Banco de México

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2022-0-98001-20-0016-2023

Modalidad: Presencial

Núm. de Auditoría: 16

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 2022 considerando lo dispuesto en el Plan Estratégico de la ASF.

Objetivo

Fiscalizar la gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, administración de riesgos, seguridad de la información, continuidad de las operaciones, calidad de datos, desarrollo de aplicaciones y aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que se realizaron conforme a las disposiciones jurídicas y normativas aplicables.

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	456,336.0
Muestra Auditada	67,237.6
Representatividad de la Muestra	14.7%

El universo seleccionado por 456,336.0 miles de pesos corresponde al total de pagos de los contratos relacionados con las Tecnologías de Información y Comunicaciones (TIC) en el ejercicio fiscal de 2022; la muestra auditada está integrada por cuatro contratos y dos convenios para prestar los servicios técnicos especializados, la renovación del software para la gestión de servidores, la adquisición de crecimiento para sistemas de almacenamiento, así como el incremento de la base de servidores institucionales con pagos por 67,237.6 miles de pesos que representan el 14.7% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de TIC en el Banco de México (Banxico) relacionada con la Ciberseguridad de la Banca Electrónica y los Sistemas de Pagos.

Los recursos objeto de revisión en esta auditoría se encuentran reportados en el presupuesto de gasto corriente e inversión física correspondiente al ejercicio de 2022, el cual fue aprobado por la Junta de Gobierno del Banco de México en sesión celebrada el 30 de noviembre de 2021.

Antecedentes

En la fiscalización de la Cuenta Pública de 2018, se detectó que la institución operaba los sistemas de pagos sin una apropiada segregación de funciones, también se identificó que ninguna entidad de la banca de desarrollo fue sujeta a una visita de inspección por parte del banco central; asimismo, se observó que el banco no compartió los hallazgos en materia de riesgo tecnológico y seguridad de la información con otras instancias reguladoras. De estas observaciones, se promovieron y emitieron las acciones correspondientes, que obran en el informe individual de la auditoría número 54-GB "Auditoría de Ciberseguridad a la Banca Electrónica y Medios de Pago del Sistema Financiero del Gobierno Mexicano".

Entre 2018 y 2022, el Banxico erogó 2,161,098.8 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la manera siguiente:

RECURSOS EROGADOS EN MATERIA DE TIC EN LOS ÚLTIMOS CINCO AÑOS
(Miles de pesos)

	2018	2019	2020	2021	2022	Total
Monto por año	340,104.4	353,835.4	502,738.5	508,084.4	456,336.0	2,161,098.8

FUENTE: Elaborado con información proporcionada por el Banco de México.
NOTA: Diferencias por redondeo.

Con base en el análisis efectuado mediante procedimientos de auditoría, se evaluaron los mecanismos de control implementados con el fin de establecer si son suficientes para el cumplimiento de los objetivos de las contrataciones de TIC, así como determinar el alcance, naturaleza y muestra de la revisión, y se obtuvieron los resultados que se presentan en este informe.

Resultados

1. Análisis Presupuestal

De acuerdo con el Presupuesto del Banco Central para el Ejercicio Fiscal de 2022 aprobado por la Junta de Gobierno del Banco de México mediante la sesión del 30 de noviembre de 2021, se autorizó un presupuesto inicial de 11,799,133.8 miles de pesos; con las ampliaciones y reducciones el presupuesto modificado mantuvo el monto asignado inicialmente, del cual, se ejercieron recursos por 10,590,438.2 miles de pesos.

Del análisis de la información de los estados presupuestales para el ejercicio de 2022, se concluyó que el Banco de México tuvo un presupuesto pagado de 9,684,423.5 miles de pesos, de los cuales 456,336.0 miles de pesos corresponden a recursos relacionados con las TIC, que representan el 4.7% del presupuesto, como se muestra a continuación:

RECURSOS PAGADOS EN TIC DURANTE EL EJERCICIO DE 2022
(Miles de pesos)

Unidad Administrativa	**Pagado**	**Pagado TIC**	**%**
Dirección General de Emisión	5,602,615.5	12,167.4	0.2
Dirección General de Administración	1,535,866.7	9,256.0	0.6
Dirección General de Tecnologías de la Información	662,382.8	386,951.7	58.4
Dirección General de Investigación Económica	395,391.8	7,808.5	2.0
Dirección General de Operaciones de Banca Central	267,576.6	9,557.2	3.6
Dirección General de Contraloría y Administración de Riesgos	241,140.0	11,841.2	4.9
Dirección General de Estabilidad Financiera	225,883.6	10,604.9	4.7
Dirección General de Asuntos del Sistema Financiero	159,566.6	1,048.7	0.7
Dirección de Educación Financiera y Fomento Cultural	119,522.1	2,861.6	2.4
Dirección General Jurídica	133,003.4	74.2	0.1
Dirección de Vinculación Institucional y Comunicación	108,299.2	3,285.5	3.0
Junta de Gobierno	88,359.7	148.7	0.2
Unidad de Auditoría	67,598.5	85.1	0.1
Dirección General de Sistema de Pagos e Infraestructuras de Mercados	33,139.3	207.4	0.6
Unidad de Transparencia	19,440.3	425.0	2.2
Secretaría de la Junta de Gobierno	12,923.5	13.0	0.1
Dirección de Análisis y Políticas de Riesgos Ambientales y Sociales	11,714.1	-	-
Totales	**9,684,423.5**	**456,336.0**	**4.7**

FUENTE: Elaborado con información proporcionada por el Banco de México.
NOTA: Diferencias por redondeo.

Los recursos pagados en materia de las TIC por 456,336.0 miles de pesos se integran como se muestra a continuación:

GASTOS DE TIC EN EL BANCO DE MÉXICO DURANTE EL EJERCICIO DE 2022
(Miles de pesos)

Número de cuenta	Cuenta	Pagado
597010105401000000	Adquisición Equipo de TI y nuevas licencias SW para Emisión	23,162.3
597010105800000000	Adquisición Equipo de TI y nuevas licencias SW	237,178.1
345435105000000000	Cuotas Eventuales a Asociaciones de TI	726.1
345371206000000000	Gastos Adquisición y Baja de Bienes y Desechos TI	13.8
344501200000000000 345501200000000000	Honorarios, Consultorías y Asesorías en TI	23,568.3
344351600000000000 345351600000000000	Insumos de TI	3,544.2
345370212000000000	Mantenimiento a Equipo de Audio y Video	542.2
344370210000000000 345370210000000000	Mantenimiento a Equipo de Cómputo	3,794.9
344370209000000000 345370209000000000	Mantenimiento a Equipo de Telecomunicaciones	31,216.6
344370214000000000 345370214000000000	Mantenimiento a Equipos de Seguridad Electrónica	30,850.0
345370211000000000	Mantenimiento de equipos de apoyo al cómputo	9,333.9
344352500000000000 345352500000000000	Servicio Corporativo suministro de TI a través internet	45,971.5
345351801000000000	Servicio Corporativo de Telecomunicaciones	8,867.4
344351802000000000 345351802000000000	Servicio Externo de Telecomunicaciones	12,450.0
345351900000000000	Servicios de Información Electrónica	21,455.6
345355100000000000	Servicios de Organización de Información	202.7
344352904000000000 345352904000000000	Servicios Técnicos Especializados de TI	3,458.2
Totales		**456,336.0**

FUENTE: Elaborado con información proporcionada por el Banco de México.
NOTA: Diferencias por redondeo.

Del universo seleccionado en el ejercicio de 2022 por 456,336.0 miles de pesos que corresponde al total de pagos ejercidos en los contratos relacionados con las TIC, se erogaron 67,237.6 miles de pesos en cuatro contratos y dos convenios que representan el 14.7% del universo seleccionado, y que son los siguientes:

MUESTRA DE CONTRATOS Y CONVENIOS DE TIC PAGADOS DURANTE EL EJERCICIO DE 2022
(Miles de pesos y de dólares)

Tipo Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto	Pagado
				Del	Al	MXN/USD	MXN
Licitación Pública Nacional	19-1147-2-Subcontrat	Esparta Servicios Eficientes, S.A. de C.V., con Imago Centro de Inteligencia de Negocios, S.A. de C.V., y Gurges Implementación de Negocios, S.A. de C.V.	Servicios especializados para llevar a cabo actividades de distinta naturaleza en proyectos específicos	01/11/2020	31/10/2025	580,000.0[1]	34,086.6
Licitación Pública Internacional	C000009653	GNR Apoyo Estratégico, S.A. de C.V.	Renovación del software para la gestión de servidores virtuales	02/06/2022	01/06/2023	271.9[2]	6,271.2
Adjudicación Directa	0000147861	GNR Apoyo Estratégico, S.A. de C.V.	Adquisición de crecimiento de sistemas de almacenamiento y el incremento de la base de servidores	29/07/2022	24/11/2026	819.9[2]	18,983.1
Adjudicación Directa	0000148009	Teleinformática en Servicios Avanzados, S.A. de C.V.	Adquisición de servidores y sistemas de almacenamiento	10/08/2022	09/03/2027	586.8[2]	7,896.7
	Carta Convenio No. 0000148009-1		Prorrogar el plazo de entrega de los bienes				
	Carta Convenio No. 0000148009-2		Modificación del plazo y forma de pago				
Total							**67,237.6**

FUENTE: Elaborado con información proporcionada por el Banco de México.

NOTA[1]: Cifras en pesos.
NOTA[2]: Cifras en dólares.

Se verificó que los pagos se reconocieron en las partidas presupuestarias correspondientes; el análisis de los contratos y convenios de la muestra se presenta en los resultados subsecuentes.

2. Servicios especializados para llevar a cabo actividades de distinta naturaleza en proyectos específicos

Se analizó el contrato número "19-1147-2-Subcontrat" suscrito con Esparta Servicios Eficientes, S.A. de C.V., conjuntamente con Imago Centro de Inteligencia de Negocios, S.A. de C.V., y Gurges Implementación de Negocios, S.A. de C.V., el cual se adjudicó mediante licitación pública nacional con fundamento en los artículos 57, primer párrafo, de la Ley del

Banco de México; 21, 22, fracción I, 32, fracción I, 44, y 46, de las Normas del Banco de México en materia de adquisiciones y arrendamientos de bienes muebles así como de servicios; y en la disposición vigésima séptima de la Norma Administrativa Interna en materia de adquisiciones y arrendamientos de bienes muebles así como de servicios del Banco de México, con vigencia del 1 de noviembre de 2020 al 31 de octubre de 2025 por un monto de 580,000.0 miles de pesos, con el objeto de prestar los "Servicios especializados para llevar a cabo actividades de distinta naturaleza en proyectos específicos que el Banco de México determine"; se efectuaron pagos por 34,086.6 miles de pesos durante el ejercicio de 2022, de cuya revisión se determinó lo siguiente:

Alcance del servicio

Contrato abierto para el desarrollo de diversas actividades de distinta naturaleza por parte del proveedor con perfiles relacionados con las TIC como el digitalizador de documentos; el técnico en sistemas; el analista de organización de la información; el asesor de atención a usuarios; el desarrollador de sistemas Java; el soporte de primer nivel para la línea frontal de servicios de red; el técnico especialista en equipo de audio y video; el analista de gestión y monitoreo; el desarrollador de procesos de trasformación de datos y la operadora telefónica, entre otros.

Pagos del contrato

En el ejercicio de 2022 se realizaron pagos por 34,086.6 miles de pesos para perfiles con diversas especialidades, de los cuales se revisó una muestra de 3,963.4 miles de pesos (11.6%) que corresponde a los especialistas de sistemas y organización de la información.

Revisión técnica, funcional y administrativa

Se revisó la entrega de los servicios especializados de conformidad con lo establecido en el contrato, el anexo, las solicitudes de contratación, las cédulas mensuales de determinación de cuotas y las bitácoras de actividades, y se identificó lo siguiente:

Precio y forma de pago de los honorarios

Para la forma de pago de los honorarios de los especialistas, las gerencias usuarias determinaron el importe total a pagar a partir del nivel salarial similar a los puestos internos del banco y a esa cantidad se le consideró el impuesto.

El Banxico, en el transcurso de la auditoría y con motivo de la intervención de la ASF, instruyó las acciones necesarias para establecer los mecanismos para determinar los honorarios brutos mensuales a pagar por los servicios especializados.

Inspección y Supervisión del Banco

- El contrato estableció que para la correcta supervisión de la prestación de los servicios el banco podía grabar las llamadas con el proveedor donde consten las autorizaciones para

efectuar los servicios contratados; sin embargo, no se realizaron grabaciones debido a que el área que lleva esta gestión no se encuentra autorizada para realizarlas.

- Por otra parte, la autorización de los servicios a cargo de las áreas usuarias fue registrada en el sistema mediante una bitácora de actividades, la cual carece del detalle de los trabajos realizados por los especialistas; no obstante, la entidad fiscalizada consideró dicha bitácora como constancia del cumplimiento de las cantidades, características, especificaciones, términos y condiciones de los trabajos devengados.

Perfiles de Sistemas

Digitalizadores de documentos de organización de la información

- En la bitácora de actividades de un personal especializado femenino, se reportaron trabajos 3 días antes de su contratación el 15 de febrero de 2022; asimismo, aun cuando la especialista causó baja el día 20 de abril del mismo año, se identificaron actividades a su nombre hasta el día 28 del mismo mes.

- El registro de actividades de un personal especializado masculino no contiene los trabajos realizados en los meses de mayo, octubre, noviembre y diciembre de 2022. Cabe señalar que el banco manifestó que el especialista se incorporó a otra unidad administrativa a partir de octubre; sin embargo, se carece de la bitácora de actividades y de la "Solicitud de Digitalización de Documentos", la cual no incluyó todas las actividades requeridas por el proyecto para establecer los mecanismos adecuados de supervisión.

- No se identificaron los trabajos de otro personal especializado masculino en la bitácora de actividades de enero de 2022. Cabe mencionar que el recurso causó baja el 24 de febrero del mismo año; no obstante, se reportaron actividades a su nombre el día 28 del mismo mes; de igual manera, se carece de la "Solicitud de Digitalización de Documentos".

En conclusión, no se tienen grabaciones de las llamadas donde consten las autorizaciones para efectuar los servicios; asimismo, la bitácora de actividades carece del detalle de los trabajos realizados.

2022-0-98001-20-0016-01-001 **Recomendación**

Para que el Banco de México fortalezca las políticas, procedimientos y controles para evaluar la autorización para grabar las llamadas de las áreas usuarias donde se otorgue el consentimiento para efectuar los servicios, así como detallar los trabajos realizados en la bitácora de actividades del sistema, con la finalidad de asegurar la autorización, el cumplimiento y la trazabilidad de los requerimientos realizados por los servicios especializados en beneficio de la institución.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados

Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2022-9-98001-20-0016-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que la Dirección General de la Contraloría y Administración de Riesgos del Banco de México 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, respecto del contrato número 19-1147-2-Subcontrat "Servicios especializados para llevar a cabo actividades de distinta naturaleza en proyectos específicos que el Banco de México determine", tuvieron omisiones en la supervisión de las actividades relacionadas con la administración de los servicios que brinda el archivo institucional, así como en la coordinación de los servicios de digitalización a fin de apoyar a las unidades administrativas de la institución en la gestión de los documentos, por la falta de integración de las cantidades, características, especificaciones, términos y condiciones de los trabajos solicitados a los digitalizadores de documentos del grupo de organización de la información, en incumplimiento de las Normas y criterios generales del presupuesto de gasto corriente e inversión física del Banco de México, disposición Vigésima; de la Norma administrativa interna del proceso de pagos institucionales de bienes y servicios del Banco de México, numeral I.I.4.1; del Manual de Organización del Banco de México, función segunda de la Gerencia de Organización de la Información y función tercera de la Subgerencia de Coordinación de Archivos, y del contrato número "19-1147-2-Subcontrat", cláusula "8. Inspección y Supervisión del Banco", párrafo cuarto.

3. Adquisición de servidores, sistemas de almacenamiento y licencias de software

Se analizaron los contratos números 0000147861, 0000148009 y C000009653, celebrados con GNR Apoyo Estratégico, S.A. de C.V., y Teleinformática en Servicios Avanzados, S.A. de C.V., los dos primeros mediante adjudicación directa de conformidad con los artículos 57, fracción II, de la Ley del Banco de México, y 39, fracción III, de las Normas del Banco de México en materia de adquisiciones y arrendamientos de bienes muebles, así como de servicios; y el tercer contrato por licitación pública internacional de conformidad con los artículos 57, primer párrafo, de la Ley de Banco de México; 15, fracción I, y 32, fracción II, de las Normas del Banco de México en materia de adquisiciones y arrendamientos de bienes muebles, así como de servicios; los tres con vigencia del 2 de junio de 2022 al 9 de marzo de 2027 por un monto acumulado de 1,678.6 miles de dólares, con el objeto de la compra de los equipos, las licencias de uso de software, los materiales y los accesorios para su instalación y funcionamiento. Adicionalmente se suscribieron dos convenios modificatorios, el primero para conceder una prórroga en la entrega de los bienes y el segundo con objeto de establecer la cesión de derechos de cobro a los proveedores asociados. Se efectuaron pagos por 33,151.0 miles de pesos durante el ejercicio 2022 y se determinó lo siguiente:

Alcance del contrato

La compra de servidores y sistemas de almacenamiento con los materiales y accesorios para su instalación y funcionamiento, así como las licencias de uso de software de virtualización con la finalidad de atender el programa del reemplazo general de la infraestructura y almacenamiento de la institución.

Revisión técnica, funcional y administrativa

Se realizaron pruebas a 36 servidores, 5 sistemas de almacenamiento y 307 actualizaciones de licencias de virtualización; de cuyo resultado se observó el cumplimiento de las características y especificaciones técnicas establecidas en el contrato.

4. Ciberseguridad de la Banca Electrónica y los Sistemas de Pago

En la fiscalización de la Cuenta Pública de 2018, se practicó la auditoría número 54-GB "Auditoría de Ciberseguridad a la Banca Electrónica y Medios de Pago del Sistema Financiero del Gobierno Mexicano", con la finalidad de evaluar los controles y procedimientos aplicados en la administración de los mecanismos de ciberseguridad, con un enfoque en las acciones fundamentales para asegurar la protección de sus activos de información relacionados con los sistemas de pago (SPEI y SPID) para verificar que mantienen la integridad, confiabilidad y disponibilidad en la realización de las transacciones en la banca electrónica.

La Auditoría Superior de la Federación desarrolló un modelo para evaluar el nivel de madurez de la ciberseguridad en la administración y operación del Sistema de Pagos Electrónicos Interbancarios (SPEI) y el Sistema de Pagos Interbancarios en Dólares (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); los apartados "A. En la Infraestructura Tecnológica" y "B. En los Canales Electrónicos" del "Apéndice M: Requisitos de Seguridad Informática y de Gestión del Riesgo Operacional" del Manual del SPEI del Banco de México (Banxico); el "Apéndice E: Seguridad Informática y Gestión de Riesgo Operacional" del Manual del SPID 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.

Los niveles de madurez utilizados en esta auditoría fueron definidos con base en la integración del modelo de madurez de la capacidad (CMMI) y la herramienta de evaluación de ciberseguridad del Consejo Federal de Examen de Instituciones Financieras (FFIEC), de conformidad con los niveles siguientes:

NIVELES DE MADUREZ PARA LA EVALUACIÓN DE LA CIBERSEGURIDAD EN LOS SISTEMAS DE PAGOS

Nivel	Descripción
Incompleto (0)	Carece de actividades o éstas no se llevan a cabo de forma completa por lo que no se cubren los objetivos del proceso.
Inicial (1)	Las actividades se realizan, pero no se logra el cumplimiento de los objetivos del proceso.
Administrado (2)	El proceso logra sus propósitos en una forma organizada, los procesos están bien definidos.
Definido (3)	El proceso logra sus propósitos en una forma organizada, existen estándares y mejores prácticas en toda la organización.
Cuantitativo (4)	El proceso logra su propósito, está bien definido y su desempeño es medido cuantitativamente.
Optimizado (5)	El proceso logra su propósito, está bien definido, su desempeño es medido y se lleva a cabo la mejora continua.

FUENTE: Modelo de madurez desarrollado por la ASF con base en el modelo CMMI y la herramienta de evaluación del FFIEC.

Para alcanzar el siguiente nivel de madurez, es necesario cumplir al menos con el 75.0% del nivel anterior, el primer nivel considera que se deben cumplir todos los requerimientos legales, así como las guías recomendadas por las entidades de supervisión. Los requerimientos solicitados por los manuales del SPEI y SPID emitidos por el Banxico se encuentran incluidos en el primer y segundo nivel de madurez.

En el análisis del modelo, fueron revisadas 5 funciones, 17 categorías, 65 subcategorías y 376 controles, como resultado del comparativo respecto de la evaluación practicada en la Cuenta Pública de 2018 se obtuvo lo siguiente:

COMPARATIVO DE LA EVALUACIÓN DE LA CIBERSEGURIDAD EN LOS SISTEMAS DE PAGOS

Categoría	2018	2022
ID.AM Gestión de Activos		
ID.BE Entorno Organizacional		
ID.GV Gobernanza		
ID.RA Evaluación de Riesgos		
PR.AC Gestión de Identidad y Control de Acceso		
PR.AT Concienciación y Capacitación		
PR.DS Seguridad de los Datos		
PR.IP Procesos y Procedimientos de Protección de la Información		
PR.MA Mantenimiento		
PR.PT Tecnología de Protección		
DE.AE Anomalías y Eventos		
DE.CM Monitoreo Continuo de la Seguridad		
DE.DP Procesos de Detección		
RS.RP Planificación de la Respuesta		
RS.CO Comunicaciones		
RS.AN Análisis		
RC.CO Comunicaciones		

FUENTE: Elaborado con información proporcionada por el Banco de México.

En conclusión, se identificó una mejora en el promedio de la calificación de los controles de 1.0 a 2.8 en el nivel de madurez; no obstante, el 4.6% de las subcategorías se encuentra debajo del nivel de madurez 2 (administrado).

2022-0-98001-20-0016-01-002 **Recomendación**

Para que el Banco de México continúe con las políticas, los procesos, los procedimientos y los controles en la función de identificación de la ciberseguridad en los sistemas de pagos, a efecto de que se prioricen y difundan las metas de la gestión de riesgos de seguridad cibernética con todos los involucrados en la operación de los sistemas de pago.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2022-0-98001-20-0016-01-003 **Recomendación**

Para que el Banco de México continúe con las políticas, los procesos, los procedimientos y los controles en la función de protección de la ciberseguridad en los sistemas de pago, con la finalidad de instrumentar políticas de seguridad de la información que aborden el propósito, el alcance, los roles, las responsabilidades, el compromiso de la dirección y la coordinación entre las unidades administrativas para gestionar la protección de los activos de información.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2022-0-98001-20-0016-01-004 **Recomendación**

Para que el Banco de México continúe con las políticas, los procesos, los procedimientos y los controles en la función de respuesta de la ciberseguridad en los sistemas de pagos, a efecto de que las actividades de respuesta se coordinen con las partes interesadas internas y externas para una atención expedita de los incidentes informáticos.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

Buen Gobierno

Impacto de lo observado por la ASF para buen gobierno: Liderazgo y dirección, Planificación estratégica y operativa, Controles internos, Aseguramiento de calidad y Vigilancia y rendición de cuentas.

Resumen de Resultados, Observaciones y Acciones

Se determinaron 4 resultados, de los cuales, en 2 no se detectaron irregularidades y los 2 restantes generaron:

4 Recomendaciones y 1 Promoción de Responsabilidad Administrativa Sancionatoria.

Consideraciones para el seguimiento

Los resultados, observaciones y acciones contenidos en el presente informe 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 de auditoría se encuentran sujetas al proceso de seguimiento, por lo que, debido a la información y consideraciones que en su caso proporcione la entidad fiscalizada podrán atenderse o no, solventarse o generar la acción superveniente que corresponda de conformidad con el marco jurídico que regule la materia.

Dictamen

El presente dictamen se emite el 6 de febrero de 2024, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue fiscalizar la gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, la administración de riesgos, la seguridad de la información, la continuidad de las operaciones, la calidad de datos, el desarrollo de aplicaciones y el aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que esto se realizó conforme a las disposiciones jurídicas y normativas aplicables y, específicamente, respecto de la muestra revisada que se establece en el apartado relativo al alcance, se concluye que, en términos generales, el Banco de México cumplió con las disposiciones legales y normativas aplicables en la materia, excepto por los aspectos observados siguientes:

- En relación con los servicios especializados para llevar a cabo actividades de distinta naturaleza en proyectos específicos, no se tuvo el detalle de los trabajos realizados en la bitácora de actividades; asimismo, se carece de la grabación de las llamadas con las autorizaciones para realizar los servicios.

- Se identificó una mejora en el promedio de la calificación de los controles de 1.0 a 2.8 en el nivel de madurez respecto de la ciberseguridad de los sistemas de pago; no obstante, el 4.6% de las subcategorías se encuentra debajo del nivel de madurez 2 (administrado).

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Mtro. Genaro Héctor Serrano Martínez	Mtro. Roberto Hernández Rojas Valderrama

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. Verificar que las cifras reportadas en la Cuenta Pública se corresponden con las registradas en el estado del ejercicio del presupuesto y que cumplen con las disposiciones y normativas aplicables y analizar la integración del gasto ejercido en materia de TIC en los capítulos asignados de la Cuenta Pública fiscalizada.

2. Validar que el estudio de factibilidad comprende el análisis de las contrataciones vigentes, la determinación de la procedencia de su renovación, la pertinencia de realizar contrataciones consolidadas, y los costos de mantenimiento, soporte y operación que impliquen la contratación, vinculados con el factor de temporalidad para determinar la conveniencia de adquirir, arrendar o contratar servicios, así como la investigación de mercado.

3. Verificar el procedimiento de contratación, el cumplimiento de las especificaciones técnicas y distribución del bien o servicio de acuerdo con las necesidades requeridas por las áreas solicitantes; revisar que los bienes adquiridos fueron contemplados en el Programa Anual de Adquisiciones, Arrendamientos y Servicios; validar la información del registro de accionistas para identificar asociaciones indebidas, subcontrataciones en exceso y transferencia de obligaciones y verificar la situación fiscal de los proveedores para conocer el cumplimiento de sus obligaciones fiscales, aumento o disminución de obligaciones, entre otros.

4. Comprobar que los pagos realizados por los trabajos contratados estuvieron debidamente soportados, que contaron con controles que permitieron su fiscalización, y que correspondieron a trabajos efectivamente devengados que justifiquen las facturas pagadas y la autenticidad de los comprobantes fiscales; asimismo, verificar la entrega en tiempo y forma de los servicios, así como la pertinencia de su penalización o deductivas en caso de incumplimientos.

5. Analizar los contratos y anexos técnicos relacionados con la administración de proyectos, desarrollo de soluciones tecnológicas, servicios administrados para la operación de infraestructura y sistemas de información, telecomunicaciones y demás relacionados con las TIC para verificar antecedentes, investigación de mercado, adjudicación, beneficios esperados, entregables (términos, vigencia, entrega, resguardo, garantías, pruebas de cumplimiento y sustantivas), implementación y soporte de los servicios; verificar que el plan de mitigación de riesgos fue atendido, así como el manejo del riesgo residual y la justificación de los riesgos aceptados por la entidad.

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

Áreas Revisadas

Las direcciones de Recursos Materiales y de Contabilidad, Planeación y Presupuesto adscritas a la Dirección General de Administración, así como la Dirección General de Tecnologías de la Información, ambas direcciones generales adscritas a la Gubernatura del Banco de México.

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: el Manual de Operación del SPEI del Banco de México, Anexo "M: Requisitos de Seguridad Informática y de Gestión de Riesgo Operacional", numerales "1.1 Seguridad Informática", apartado "A. En la Estructura Tecnológica", "1.2 Gestión del riesgo

operacional", apartado "Políticas y procedimientos para la gestión de riesgos operacionales"; el Manual de Operación del SPID del Banco de México, "Anexo C. Requisitos de seguridad informática y de gestión del riesgo operacional", apartados "Gestión del Riesgo Operacional" y "Seguridad Informática"; las Normas y criterios generales del presupuesto de gasto corriente e inversión física del Banco de México, disposición Vigésima; la Norma administrativa interna del proceso de pagos institucionales de bienes y servicios del Banco de México, numeral I.I.4.1; la Norma Administrativa Interna en materia de adquisiciones y arrendamientos de bienes muebles, así como de servicios del Banco de México, disposición Trigésima Séptima; el Macroproceso de Planeación, Presupuesto, Contrataciones, Pagos e Ingresos Institucionales del Banco de México, numerales 1.1.1, 1.1.2, y 1.1.3, del proceso de Planeación institucional; el Manual de Procedimientos de Operación "Planeación Institucional" del Banco de México, disposición Quinta del Título Segundo, Descripción de Actividades, Capítulo I, Definición de la Estrategia; el Manual de Organización del Banco de México, función segunda de la Gerencia de Organización de la Información y función tercera de la Subgerencia de Coordinación de Archivos; la Circular sobre lineamientos, de austeridad, ahorro y disciplina del gasto en Banco de México del 28 de diciembre de 2018, dictamen organizacional acerca de la contratación de personal externo; y el contrato número "19-1147-2-Subcontrat", párrafo cuarto de la cláusula "8. Inspección y Supervisión del Banco".

Fundamento Jurídico de la ASF para Promover Acciones y Recomendaciones

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.