes niveles bajos, de acuerdo con la metodología aplicada por la ASF y la información entregada inicialmente por las entidades auditadas.

Se entregó el resultado del análisis a cada una de las entidades evaluadas por medio de un reporte que contiene el detalle de los hallazgos y recomendaciones específicas para que iniciaran las acciones necesarias o en su caso presentaran evidencia adicional para incrementar sus niveles de madurez en cada una de las 65 categorías revisadas.

Durante el proceso de auditoría esta entidad de Fiscalización Superior estableció contacto en diversas ocasiones con las entidades auditadas para revisar los avances de las acciones

para cada una de las subcategorías evaluadas, con base en ello las entidades aportaron nueva evidencia, lo que motivó una segunda evaluación por parte de la ASF.

De esta segunda evaluación, se observó que una entidad continuó presentando un nivel de madurez muy bajo, tres entidades bajo, una entidad medio bajo y dos entidades niveles medios de madurez.

Esta revisión contribuye a la mejora de la ciberseguridad en los Sistemas de Pagos en temas regulatorios, de supervisión, vigilancia y condiciones de operación de los participantes y del administrador de estos sistemas.

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
C. Valderrama Roberto Hernández Rojas	Alejandro Carlos Villanueva Zamacona

Comentarios de la Entidad Fiscalizada

Es importante señalar que la documentación proporcionada por la entidad fiscalizada para aclarar o justificar los resultados y las observaciones presentadas en las reuniones fue analizada con el fin de determinar la procedencia de eliminar, rectificar o ratificar los resultados y las observaciones preliminares determinados por la Auditoría Superior de la Federación y que se presentó a este órgano técnico de fiscalización para efectos de la elaboración definitiva del Informe General Ejecutivo del Resultado de la Fiscalización Superior de la Cuenta Pública.

Apéndices

Procedimientos de Auditoría Aplicados

1. Análisis de las funciones de Acuerdo a su Normativa.

   Verificar el cumplimiento de las atribuciones con las que cuenta la Comisión Nacional Bancaria y de Valores (CNBV) en materia de control, revisión, evaluación y vigilancia conforme a lo establecido en las Disposiciones de carácter general aplicables a las instituciones de crédito; confirmar que la CNVB realiza el seguimiento a los incidentes ocurridos en cuestión de temas de Ciberseguridad, así como con las normas

incumplidas por los participantes y el cumplimiento de lo indicado en las nuevas disposiciones.

Comprobar que las disposiciones emitidas por BANXICO incluyan controles de ciberseguridad que contribuyan con el buen funcionamiento de los Sistemas de Pago, así como un monitoreo continuo de los participantes. Asimismo, que como ente regulador cuente con una metodología basada en el control, revisión, evaluación y vigilancia de la Banca de Desarrollo.

Comprobar que BANXICO cuenta y cumple con las regulaciones y normativa interna dispuestas para el Sistema de Pagos Electrónicos Interbancarios (SPEI) y el Sistema de Pagos Interbancarios en Dólares (SPID), en sus funciones de regulador, supervisor, operador y participante en los Sistemas de Pagos.

Comprobar que los participantes de la Banca de Desarrollo cumplen con las regulaciones dispuestas para el SPEI y SPID.

2. Análisis del marco normativo y su cumplimiento

   Comprobar que los entes reguladores BANXICO y la CNBV hayan realizado revisiones en cuanto a controles de ciberseguridad. Verificar el debido cumplimiento a las disposiciones que fortalecen los controles de Ciberseguridad relacionados a los Sistemas de Pagos.

   Corroborar la implementación de controles observados durante las visitas realizadas por los entes reguladores.

3. Ciberseguridad.

   Revisar y evaluar los componentes para la prestación de los servicios del SPEI y el SPID.

   Evaluar los controles y procedimientos aplicados en la administración de los mecanismos de ciberseguridad, con un enfoque en las acciones fundamentales que cada entidad debe implementar para asegurar la protección de sus activos de información relacionados con SPEI y SPID, tales como el inventario y autorización de dispositivos y software; configuración del hardware y software en dispositivos móviles, laptops, estaciones y servidores; evaluación continua de vulnerabilidades y su remediación; controles en puertos, protocolos y servicios de redes; protección de datos; controles de acceso en redes inalámbricas; seguridad del software aplicativo interno o de terceros; análisis y pruebas de vulnerabilidades, proveedores que soportan operaciones críticas, con la finalidad de verificar que los medios de pago (SPEI y SPID) mantienen la integridad, confiabilidad y disponibilidad en la realización de las transacciones en la Banca de Desarrollo.

Áreas Revisadas

La Dirección de Regulación y Supervisión, Dirección de Sistemas de Pagos (ahora Dirección General de Sistemas de Pagos e Infraestructuras de Mercados) en BANXICO. La Dirección General de Tecnologías de la Información y Dirección General de Operaciones y Sistemas de Pagos en BANCOMEXT. La Dirección de Informática, (ahora Dirección de Tecnologías de la Información y Telecom), la Dirección de Operaciones Bancarias, la Subdirección de Tecnología y Seguridad Informática en BANJERCITO. La Dirección de Tecnologías de Información y Comunicaciones en BANOBRAS. La Dirección General Adjunta de Tecnologías y Operación en Banco del Bienestar. La Dirección de Informática, la Subdirección de Calidad Informática, Producción e Infraestructura Central, la Dirección de Administración de Riesgos en NAFIN y la Dirección General Adjunta de Administración, Operación y Tecnologías en SHF.

Disposiciones Jurídicas y Normativas Incumplidas

Durante el desarrollo de la auditoría practicada, se determinaron incumplimientos de las leyes, reglamentos y disposiciones normativas que a continuación se mencionan:

1. Otras disposiciones de carácter general, específico, estatal o municipal: de las Declaraciones I incisos E, F, y G, Octava, Décimo Primera y Décimo Quinta del contrato 012/2018 celebrado con el proveedor LGEC S.A. de C.V, requisito 1.1 fracción ii, Requisito 11 incisos a ,b, c, y d del Apéndice M del Manual de Operación del SPEI versión 5.3.3 del 22 de junio de 2017, Requisito 11 incisos a y b del Anexo C del Manual de Operación del SPID versión 3.1 del 30 de diciembre de 2016, Capitulo III, regla 12a de la circular 13/2017 publicada en el D.O.F. el 04 de julio de 2017, Capitulo III regla 15a, fracción X de la circular 10/2018 de fecha 27 de julio de 2018, Capitulo IV, sección I, regla 56a, fracción I, apartado A, incisos a, a bis, b numeral 3; en el artículo 86, inciso b), numeral 1 y 164 fracción V de las Disposiciones de carácter general aplicables a las instituciones de crédito del 27 de diciembre de 2017, Fracción III Subdirección de Tecnología y Seguridad Informática, Objetivo 1, Función1; Dirección de Informática, Objetivo 2 función 3; Gerencia de Computo y Seguridad Función 13, Subdirección de Servicios de Informática Objetivo 1, función 2; Gerencia de Centro de Cómputo y Seguridad Objetivo 1,: Dirección de Operaciones Bancarias, Objetivo 2, Gerencia de Operaciones de Tesorería Objetivo 1; Dirección de Auditoría Interna Funciones 1 y 2; Órgano Interno de Control, Titular del Órgano Interno de Control, Función 1; del Manual General de Organización del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. del 30 de septiembre de 2016: Fracción III. Subdirección de Tecnología y Seguridad Informática Función 7 y 12: Dirección de Informática Función 4 del Manual General de Organización del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. del 30 de abril de 2018 y del 30 de noviembre.

   del Artículo 66 fracción I, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, última reforma publicada el 30 de marzo de 2016 en el Diario Oficial de la Federación (D.O.F).

Fundamento Jurídico de la ASF para Promover Acciones

Las facultades de la Auditoría Superior de la Federación para promover o emitir las acciones derivadas de la auditoría practicada encuentran su sustento jurídico en las disposiciones siguientes:

Artículo 79, fracciones II, párrafo tercero, y IV, de la Constitución Política de los Estados Unidos Mexicanos.

Artículos 10, fracción I, 14, fracción III, 15, 17, fracción XV, 36, fracción V, 39, 40, de la Ley de Fiscalización y Rendición de Cuentas de la Federación.