TIPO DE REVISIÓN: Combinada de Cumplimiento y Desempeño

Número de auditoría:
54-GB

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

Ente fiscalizado

Comisión Nacional Bancaria y de Valores (CNBV)

¿Qué se auditó?

Se revisó la ciberseguridad de los Sistemas de Pago (SPEI y SPID), desde la normativa emitida por BANXICO, los procesos y controles que tiene en su rol de: supervisor, vigilancia operador y participante; y la coordinación con la CNBV. También se revisaron los mecanismos de actuación realizados por BANJERCITO y BANXICO durante y posterior el incidente de ciberseguridad ocurrido en BANJERCITO. Se evaluaron los niveles de madurez de la ciberseguridad en los Sistemas de Pago en 6 participantes de la Banca de Desarrollo y BANXICO como operador, para lo cual, la ASF desarrolló una metodología basada en las mejores prácticas internacionales de ciberseguridad.

¿Por qué se practicó esta auditoría?

CRITERIOS DE SELECCIÓN

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

Los Sistemas de Pago de alto valor más representativos en el Sector Financiero Mexicano son los siguientes: Sistema de Pagos Electrónicos Interbancarios (SPEI) y el Sistema de Pagos Interbancarios en Dólares (SPID).

Los sistemas de Pago son regulados por el Banco de México.

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.

UNIVERSO SELECCIONADO

El Banco de México (BANXICO) como organismo regulador, así como 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. (BANJERCITO), Banco Nacional 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).

MUESTRA AUDITADA

N/A

Principales resultados de la auditoría

- *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.*

- *BANXICO en su rol de operador de los Sistemas de Pago, carece de una normativa en materia de seguridad informática y de gestión del riesgo operacional y no lleva a cabo procesos de revisión por un tercero independiente de la Dirección General de Sistemas de Pagos de Infraestructuras de Mercados (DGSPIM) y de la Dirección General de Tecnologías de Información (DGTI).*

- *BANXICO no cuenta con mecanismos que le permitan determinar el perfil de riesgo de cada participante del Sistema de Pagos Electrónicos Interbancarios (SPEI), tomando en cuenta el nivel de cumplimiento de sus controles de seguridad informática y gestión del riesgo operacional, cambios relevantes en su infraestructura, procesos y ciberamenazas.*

- *En BANXICO, la 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.*

- *En la revisión de la madurez de la 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. De la 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.*

- *La Comisión Nacional Bancaria y de Valores y el Banco de México, no comparten la información de los hallazgos y observaciones en materia de riesgo tecnológico y seguridad de la información que identifican en las actividades de supervisión y vigilancia que realizan.*

- *BANJERCITO en el incidente de ciberseguridad ocurrido el 24 de abril de 2018, no contaba con planes de respuesta ante incidentes, por lo que no llevó a cabo una cadena de custodia que asegurara la integridad de todos los componentes involucrados en el incidente referido e hizo un pago por 1.5 millones de pesos por el deducible del seguro sin haber realizado labores de investigación para deslindar posibles responsabilidades.*

- *BANXICO no considera en su plan de respuesta a incidentes de seguridad, posibles escenarios de actuación ante eventos en los participantes que puedan afectar al operador y a otros participantes.*

Escanea el código y descarga el informe de auditoría completo.

Principales acciones emitidas

- *Se emitieron 13 Recomendaciones, dos Promociones de Responsabilidad Administrativa Sancionatoria y un Pliego de Observaciones por los cuales se determinaron 1.5 millones de pesos pendientes por aclarar.*