COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ESPECIAL 19/2025
DEL 19 DE JUNIO DE 2025

A las doce horas con treinta minutos del 19 de junio de 2025, participan en la presente sesión a través de medios electrónicos de comunicación, José Ramón Rodríguez Mancilla, Gerente de Organización de la Información, en suplencia del Director de Seguridad y Organización de la Información; Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, en suplencia de la Titular de la Unidad de Transparencia; y Edgar Miguel Salas Ortega, Gerente de Instrumentación Jurídica, en suplencia del Director Jurídico, todos ellos integrantes del Comité de Transparencia de este Instituto Central, así como Sergio Zambrano Herrera, Gerente de Gestión de Transparencia, en su carácter de Secretario de este órgano colegiado, de conformidad con la Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el veintinueve de abril de dos mil veinticinco (Reglas).----------

Quien ejerce en este acto las funciones de Secretariado del Comité de Transparencia manifestó que existe quórum para la celebración de la presente sesión, de conformidad con lo previsto en los artículos 39, párrafos segundo y tercero, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 77 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 4o. del Reglamento Interior del Banco de México (RIBM); así como con la Quinta y Sexta de las Reglas. Por lo anterior, se procedió en los términos siguientes: ----------

APROBACIÓN DEL ORDEN DEL DÍA. ----------

Quien ejerce en este acto las funciones de Secretariado del Comité de Transparencia, sometió a consideración de los integrantes de ese Órgano Colegiado el documento que contiene el orden del día.----------

Este Comité de Transparencia, con fundamento en los artículos 39, párrafo segundo, 40, fracción VIII, de la LGTAIP; 77 de la LGPDPPSO; 4o. y 31, fracción XX, del RIBM; así como con la Quinta de las Reglas, por unanimidad, aprobó el orden del día en los términos del documento que se adjunta a la presente Acta como **"ANEXO 1"** y procedió a su desahogo, conforme a lo siguiente: ----------

PRIMERO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE DESARROLLO E INNOVACIÓN DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia D20-015/2025, de fecha 25 de marzo de 2025, suscrito por quien es titular de la Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, el cual se agrega a la presente Acta como "**ANEXO 2**", por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de ampliar el periodo de reserva de la información referida en dicho oficio, de conformidad con la fundamentación y motivación señalada en el mismo, así como en la prueba de daño correspondiente, y solicitó a este Órgano Colegiado aprobar la ampliación del periodo de reserva. ----------

Al respecto, se resolvió lo siguiente:----------

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 3, fracción XIX, 39, y 40, fracción VII, de la LGTAIP; 31, fracción IX, del RIBM; así como Quinta de las Reglas, resolvió aprobar la ampliación del periodo de reserva de la información referida, en términos de la resolución que se agrega a la presente Acta como "**ANEXO 3**". ----------

SEGUNDO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE DESARROLLO E INNOVACIÓN DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia D20-016/2025, de fecha 25 de marzo de 2025, suscrito por quien es titular de la Dirección de Desarrollo e

Innovación de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, el cual se agrega a la presente Acta como "**ANEXO 4**", por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de ampliar el periodo de reserva de la información referida en dicho oficio, de conformidad con la fundamentación y motivación señalada en el mismo, así como en la prueba de daño correspondiente, y solicitó a este Órgano Colegiado aprobar la ampliación del periodo de reserva. ----------

Al respecto, se resolvió lo siguiente:----------

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 3, fracción XIX, 39, y 40, fracción VII, de la LGTAIP; 31, fracción IX, del RIBM; así como Quinta de las Reglas, resolvió aprobar la ampliación del periodo de reserva de la información referida, en términos de la resolución que se agrega a la presente Acta como "**ANEXO 5**". ----------

TERCERO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE DESARROLLO E INNOVACIÓN DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia D20-017/2025, de fecha 25 de marzo de 2025, suscrito por quien es titular de la Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, el cual se agrega a la presente Acta como "**ANEXO 6**", por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de ampliar el periodo de reserva de la información referida en dicho oficio, de conformidad con la fundamentación y motivación señalada en el mismo, así como en la prueba de daño correspondiente, y solicitó a este Órgano Colegiado aprobar la ampliación del periodo de reserva. ----------

Al respecto, se resolvió lo siguiente:----------

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 3, fracción XIX, 39, y 40, fracción VII, de la LGTAIP; 31, fracción IX, del RIBM; así como Quinta de las Reglas, resolvió aprobar la ampliación del periodo de reserva de la información referida, en términos de la resolución que se agrega a la presente Acta como "**ANEXO 7**". ----------

CUARTO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE PROGRAMACIÓN Y DISTRIBUCIÓN DE EFECTIVO DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de fecha 20 de marzo de 2025, suscrito por quien es titular de la Dirección de Programación y Distribución de Efectivo del Banco de México, el cual se agrega a la presente Acta como "**ANEXO 8**", por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de ampliar el periodo de reserva de la información referida en dicho oficio, de conformidad con la fundamentación y motivación señalada en el mismo, así como en la prueba de daño correspondiente, y solicitó a este Órgano Colegiado aprobar la ampliación del periodo de reserva. ----------

Al respecto, se resolvió lo siguiente:----------

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 3, fracción XIX, 39, y 40, fracción VII, de la LGTAIP; 31, fracción IX, del RIBM; así como Quinta de las Reglas, resolvió aprobar la ampliación del periodo de reserva de la información referida, en términos de la resolución que se agrega a la presente Acta como "**ANEXO 9**". ----------

QUINTO. VERSIÓN PÚBLICA ELABORADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de fecha 09 de junio de 2025, suscrito por quien es titular de la Dirección de Infraestructura de Tecnologías de la Información del Banco de México, el cual se agrega a la presente Acta como **"ANEXO 10"**, por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de clasificar la información referida en dicho oficio, de

conformidad con la fundamentación y motivación expresadas en el mismo y en la prueba de daño correspondiente, y solicitó a este Comité de Transparencia confirmar la clasificación referida. ----------
Al respecto, se resolvió lo siguiente:----------
Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 3, fracción XIX, 39, y 40, fracción II, de la LGTAIP; 31, fracción III, del RIBM; así como con la Quinta de las Reglas, resolvió confirmar la clasificación de la información referida en términos de la resolución que se agrega al apéndice de la presente Acta como **"ANEXO 11"**. ----------
Al no haber más asuntos que tratar, se da por terminada la sesión a las doce horas con cuarenta y cinco minutos de la misma fecha de su celebración, y en términos de la Quinta de las Reglas, quien ejerce las funciones de Secretariado en este acto, hace constar el voto de los integrantes del Comité de Transparencia que participaron en la misma a través de medios electrónicos de comunicación, la cual se llevó a cabo en tiempo real, y quienes integraron el quórum no la abandonaron durante su desarrollo. La presente Acta se firma por los integrantes del Comité de Transparencia que participaron en la sesión, así como por quien ejerce en este acto las funciones de Secretariado. Conste. ----------

COMITÉ DE TRANSPARENCIA

_____
JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente
Dirección de Seguridad y Organización de la Información

_____
RODRIGO VILLA COLLINS
Integrante Suplente
Unidad de Transparencia

_____
EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente
Dirección Jurídica

_____
SERGIO ZAMBRANO HERRERA
Secretario

PAJC
NMDS
MDF

Documento firmado digitalmente, su validación requiere hacerse electrónicamente.
Información de las firmas:

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
23/06/2025 09:24:35	SERGIO ZAMBRANO HERRERA	7d3b62e974cb4a958420ae04d5b8ad57476dd76f04bd410c56f179659326fc64
23/06/2025 11:22:06	Rodrigo Villa Collins	22f79c308bd7b28db390d3a5248291e48dbec0facf1123d2bbd81632a7bde28c
23/06/2025 11:55:17	JOSE RAMON RODRIGUEZ MANCILLA	18b9cbba375665321f9a0031c3074e8bbc993c4f742f5b5993b41aa6435e1430
23/06/2025 12:23:45	Edgar Miguel Salas Ortega	521c26788e57f6f19b981b97aa636cd6c204babacc0acbfc5b7ce8990db0f50a

"ANEXO 1"

BANCO DE MÉXICO®

"2025, Año de la Mujer Indígena"

COMITÉ DE TRANSPARENCIA

ORDEN DEL DÍA

ACTA DE LA SESIÓN ESPECIAL 19/2025
DEL 19 DE JUNIO DE 2025

PRIMERO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE DESARROLLO E INNOVACIÓN DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP.

SEGUNDO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE DESARROLLO E INNOVACIÓN DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP.

TERCERO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE DESARROLLO E INNOVACIÓN DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP.

CUARTO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE PROGRAMACIÓN Y DISTRIBUCIÓN DE EFECTIVO DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP.

QUINTO.VERSIÓN PÚBLICA ELABORADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP.

Uso Público
Información de acceso público

"ANEXO 2"

BANCO DE MÉXICO®

Se recibe oficio y prueba de daño . . . . . .
J 15383 25 marzo 2025
12:01

"2025, Año de la mujer indígena"

Ciudad de México, 25 de marzo de 2025
Ref: D20-015/2025

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
P r e s e n t e.

Me refiero a la clasificación de reserva realizada, en su momento, para el cumplimiento de las obligaciones de transparencia señaladas en el Título Quinto de la Ley General de Transparencia y Acceso a la Información Pública por la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados B y la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A, respecto de la información contenida en el documento que se señala a continuación:

TÍTULO DEL DOCUMENTO CLASIFICADO
Contrato suscrito por las partes (Audiencia externa – Contrato no. 0000024208) 800-19-0531-1-CONT-O

Al respecto, me permito resaltar que dicha clasificación fue confirmada por el Comité de Transparencia mediante resolución de 25 de junio de 2020, emitida en la sesión Especial 17/2020, en términos de la fundamentación y motivación expresadas en el oficio de 19 de junio de 2020, suscrito por la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados B y la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A, y en la prueba de daño correspondiente.

Dicha clasificación se realizó por el periodo de 5 años contados a partir de la confirmación de la misma, lo cual ocurrió el 25 de junio de 2020 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **25 de junio de 2025.**

Sobre el particular, con fundamento en los artículos 104, párrafo tercero, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 2o., 3o. y 4o., de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, y tercero, 10, 12 Bis y 20, del Reglamento Interior del Banco de México (RIBM); así como Segundo, fracción XVII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; me permito informarles que esta unidad administrativa **estima que las causas para mantener clasificada como reservada la información referida en el presente oficio subsisten a la fecha, y lo seguirán al menos por los próximos 5 años, contados a partir de la citada fecha de expiración del plazo de reserva,** referida en el párrafo precedente.

Lo anterior, **en términos de la fundamentación y motivación expresadas en la prueba de daño correspondiente, que se pone a disposición de ese Comité de Transparencia.**

Por lo expuesto, y con fundamento en el artículo 104, párrafo tercero, de la LGTAIP, **solicito atentamente a ese Comité de Transparencia confirme la ampliación del plazo de reserva de la**

información referida en el presente oficio, por 5 años más, contados a partir de la fecha de expiración del plazo de reserva respectivo.

Asimismo, informo que el personal que por la naturaleza de sus atribuciones tiene acceso a la referida información clasificada es el adscrito a: Dirección General de Tecnologías de la Información (Director General), Dirección de Infraestructura de Tecnologías de la Información (Director), Gerencia de Cómputo (Gerente), Gerencia de Seguridad de Tecnologías de la Información (Gerente), Gerencia de Telecomunicaciones (Gerente), Subgerencia de Administración de Servicios de Cómputo (Subgerente), Subgerencia del Centro de Defensa de Ciberseguridad (Subgerente), Subgerencia de Planeación y Regulación (Subgerencia), Subgerencia de Seguridad Informática, Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Subgerente, Subgerencia de Administración de Servicios de Telecomunicaciones (Subgerente); el personal adscrito a las Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales, Gerencia de Abastecimiento a Emisión y Recursos Humanos y la Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales; Dirección de Auditoría y la Dirección de Control Interno; asimismo, Dirección General de Sistemas de Pagos e Infraestructuras de Mercados (Director General), Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructura de Mercados (Director), Gerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados (Gerente), Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A (Subgerente), y Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados B (Subgerente).

Atentamente

Ángel Salazar Sotelo
Director de Desarrollo e Innovación de Sistemas
de Pagos e Infraestructuras de Mercados

PRUEBA DE DAÑO

INFORMACIÓN REFERENTE A LA CONTRATACIÓN DE CONSULTORÍAS EN SEGURIDAD INFORMÁTICA REALIZADAS A LOS SISTEMAS DE PAGOS Y APLICACIONES QUE DISEÑA, ADMINISTRA Y OPERA EL BANCO DE MÉXICO, EN SU FUNCIÓN DE PROMOVER EL SANO DESARROLLO DE SISTEMA FINANCIERO Y PROPICIAR EL BUEN FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS.

En términos de lo dispuesto por los artículos 6o., párrafo cuarto, apartado A, fracciones I y VIII, cuarto párrafo, y 28, párrafos séptimo y octavo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM); 112, fracciones IV y VII de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP), es de clasificarse como información reservada aquella cuya publicación pueda:

- Afectar la efectividad de las medidas adoptadas en relación con las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país;
- Poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistemático o del sistema financiero del país;
- Obstruir la prevención de delitos.

Al establecer los parámetros de la información cuya divulgación pueda afectar considerablemente la instrumentación y por ende la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, o que dañe el buen funcionamiento del sistema de pagos, es indispensable identificar los objetivos de protección de la información, por tanto, es preciso dar a conocer los riesgos a los cuales puede estar expuesta la información materia de la prueba de daño.

La Ley del Banco de México, en sus artículos 2o, 3o. y 7o., establece las funciones y los actos que este Instituto Central puede llevar a cabo. Particularmente, en el artículo 2o, prevé, entre otras, que tiene como finalidad promover el sano desarrollo de sistema financiero y el propiciar el buen funcionamiento de los sistemas de pagos.

Los sistemas de pagos, en términos del artículo 2o., fracción VIII, de la Ley de Sistemas de Pagos, son acuerdos o procedimientos que reúnen los requisitos señalados en dicha ley y que tienen por objeto la compensación de órdenes de transferencia o la liquidación de órdenes de transferencia aceptadas donde participen, al menos tres sociedades autorizadas para actuar como instituciones financieras. Asimismo, también son considerados sistemas de pagos aquellos instrumentos, procedimientos y reglas que tienen por objeto la compensación o liquidación de órdenes de transferencia aceptadas, en los que el Banco de México actúe como Administrador del sistema. Del buen funcionamiento de los sistemas de pagos depende la ejecución de las transacciones comerciales y financieras del país como el pago de salarios, cobro de impuestos, adquisición de bienes y servicios, liquidación de operaciones en los mercados financieros y la correcta y oportuna implementación de la política monetaria.

Por lo anterior, al tener el Banco de México, por mandato de Ley, la facultad de promover el sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos, en un mundo globalizado y digital, el ejercicio de estas funciones no puede ser concebida sin el uso de herramientas de tecnologías de la información y comunicaciones eficientes, confiables y seguras; en efecto, la secrecía, sigilo y cuidado de la información que mantiene la estabilidad y buen funcionamiento del sistema financiero, de los sistemas de pagos, y de la economía nacional en su conjunto, debe ser tratada de manera cautelosa. En este tenor, la presente prueba de daño constituye los **límites al principio de máxima publicidad**, misma que permite la

reserva de la información, con la única intención de proteger el **interés público sobre el interés individual de dar a conocer la información motivo de la presente prueba de daño.**

En el caso en concreto, el dar a conocer detalles sobre **información referente a la contratación de consultorías en seguridad informática realizadas a los sistemas de pagos y aplicaciones que diseña, administra y opera el Banco de México en su función de promover el sano desarrollo de sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos**, entre las cuales se advierte la referente a características técnicas, de seguridad informática y de gestión del riesgo operacional, especificaciones generales de los sistemas y aplicaciones e información de códigos fuente; podría disminuir la efectividad de las medidas implementadas en el diseño y programación de los sistemas de pagos y aplicaciones del Banco de México en su función de promover el sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos.

Lo anterior, **toda vez que la divulgación de la información representa un riesgo al interés público,** ya que de revelar o divulgar dicha información posibilitaría la creación de mecanismos que faciliten el acceso indebido a los propios sistemas de pagos y de las aplicaciones desarrolladas, generar vulnerabilidades y riesgos en los propios sistemas, la substracción de información técnica y datos que en ellas se resguardan, lo cual disminuiría la efectividad y eficacia de las medidas implementadas por este Instituto Central en los sistemas de pagos y aplicaciones que diseña, poniendo en riesgo el funcionamiento de dichos sistemas; o bien, podría obstruir la prevención de delitos, por lo que dicha información se clasifica como reservada, toda vez que dicho riesgo es:

1. **Real**, dado que la difusión de esta información posibilita a personas o grupos de ellas con intenciones delincuenciales el identificar de manera directa o a través de técnicas de ingeniería social las especificaciones de seguridad informática, especificaciones técnicas, y, en general, información relacionada con las características técnicas de los sistemas y aplicaciones que diseña el Banco de México, lo cual, posibilitaría la creación de mecanismos que faciliten el acceso indebido al propio sistema de las aplicaciones y en un caso extremo a los sistemas de pagos del propio Banco de México por su conexión directa con este, lo cual, podría menoscabar la efectividad de los mismos a tal grado, que su destrucción o inhabilitación afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero y económico, del país, arriesgando el funcionamiento de esos sistemas y, en consecuencia, de la economía nacional en su conjunto.

   Los riesgos aludidos tienen mayor probabilidad de materializarse con la divulgación de la información citada, debido a que **los delincuentes podrían diseñar estrategias para llevar a cabo ataques** dirigidos específicamente a los sistemas de pagos y de las aplicaciones cuya finalidad en común es la de propiciar el buen funcionamiento de los sistemas de pagos y el sano desarrollo del sistema financiero. Dichos ataques focalizados podrían tener mayor probabilidad de éxito debido a que los delincuentes tendrían la posibilidad de dedicar todos sus recursos a ataques específicos identificados con base en la información específica contenida en los documentos clasificados.

   Incluso, los ataques cibernéticos originados por la divulgación de la información citada, pueden provocar un ataque exitoso, que pondría en riesgo la información que en ellas se almacena, así como alterar, extraer o suprimir la información que se trata, como datos personales referente a sus usuarios, lo cual sería contrario al fin que buscan estas aplicaciones que es promover el sano desarrollo de sistema financiero y al buen funcionamiento de los sistemas de pagos, finalidades que el Banco de México debe llevar acabo de conformidad con las atribuciones establecidas en su Ley. .

Está documentado en la literatura especializada en la materia que **los principales elementos de información que requiere conocer un cibercriminal son: la arquitectura de los sistemas, sus especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad informática instrumentados**, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir en estos elementos y atacar a los sistemas.[1]

En el caso en concreto, la información relacionada con **las contrataciones sobre especificaciones técnicas en materia de seguridad informática, procesos de continuidad operativa, información sobre los componentes de los sistemas informáticos y de los código fuente**, entre otros, por lo que su divulgación proporcionaría elementos de información que **facilitarían a los criminales aprovechar los supuestos puntos débiles** y en consecuencia llevar a cabo ataques más certeros con la finalidad de causar daños o disrupción de servicios, obtener información, o generar ataques que a su vez terminen impactando en la estabilidad del sistema financiero por su relación directa con esta finalidad que tiene encomendada el Banco Central de la nación.

Por lo anterior, mantener clasificada con carácter de reservada la información materia de esta prueba de daño, permite reducir sustancialmente ataques que pudieran resultar efectivos en contra de los sistemas de pagos y aplicaciones del Banco de México.

2. **Demostrable**, ya que es un hecho notorio **que durante los últimos años se ha observado un incremento sostenido de ataques informáticos en el sector financiero a nivel mundial, incluyendo bancos centrales y diversas instituciones financieras.** Las investigaciones realizadas señalan que estos ataques han sido orquestados por organizaciones criminales internacionales con herramientas y técnicas sofisticadas que, además de dañar la reputación de las instituciones afectadas, han generado cuantiosas pérdidas económicas.[2]

   En relación con lo anterior, es importante señalar que **a 2023 México ocupó el primer lugar en ciberataques en Latinoamérica y el cuarto a nivel global**[3] y se encuentra en el en el top 3 de países con más ataques a servicios financieros.[4] Asimismo, **recibió la mayor cantidad de intentos de ciberataques con 187 mil millones**, seguido por Brasil con 103 mil millones de ciberataques, Colombia con 103 mil millones y Perú con 15 mil millones.[5]

   Por otro lado, el Centro de Quejas de Delitos de Internet (IC3, por sus siglas en inglés) manifestó que en 2023 las pérdidas con motivo de las quejas recibidas por delitos en internet, ascendieron a un total de 12.5 Billones de dólares, alrededor del mundo.[6] Por lo anterior, este Instituto Central[7] y

---

[1] Wilshusen, G. C., & Powner, D. A., "Cybersecurity: Continued efforts are needed to protect information systems from evolving threats (No. GA0-10-230T)", GOVERNMENT ACCOUNTABILITY OFFICE WASHINGTON DC, 2009.

[2] Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Congressional Research Service Documents, CRS RL32331 (Washington DC).

[3] Redacción el Heraldo de México, "México ocupa el primer lugar en ciberataques en Latinoamérica y el cuarto a nivel global", El Heraldo, 24 de febrero 2023, disponible en: https://heraldodemexico.com.mx/tecnologia/2023/2/24/mexico-ocupa-el-primer-lugar-en-ciberataques-en-latinoamerica-el-cuarto-nivel-global-484179.html, Consultado el 28 de febrero 2025.

[4] Ramírez, Selene, "México en el top 3 de países con más ataques a servicios financieros", Expansión, 23 agosto 2023, disponible en: https://expansion.mx/tecnologia/2023/08/23/mexico-en-el-top-3-de-paises-con-mas-ataques-a-servicios-financieros#:~:text=A%20nivel%20global%2C%20M%C3%A9xico%20es,el%20mayor%20productor%20de%20malware, Consultado el28 de febrero 2025.

[5] Forninet, "Fortinet informa que América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en 2022", Forninet , 27 de febrero de 2023, Florida, disponible en: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent, consultado el 28 de febrero 2025.

[6] Federal Bureau Investigation (FBI), "2023 Internet Crime Report", Publicado en diciembre de 2023, disponible en: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf, consultado el 28 de febrero 2025.

[7] Banco de México, "Estrategia de Ciberseguridad del Banco de México 2024-2027", 2024, disponible en la siguiente dirección electrónica: https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf, consultado el 28 de febrero 2025.

autoridades como la Secretaría de Hacienda y Crédito Público[8] se han pronunciado sobre la importancia de fortalecer la ciberseguridad para la estabilidad del sistema financiero.

Adicionalmente, se citan algunos de los ataques más relevantes que se han identificado:

i. El ataque que se perpetró contra BANCOMEXT el 9 de enero de 2018 a través de una afectación en su plataforma de pagos internacionales provocada por un tercero. Dicho ataque es similar a intromisiones ocurridas en otras instituciones en México y América Latina.[9]

ii. El intento de degradación de servicio al que fue expuesto el Banco de México en su página principal el 7 de julio del 2020, en el cual se reportó que hubo intermitencias en la página web principal durante aproximadamente 30 minutos. Asimismo, se informó que, los mecanismos y protocolos de protección establecidos por el Banco de México para este tipo de circunstancias evitaron afectaciones a sus procesos en los mercados financieros y sistemas de pagos.[10]

iii. El ataque ocurrido a las instituciones financieras participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI®), el cual consistió en la alteración de sus aplicativos para conectarse a esta IMF, mediante código malicioso, el cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero.[11] A la fecha de publicación del comunicado emitido por Banco de México, se estimó un daño a los participantes del SPEI® de aproximadamente 300 millones de pesos.[12]

iv. El robo de información que sufrió la Secretaría de la Función Pública, entre mayo y junio de 2020, en la que la Secretaría explicó que el grupo de atacantes detectó una vulnerabilidad en la configuración de una base de datos que permitió *"un ataque técnico en el que se accedió a los índices de la base de datos, pudiéndose haberse realizado una copia de la información y se introdujo un aviso de extorsión"*. Asimismo, una investigación reveló que la base de datos, con información de más de 830 mil funcionarios, estuvo disponible en internet, más de un mes.[13]

v. El incidente se seguridad que sufrió la Comisión Nacional de Seguros y Fianzas (CNSF). La organización Bank Security difundió que una persona había puesto a subasta accesos de administración de red y 10 GB de datos confidenciales de la CNSF, esto como consecuencia del ataque denominado "Lockbit", una de las más recientes formas de "ransomware" que los cibercriminales usan para encriptar la información de los sistemas infectados y pedir rescate, y que en caso de no pagarlo extraen la información con el fin de hacerla pública. Posteriormente,

---

[8] Secretaría de Hacienda y Crédito Público, "Fortalecer la ciberseguridad, relevante para el desarrollo de México.", 29 de octubre de 2017, https://www.gob.mx/shcp/prensa/informe-semanal-del-vocero-132251?idiom=es, consultado el 28 de febrero 2025.

[9] BANCOMEXT. "Acción oportuna de BANCOMEXT salvaguarda intereses de clientes y la institución". 10 de enero de 2018. https://www.bancomext.com/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion/, consultado el 28 de febrero 2025.

[10] Banco de México, Comunicado de prensa "El Banco de México informa sobre el estado operativo de su página web", 7 de julio de 2020, disponible en https://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B8A57A6F9-E0F8-969E-202E-64EF6394EBD3%7D.pdf, consultado el 28 de febrero 2025.

[11] Banco de México. "Información sobre los ataques a los Participantes del SPEI", mayo 2018, disponible en: https://www.banxico.org.mx/spei/d/%7BFFC53F5A-CA04-3098-EBF6-B0F17E533183%7D.pdf, consultado el 28 de febrero 2025.

[12] Banco de México, "Puntos importantes sobre la situación actual del SPEI", 22 de mayo de 2018, https://www.banxico.org.mx/spei/d/%7BB806F1E8-686D-B9F1-0452-EC375543C801%7D.pdf, consultado el 28 de febrero 2025.

[13] R3D: Red en Defensa de los Derechos Digitales, "Secretaría de la Función Pública sufrió robo de información; falló en proteger datos personales, alerta el INAI", 16 de diciembre de 2020, disponible en: https://r3d.mx/2020/12/16/secretaria-de-la-funcion-publica-sufrio-robo-de-informacion-fallo-en-proteger-datos-personales-alerta-el-inai/, consultado el 28 de febrero 2025.

el 28 de noviembre del 2020, la CNSF anunció, vía Twitter, que sufrió un ataque cibernético que afectó su continuidad operativa.[14]

vi. El ataque cibernético a los sistemas informáticos de la Secretaría de la Defensa Nacional, mejor conocida como Sedena,[15] realizado por los ciberactivistas Guacamaya, el cual hasta 2022, es el mayor ciberataque en la historia del país porque da a conocer miles de documentos confidenciales del gobierno federal.

vii. La Comisión Nacional Bancaria y de Valores (CNBV), declara que a septiembre de 2024 recibió 15 reportes de incidentes de ciberseguridad por parte de las entidades financieras, la misma cantidad de incidentes que se tuvieron en 2023, no obstante, señalan que es posible que falte información necesaria de los incidentes de seguridad en instituciones bancarias porque, incluso estando obligadas a reportarlos, no informan de manera oportuna sobre los percances de los que son víctimas.[16]

viii. El incidente que afectó el proceso de operaciones con tarjetas de crédito y débito durante el sábado 10 de agosto de 2019, tanto en terminales punto de venta como en cajeros automáticos, el cual se debió a problemas relacionados con la infraestructura eléctrica de la cámara de compensación para pagos que ofrece la empresa privada Promoción y Operación S.A. de C.V. (Prosa), afectando a 25 millones de usuarios.[17]

ix. El incidente de ciberseguridad que experimentó la empresa Coca-Cola FEMSA, por el cual implementó sus protocolos de protección y respuesta de ciberseguridad para evitar un impacto adverso en sus aplicaciones de tecnologías de la información. La empresa comunicó que se encuentra trabajando con expertos en medidas para evitar un impacto adverso en sus aplicaciones de tecnologías de la información.[18]

x. Las fallas presentadas en los servicios financieros proporcionados por Caja Popular Mexicana, S.C. de A.P. de R.L. de C.V., durante el seguimiento la sociedad manifestó a la Comisión Nacional Bancaria y de Valores que las fallas en los servicios financieros se debieron a un incidente de ciberseguridad.[19]

---

[14] Riquelme, Rodrigo, *"Esto es todo lo que sabemos del hackeo a la Comisión Nacional de Seguros y Fianzas"*, El economista, 08 de diciembre de 2020, https://www.eleconomista.com.mx/sectorfinanciero/Esto-es-todo-lo-que-sabemos-del-hackeo-a-la-Comision-Nacional-de-Seguros-y-Fianzas-20201208-0048.html, consultado el 28 de febrero 2025.

[15] Bravo, Jorge, ""Hackeo" a la Sedena y desidia en ciberseguridad", Proceso, octubre 2022, disponible en: https://www.proceso.com.mx/opinion/2022/10/12/hackeo-la-sedena-desidia-en-ciberseguridad-294998.html, consultado el 28 de febrero 2025.

[16] R3D: Red en Defensa de los Derechos Digitales, *"La CNBV señala que las instituciones financieras ocultan incidentes de ciberseguridad"*, 23 de septiembre de 2024, disponible en: https://r3d.mx/2024/09/23/la-cnbv-senala-que-las-instituciones-financieras-ocultan-incidentes-de-ciberseguridad/ consultado el 28 de febrero 2025.

[17] Morales, Yolanda, *"Problemas en infraestructura eléctrica de Prosa provocó los fallos en pagos con tarjetas: Banxico"*, El economista, 13 de agosto de 2019, disponible en: https://www.eleconomista.com.mx/sectorfinanciero/Problemas-en-infraestructura-electrica-de-Prosa-provoco-los-fallos-en-pagos-con-tarjetas-Banxico-20190813-0022.html, consultado el 28 de febrero 2025.

[18] Coca-Cola FEMSA, Coca-*Cola FEMSA Anuncia Incidente de Ciberseguridad*, Ciudad de México, México - 26 de abril de 2023, disponible en: https://www.bmv.com.mx/docs-pub/eventemi/eventemi_1273871_1.pdf, consultado el 28 de febrero 2025.

[19] Comisión Nacional Bancaria y de Valores, *"CNBV realiza seguimiento a Caja Popular Mexicana"*, 22 de julio de 2023, disponible a través de la liga de electrónica: https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/SECTOR-POPULAR/Difusi%C3%B3n/Prensa%20%20Sociedades%20Cooperativas%20de%20Ahorro%20y%20Prstam/Comunicado%20de%20Prensa%2024%20CPM.pdf; y *"CNBV continúa con el seguimiento y vigilancia a Caja Popular Mexicana (CPM)"*, con fecha del 31 de agosto de 2023, disponible a través de la liga de electrónica: https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/SECTOR-POPULAR/Difusi%C3%B3n/Prensa%20%20Sociedades%20Cooperativas%20de%20Ahorro%20y%20Prstam/Comunicado%20de%20Prensa%2029%20CNBV%20contin%C3%BAa%20con%20el%20seguimiento%20y%20vigilancia%20a%20CPM.-2.pdf, consultado el 28 de febrero 2025.

xi. El incidente de ciberseguridad al Fondo Monetario Internacional detectado el 16 de febrero de 2024 en el cual manifestaron que se vieron comprometidas once cuentas de correo electrónico de dicho organismo.[20]

xii. La Presidencia de la República del Gobierno de México informó sobre el ingreso no autorizado a un archivo que contenía información parcial de periodistas acreditados de la fuente presidencial, viéndose afectados 263 periodistas de los cuales existían datos personales en su conjunto, es decir, 168 credenciales de elector que tenían domicilio completo, 63 pasaportes, uno más, ilegible; dos currículums; una licencia de conducir de Estados Unidos; una Clave Única de Registro de Población y 10 documentos expedidos por el Instituto Nacional de Migración; hay cuatro personas de las que sólo aparece su fotografía, sin ningún dato más.[21]

xiii. Grupo Coppel reportó un incidente de ciberseguridad que generó fallas en sus sistemas el lunes 15 de abril de 2024, cuando sus clientes reportaron que no podían ingresar a su página web para realizar diversos trámites.[22]

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[23] consideran que la obtención de información técnica de especificaciones, es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

Inclusive, uno de los modus operandi de los ciberataques es precisamente a través de la obtención de **información pública**, información fácilmente accesible o información inaccesible, lo cual puede ocurrir mediante solicitudes de acceso a la información, o bien, a través de las organizaciones que operan o tienen acceso a los sistemas, en complicidad o no, con el único objeto de **conocer las vulnerabilidades en las instituciones, empresas, sistemas e infraestructura de tecnologías de la información.**[24]

Por otro lado, es de destacar que **los cibercriminales han utilizado técnicas de ingeniería social para obtener información y con ello acceder o vulnerar incluso los sistemas más seguros**. Una de las formas más comunes de vulnerar los sistemas es mediante la obtención de información a través de diversas fuentes y mecanismos que les permita diseñar ataques informáticos encaminados a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros elementos, con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes. Las corporaciones multinacionales y las agencias de noticias han

---

[20] Fondo Monetario Internacional, *"El FMI investiga un incidente de ciberseguridad"*, 15 de marzo de 2024, disponible a través de la liga electrónica: https://www.imf.org/es/News/Articles/2024/03/15/pr2488-imf-investigates-cyber-security-incident, consultado el 28 de febrero 2025.

[21] Presidencia de la República, *"Gobierno de México denunciará ante FGR por sustracción ilegal externa de datos de periodistas"*. 29 de enero de 2024, disponible a través de la liga electrónica: https://www.gob.mx/segob/prensa/gobierno-de-mexico-denunciara-ante-fgr-por-sustraccion-ilegal-externa-de-datos-de-periodistas-356608?state=published#:~:text=El%20subsecretario%20de%20Derechos%20Humanos,localicen%20a%20quienes%20resulten%20responsables, consultado el 28 de febrero 2025.

[22] Redacción El Economista, *"Coppel reporta incidente de ciberseguridad en sus sistemas; garantiza protección de datos de sus clientes"*, El Economista, 20 de abril de 2024, disponible a través de la liga electrónica: https://www.eleconomista.com.mx/sectorfinanciero/Coppel-reporta-incidente-de-ciberseguridad-en-sus-sistemas-garantiza-proteccion-de-datos-de-sus-clientes-20240420-0015.html, consulado el 28 de febrero 2025.

[23] Offensive Security, INFORMATION GATHERING IN METASPLOIT, disponible en: https://www.offensive-security.com/metasploit-unleashed/information-gathering/, consultado el 28 de febrero 2025.

[24] El Economista, *El sistema financiero mexicano fue víctima de una campaña de ciberataques*, 15 de mayo de 2018. https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html consultado el 28 de febrero 2025.

sido víctimas de sofisticados ataques dirigidos contra sus sistemas de información derivado de la aplicación de técnicas de ingeniería social.[25]

Por lo anterior, **los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuyo rol no esté autorizado,**[26] en el entendido de que dicha información, al estar en posesión de personas no autorizadas, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central de la nación, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

3. **Identificable**, puesto que, a la fecha de realización de la presente prueba de daño, es un hecho notorio que el sector financiero a nivel mundial, incluyendo bancos centrales y diversas instituciones financieras, están siendo objeto de ciberataques dirigidos a vulnerar sistemas que resguardan información, incluso información personal, como quedó demostrado en la sección anterior. Si bien dichos ataques no han logrado irrumpir en los sistemas del Banco de México, resulta claramente que se debe de prever la protección de la información.

   En ese sentido, **un ataque informático derivado de divulgar la información materia de la presente prueba de daño, podría resultar en la vulneración o sustracción de la información de los sistemas de pagos y aplicaciones diseñadas por el Banco de México en su función de promover el sano desarrollo del sistema financiero.**

   Adicionalmente, una disrupción en los servicios provistos por los sistemas de pagos o de sus participantes, producto de un ataque contra estos o sus tecnologías de la información y de comunicaciones, tendría repercusiones directas para **una gran cantidad de empresas y comercios,** cuyas obligaciones a cubrir a través de pagos electrónicos interbancarios se verían afectadas durante el tiempo de la interrupción de estos servicios. Asimismo, **la población en general** que utiliza estos medios de pago, vería afectada su capacidad para realizar o cumplir con el pago de bienes y servicios, y **las instituciones bancarias y no bancarias participantes de los sistemas de pagos**, que obtienen parte de sus ingresos del cobro de comisiones por la prestación del servicio de pagos a través de estos, también resultarían gravemente perjudicadas, lo cual provocaría una seria afectación al sistema financiero. Finalmente, **las personas que reciben pagos del Gobierno Federal** mismos que son dispersados por este Instituto Central en su carácter de Agente Financiero de la Tesorería de la Federación, se verían seriamente comprometidos.

Por lo anterior, es posible identificar que **el riesgo de perjuicio que supondría la divulgación de la información materia de esta prueba de daño, supera el interés público general de que se difunda,** pues el interés público se centra en que no se comprometa la efectividad en las medidas implementadas en los sistemas financiero y económico, que propician el buen funcionamiento de esos sistemas y del sistema financiero. Por lo que, **la información, no satisface un interés público, por el contrario, es información que pone en riesgo las medidas**

---

[25] Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, 18 de diciembre de 2001., disponible en: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=891b1f29-e2e7-4484-89c0-a2137ee82f8b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments, consultado el 28 de febrero 2025.

[26] Ver por ejemplo las 10 medidas básicas de ciberseguridad de la Security Information Center, en particular la relacionada con "Implementar un programa de capacitación en seguridad cibernética para empleados "en donde recomiendan sensibilizar sobre los temas de ingeniería social que buscan obtener información mediante diversos canales de comunicación solicitando información sensible. https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_0.pdf, consultado el 28 de febrero 2025.

implementadas por este Instituto Central para la efectividad del sistema financiero. Asimismo, al realizar una interpretación sobre la alternativa que más satisface dicho interés, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México, los sistemas administrados y las aplicaciones implementadas por éste.

En consecuencia, **proporcionar la información en cuestión, no aporta un beneficio mayor a la transparencia y rendición de cuentas que sea comparable con el perjuicio que implicaría el hecho de divulgarla**, esto es, que permita planear y perpetrar ataques dirigidos específicamente a los sistemas de pagos administrados, operados y supervisados por el Banco de México y a sus aplicaciones, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información - como datos personales referente a sus usuarios y las operaciones que realizan -, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción en éstos.

Adicionalmente, **el riesgo de perjuicio que supondría la divulgación de la información, supera el interés público general de que se difunda,** ya que dar a conocer ***información referente a la contratación de consultorías en seguridad informática realizadas a los sistemas de pagos y aplicaciones que diseña, administra y opera el Banco de México en su función de promover el sano desarrollo de sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos,*** no aporta un beneficio a la transparencia que sea comparable con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento o dejar inoperantes a los sistemas.

Al respecto, debe destacarse que la información materia de la presente prueba de daño no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, **beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México las cuales, entre otras, se advierten la de promover el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.**

Por otra parte, **la limitación se adecua al principio de proporcionalidad, toda vez que** debe prevalecer el interés que más beneficie a la colectividad, y como se ha dicho, proteger la información materia de la presente prueba de daño **evitará poner en riesgo el buen funcionamiento de los sistemas de pagos del sistema financiero y de la economía nacional en su conjunto.**

En razón de lo anterior, y vistas las consideraciones expuestas en la presente prueba de daño, se solicita la reserva de dicha información, por el **plazo de 5 años más, contados a partir de la fecha de vencimiento del actual plazo de reserva**, en virtud de que esta acción atiende a la protección de las medidas de seguridad informática y especificaciones técnicas con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de pagos y las aplicaciones diseñadas por el Banco de México, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos.

En consecuencia, con fundamento en lo establecido en los artículos 6o., párrafo cuarto, apartado A, fracciones I y VIII, párrafo cuarto, y 28, párrafos séptimo y octavo, de la CPEUM; 1, 102, 103, 104, párrafo tercero, 106, 107, 108, 109, 112, fracciones IV y VII, y 113 de la LGTAIP; 1o., 2o. y 3o., fracción I, de la Ley del Banco de México; así como 4o., párrafo primero, 8o., párrafos primero, y tercero, 10, párrafo primero, del Reglamento Interior del Banco de México, es de clasificarse como reservada la ***información referente a la contratación de consultorías en seguridad informática realizadas a los sistemas de pagos y aplicaciones que diseña, administra y opera el Banco de México en su función de promover el sano desarrollo de sistema financiero***

y propiciar el buen funcionamiento de los sistemas de pagos, toda vez que, como se ha manifestado, la divulgación de dicha información menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto; así como se vería obstruida la prevención de delitos en la materia.

"ANEXO 3"

BANCO DE MÉXICO®

"2025, Año de la Mujer Indígena"

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DEL PERIODO DE RESERVA

VISTOS, para resolver sobre la ampliación del periodo de reserva de información determinada por la unidad administrativa solicitante, y:

RESULTANDO

I. Que, con la finalidad de cumplir con las obligaciones de transparencia comunes, los sujetos obligados pondrán a disposición del público, en sus respectivos medios electrónicos y en la Plataforma Nacional de Transparencia, de acuerdo con sus facultades, atribuciones, funciones u objeto social, la información de los temas, documentos y políticas que se señalan en el artículo 65 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

II. Que, del análisis realizado a la información que en su momento fue clasificada como reservada, se han puesto a consideración de este Órgano Colegiado los motivos y fundamentos para ampliar el periodo de reserva próximo a concluir.

III. Que considerando lo anterior, se solicitó al Comité de Transparencia aprobar la ampliación del plazo de reserva de la información, como se indica enseguida:

FECHA O REFERENCIA DEL OFICIO	UNIDAD(ES) ADMINISTRATIVA(S) SOLICITANTE(S) Y NOMBRE(S) DE SU(S) TITULAR(ES)	SOLICITUD DEL OFICIO	INFORMACIÓN CLASIFICADA	PLAZO DE CLASIFICACIÓN
Oficio con referencia: D20-015/2025, de fecha 25 de marzo de 2025.	Ángel Salazar Sotelo (Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México).	Ampliación del plazo de reserva de la información referida en el citado oficio.	**Información reservada** en términos de lo señalado en el oficio y en la prueba de daño correspondiente. *"INFORMACIÓN REFERENTE A LA CONTRATACIÓN DE CONSULTORÍAS EN SEGURIDAD INFORMÁTICA REALIZADAS A LOS SISTEMAS DE PAGOS Y APLICACIONES QUE DISEÑA, ADMINISTRA Y OPERA EL BANCO DE MÉXICO, EN SU FUNCIÓN DE PROMOVER EL SANO DESARROLLO DE SISTEMA FINANCIERO Y PROPICIAR EL BUEN FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS."*	**Plazo de reserva inicial:** 5 años, a partir del 25 de junio de 2020. **Plazo de reserva con ampliación:** 5 años, a partir del 26 de junio de 2025.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva de la información que soliciten las personas titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 40, fracción VII, y 104, párrafo tercero, de la LGTAIP; así como 31, fracción IX, del Reglamento Interior del Banco de México (RIBM).

SEGUNDO. Este Comité de Transparencia, tomando en cuenta que en términos del artículo 106, párrafo segundo, de la LGTAIP, advierte que las razones, motivos y circunstancias especiales que llevaron a concluir que en el caso particular se actualiza la necesidad de ampliar el periodo de reserva de la información señalada, se contienen en el oficio referido en el resultando III, así como en la prueba de daño correspondiente, los cuales se tienen aquí por reproducidos como si a la letra se insertasen.[1]

Al respecto, de conformidad con lo expresado en el oficio señalado en el resultando III, se llevó a cabo una debida ponderación de los intereses en conflicto y se acreditó que el riesgo de perjuicio rebasa el interés público; se acreditó también el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trata; se precisaron las razones por las que la divulgación de la información generaría una afectación a través de los elementos de un riesgo real, demostrable e identificable; y se acreditaron las circunstancias de modo, tiempo y lugar del daño.

En consecuencia, y considerando que, conforme a lo manifestado en la prueba de daño respectiva, la divulgación de la información correspondiente representa un riesgo al interés público, ya que: *"(…) posibilitaría la creación de mecanismos que faciliten el acceso indebido a los propios sistemas de pagos y de las aplicaciones desarrolladas, generar vulnerabilidades y riesgos en los propios sistemas, la substracción de información técnica y datos que en ellas se resguardan, lo cual disminuiría la efectividad y eficacia de las medidas implementadas por este Instituto Central en los sistemas de pagos y aplicaciones que diseña, poniendo en riesgo el funcionamiento de dichos sistemas; o bien, podría obstruir la prevención de delitos (…)"*, **este Comité de Transparencia aprueba la ampliación al periodo de reserva de la información señalada** de conformidad con lo expresado en el oficio citado en el resultando III de la presente determinación, así como en términos de la prueba de daño correspondiente, **y toma conocimiento del nuevo plazo de reserva determinado por la unidad administrativa.**

Por lo expuesto con fundamento en los artículos 40, fracción VII, y 104, párrafo tercero, de la LGTAIP; así como 31, fracción IX, del RIBM; y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este Órgano Colegiado:

RESUELVE

ÚNICO. Se aprueba la ampliación al periodo de reserva de la información clasificada como reservada señalada en el oficio mencionado en el resultando III de la presente determinación, conforme a la fundamentación y motivación expresadas en el mismo, así como en la prueba de daño correspondiente, en términos del considerando Segundo de la presente resolución.

[1] Sirven de referencia los principios de elaboración de sentencias en materia civil, contenidos en la tesis *"SENTENCIA. CUANDO EL JUEZ CITA UNA TESIS PARA FUNDARLA, HACE SUYOS LOS ARGUMENTOS CONTENIDOS EN ELLA. Cuando en una sentencia se cita y transcribe un precedente o una tesis de jurisprudencia, como apoyo de lo que se está resolviendo, el Juez propiamente hace suyos los argumentos de esa tesis que resultan aplicables al caso que se resuelve, sin que se requiera que lo explicite, pues resulta obvio que al fundarse en la tesis recoge los diversos argumentos contenidos en ella."* (Suprema Corte de Justicia de la Nación; Registro digital: 192898; Instancia: Pleno; Novena Época; Materias(s): Común; Tesis: P./J. 126/99; Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo X, Noviembre de 1999, página 35; Tipo: Jurisprudencia).

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en sesión celebrada el 19 de junio de 2025.----------

COMITÉ DE TRANSPARENCIA

_____

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente
Dirección de Seguridad y Organización de la Información

_____

RODRIGO VILLA COLLINS
Integrante Suplente
Unidad de Transparencia

_____

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente
Dirección Jurídica

AMR
URD
MDF

Documento firmado digitalmente, su validación requiere hacerse electrónicamente.
Información de las firmas:

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
23/06/2025 11:22:08	Rodrigo Villa Collins	41c3c5231f8d6dc6b6d351ee71d70c358c038b6f5cd7521e85abe7ac70631dd1
23/06/2025 11:55:20	JOSE RAMON RODRIGUEZ MANCILLA	370133f3c9db9c4b51980a1e68c4685f0c29ad4b566e91d189534b2b60175409
23/06/2025 12:23:32	Edgar Miguel Salas Ortega	824a23b5b9e98cd8b357169f7dd8702b021176a0b577979ea9a40cec13f7d39b

"ANEXO 4"

BANCO DE MÉXICO®

"2025, Año de la mujer indígena"

Se recibe oficio y prueba de daño
715383 25 marzo 2025
12:03

Ciudad de México, 25 de marzo de 2025
Ref: D20-016/2025

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
P r e s e n t e.

Me refiero a la clasificación de reserva realizada, en su momento, para el cumplimiento de las obligaciones de transparencia señaladas en el Título Quinto de la Ley General de Transparencia y Acceso a la Información Pública por la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados B y la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A, respecto de la totalidad de la información contenida en el documento que se señala a continuación:

TÍTULO DEL DOCUMENTO CLASIFICADO
Resultado de la contratación: 800-19-0531-1-CONT-O

Al respecto, me permito resaltar que dicha clasificación fue confirmada por el Comité de Transparencia mediante resolución de 25 de junio de 2020, emitida en la sesión Especial 17/2020, en términos de la fundamentación y motivación expresadas en el oficio de 19 de junio de 2020, suscrito por la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados B y la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A, y en la prueba de daño correspondiente.

Dicha clasificación se realizó por el periodo de 5 años contados a partir de la confirmación de la misma, lo cual ocurrió el 25 de junio de 2020 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **25 de junio de 2025.**

Sobre el particular, con fundamento en los artículos 104, párrafo tercero, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 2o., 3o. y 4o., de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, y tercero, 10, 12 Bis y 20, del Reglamento Interior del Banco de México (RIBM); así como Segundo, fracción XVII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; me permito informarles que esta unidad administrativa **estima que las causas para mantener clasificada como reservada la información referida en el presente oficio subsisten a la fecha, y lo seguirán al menos por los próximos 5 años, contados a partir de la citada fecha de expiración del plazo de reserva,** referida en el párrafo precedente.

Lo anterior, **en términos de la fundamentación y motivación expresadas en la prueba de daño correspondiente, que se pone a disposición de ese Comité de Transparencia.**

Por lo expuesto, y con fundamento en los artículos 104, párrafo tercero, de la LGTAIP, **solicito atentamente a ese Comité de Transparencia confirme la ampliación del plazo de reserva de la**

información referida en el presente oficio, por 5 años más, contados a partir de la fecha de expiración del plazo de reserva respectivo.

Asimismo, informo que el personal que por la naturaleza de sus atribuciones tiene acceso a la referida información clasificada es el adscrito a: Dirección General de Tecnologías de la Información (Director General), Dirección de Infraestructura de Tecnologías de la Información (Director), Gerencia de Cómputo (Gerente), Gerencia de Seguridad de Tecnologías de la Información (Gerente), Gerencia de Telecomunicaciones (Gerente), Subgerencia de Administración de Servicios de Cómputo (Subgerente), Subgerencia del Centro de Defensa de Ciberseguridad (Subgerente), Subgerencia de Planeación y Regulación (Subgerente), Subgerencia de Seguridad Informática (Subgerente), Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Subgerente), Subgerencia de Administración de Servicios de Telecomunicaciones (Subgerente); el personal adscrito a las Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales, Gerencia de Abastecimiento a Emisión y Recursos Humanos y la Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales; Dirección de Auditoría y la Dirección de Control Interno; asimismo, Dirección General de Sistemas de Pagos e Infraestructuras de Mercados (Director General), Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructura de Mercados (Director), Gerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados (Gerente), Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A (Subgerente), y Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados B (Subgerente).

Atentamente

Ángel Salazar Sotelo
Director de Desarrollo e Innovación de Sistemas
de Pagos e Infraestructuras de Mercados

PRUEBA DE DAÑO

INFORMACIÓN REFERENTE A LOS RESULTADOS DE CONSULTORÍAS EN SEGURIDAD INFORMÁTICA REALIZADAS A LOS SISTEMAS DE PAGOS Y/O APLICACIONES QUE DISEÑA, ADMINISTRA Y OPERA EL BANCO DE MÉXICO, EN SU FUNCIÓN DE PROMOVER EL SANO DESARROLLO DE SISTEMA FINANCIERO Y PROPICIAR EL BUEN FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS.

En términos de lo dispuesto por los artículos 6o., párrafo cuarto, apartado A, fracciones I y VIII, cuarto párrafo, 28, párrafos séptimo y octavo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM); así como 112, fracciones IV y VII de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); es de clasificarse como información reservada aquella cuya publicación pueda:

- Menoscabar la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país.
- Comprometer la seguridad en la provisión de moneda nacional al país.
- Obstruir la prevención de delitos.

Al establecer los parámetros de la información cuya divulgación pueda afectar considerablemente la instrumentación y por ende la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, y dañar el buen funcionamiento del sistema de pagos, es indispensable identificar los objetivos de protección de la información, por tanto, es preciso dar a conocer los riesgos a los cuales puede estar expuesta la información materia de la prueba de daño.

La Ley del Banco de México, en sus artículos 2o, 3o. y 7o., establece las funciones y los actos que este Instituto Central puede llevar a cabo. Particularmente, en el artículo 2o, prevé, entre otras, que tiene como finalidad promover el sano desarrollo de sistema financiero y el propiciar el buen funcionamiento de los sistemas de pagos.

Los sistemas de pagos, en términos del artículo 2o., fracción VIII, de la Ley de Sistemas de Pagos, son acuerdos o procedimientos que reúnen los requisitos señalados en dicha ley y que tienen por objeto la compensación de órdenes de transferencia o la liquidación de órdenes de transferencia aceptadas donde participen, al menos tres sociedades autorizadas para actuar como instituciones financieras. Asimismo, también son considerados sistemas de pagos aquellos instrumentos, procedimientos y reglas que tienen por objeto la compensación o liquidación de órdenes de transferencia aceptadas, en los que el Banco de México actúe como Administrador del sistema. Del buen funcionamiento de los sistemas de pagos depende la ejecución de las transacciones comerciales y financieras del país como el pago de salarios, cobro de impuestos, adquisición de bienes y servicios, liquidación de operaciones en los mercados financieros y la correcta y oportuna implementación de la política monetaria.

Por lo anterior, al tener el Banco de México, por mandato de Ley, la facultad de promover el sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos, en un mundo globalizado y digital, el ejercicio de estas funciones no puede ser concebida sin el uso de herramientas de tecnologías de la información y comunicaciones eficientes, confiables y seguras; en efecto, la secrecía, sigilo y cuidado de la información que mantiene la estabilidad y buen funcionamiento del sistema financiero, de los sistemas de pagos, y de la economía nacional en su conjunto, debe ser tratada de manera cautelosa. En este tenor, la presente prueba de daño constituye los **límites al principio de máxima publicidad**, misma que permite la

reserva de la información, con la única intención de proteger el **interés público sobre el interés individual de dar a conocer la información motivo de la presente prueba de daño.**

En el caso en concreto, el dar a conocer detalles sobre **información referente a los resultados de consultorías en seguridad informática realizadas a los sistemas de pagos y/o aplicaciones que diseña, administra y opera el Banco de México en su función de promover el sano desarrollo de sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos**, entre las cuales se advierte la referente a características técnicas, de seguridad informática y de gestión del riesgo operacional, especificaciones generales de los sistemas y aplicaciones e información de protección y seguridad de códigos fuente para evitar vulnerabilidades y emitir sugerencias para evitar riesgos de ataques; podría disminuir la efectividad de las medidas implementadas en el diseño y programación de los sistemas de pagos y aplicaciones del Banco de México en su función de promover el sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos.

Lo anterior, **toda vez que la divulgación de la información representa un riesgo al interés público,** ya que de revelar o divulgar dicha información posibilitaría la creación de mecanismos que faciliten el acceso indebido a los propios sistemas de pagos y de las aplicaciones desarrolladas, generar vulnerabilidades y riesgos en los propios sistemas, la substracción de información técnica y datos que en ellas se resguardan, lo cual disminuiría la efectividad y eficacia de las medidas implementadas por este Instituto Central en los sistemas de pagos y aplicaciones que diseña, poniendo en riesgo el funcionamiento de dichos sistemas; o bien, podría obstruir la prevención de delitos, por lo que dicha información se clasifica como reservada, toda vez que dicho riesgo es:

1. **Real,** dado que la difusión de esta información posibilita a personas o grupos de ellas con intenciones delincuenciales el identificar de manera directa o a través de técnicas de ingeniería social las especificaciones de seguridad informática, especificaciones técnicas, y, en general, información relacionada con las características técnicas de los sistemas y aplicaciones que diseña el Banco de México, lo cual, posibilitaría la creación de mecanismos que faciliten el acceso indebido al propio sistema de las aplicaciones y en un caso extremo a los sistemas de pagos del propio Banco de México por su conexión directa con este, lo cual, podría menoscabar la efectividad de los mismos a tal grado, que su destrucción o inhabilitación afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero y económico, del país, arriesgando el funcionamiento de esos sistemas y, en consecuencia, de la economía nacional en su conjunto.

   Los riesgos aludidos tienen mayor probabilidad de materializarse con la divulgación de la información citada, debido a que **los delincuentes podrían diseñar estrategias para llevar a cabo ataques** dirigidos específicamente a los sistemas de pagos y de las aplicaciones cuya finalidad en común es la de propiciar el buen funcionamiento de los sistemas de pagos y el sano desarrollo del sistema financiero. Dichos ataques focalizados podrían tener mayor probabilidad de éxito debido a que los delincuentes tendrían la posibilidad de dedicar todos sus recursos a ataques específicos identificados con base en la información específica contenida en los documentos clasificados.

   Incluso, los ataques originados por la divulgación de la información citada, pueden provocar un ataque exitoso, que pondría en riesgo la información que en ellas se almacena, así como alterar, extraer o suprimir la información que se trata, como datos personales referente a sus usuarios, lo cual sería contrario al fin que buscan estas aplicaciones que es promover el sano desarrollo de sistema financiero y al buen funcionamiento de los sistemas de pagos, finalidades que el Banco de México debe llevar acabo de conformidad con las atribuciones establecidas en su Ley.

Está documentado en la literatura especializada en la materia que **los principales elementos de información que requiere conocer un cibercriminal son: la arquitectura de los sistemas, sus especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad informática instrumentados**, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir en estos elementos y atacar a los sistemas.[1]

En el caso en concreto, la información relacionada con la divulgación de **los resultados de las contrataciones sobre especificaciones técnicas en materia de seguridad informática, procesos de continuidad operativa, información sobre los componentes de los sistemas informáticos, recomendaciones para evitar vulnerabilidades y ataques**, entre otros, proporcionaría elementos de información que **facilitarían a los criminales aprovechar los supuestos puntos débiles** y en consecuencia llevar a cabo ataques más certeros con la finalidad de causar daños o disrupción de servicios, obtener información, o generar ataques que a su vez terminen impactando en la estabilidad del sistema financiero por su relación directa con esta finalidad que tiene encomendada el Banco Central de la nación.

Por lo anterior, mantener clasificada con carácter de reservada la información materia de esta prueba de daño, permite reducir sustancialmente ataques que pudieran resultar efectivos en contra de los sistemas de pagos y aplicaciones del Banco de México.

2. **Demostrable**, ya que es un hecho notorio **que durante los últimos años se ha observado un incremento sostenido de ataques informáticos en el sector financiero a nivel mundial, incluyendo bancos centrales y diversas instituciones financieras.** Las investigaciones realizadas señalan que estos ataques han sido orquestados por organizaciones criminales internacionales con herramientas y técnicas sofisticadas que, además de dañar la reputación de las instituciones afectadas, han generado cuantiosas pérdidas económicas.[2]

   En relación con lo anterior, es importante señalar que **a 2023 México ocupó el primer lugar en ciberataques en Latinoamérica y el cuarto a nivel global**[3] y se encuentra en el en el top 3 de países con más ataques a servicios financieros.[4] Asimismo, **recibió la mayor cantidad de intentos de ciberataques con 187 mil millones**, seguido por Brasil con 103 mil millones de ciberataques, Colombia con 103 mil millones y Perú con 15 mil millones.[5]

   Por otro lado, el Centro de Quejas de Delitos de Internet (IC3, por sus siglas en inglés) manifestó que en 2023 las pérdidas con motivo de las quejas recibidas por delitos en internet, ascendieron a un

---

[1] Wilshusen, G. C., & Powner, D. A., "Cybersecurity: Continued efforts are needed to protect information systems from evolving threats (No. GA0-10-230T)", GOVERNMENT ACCOUNTABILITY OFFICE WASHINGTON DC, 2009.

[2] Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Congressional Research Service Documents, CRS RL32331 (Washington DC).

[3] Redacción el Heraldo de México, "México ocupa el primer lugar en ciberataques en Latinoamérica y el cuarto a nivel global", El Heraldo, 24 de febrero 2023, disponible en: https://heraldodemexico.com.mx/tecnologia/2023/2/24/mexico-ocupa-el-primer-lugar-en-ciberataques-en-latinoamerica-el-cuarto-nivel-global-484179.html, Consultado el 28 de febrero 2025.

[4] Ramírez, Selene, "México en el top 3 de países con más ataques a servicios financieros", Expansión, 23 agosto 2023, disponible en: https://expansion.mx/tecnologia/2023/08/23/mexico-en-el-top-3-de-paises-con-mas-ataques-a-servicios-financieros#:~:text=A%20nivel%20global%2C%20M%C3%A9xico%20es,el%20mayor%20productor%20de%20malware, Consultado el28 de febrero 2025.

[5] Forninet, "Fortinet informa que América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en 2022", Forninet , 27 de febrero de 2023, Florida, disponible en: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent, consultado el 28 de febrero 2025.

total de 12.5 Billones de dólares, alrededor del mundo.[6] Por lo anterior, este Instituto Central[7] y autoridades como la Secretaría de Hacienda y Crédito Público[8] se han pronunciado sobre la importancia de fortalecer la ciberseguridad para la estabilidad del sistema financiero.

Adicionalmente, se citan algunos de los ataques más relevantes que se han identificado:

i. El ataque que se perpetró contra BANCOMEXT el 9 de enero de 2018 a través de una afectación en su plataforma de pagos internacionales provocada por un tercero. Dicho ataque es similar a intromisiones ocurridas en otras instituciones en México y América Latina.[9]

ii. El intento de degradación de servicio al que fue expuesto el Banco de México en su página principal el 7 de julio del 2020, en el cual se reportó que hubo intermitencias en la página web principal durante aproximadamente 30 minutos. Asimismo, se informó que, los mecanismos y protocolos de protección establecidos por el Banco de México para este tipo de circunstancias evitaron afectaciones a sus procesos en los mercados financieros y sistemas de pagos.[10]

iii. El ataque ocurrido a las instituciones financieras participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI®), el cual consistió en la alteración de sus aplicativos para conectarse a esta IMF, mediante código malicioso, el cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero.[11] A la fecha de publicación del comunicado emitido por Banco de México, se estimó un daño a los participantes del SPEI® de aproximadamente 300 millones de pesos.[12]

iv. El robo de información que sufrió la entonces Secretaría de la Función Pública, entre mayo y junio de 2020, en la que la Secretaría explicó que el grupo de atacantes detectó una vulnerabilidad en la configuración de una base de datos que permitió *"un ataque técnico en el que se accedió a los índices de la base de datos, pudiéndose haberse realizado una copia de la información y se introdujo un aviso de extorsión"*. Asimismo, una investigación reveló que la base de datos, con información de más de 830 mil funcionarios, estuvo disponible en internet, más de un mes.[13]

v. El incidente se seguridad que sufrió la Comisión Nacional de Seguros y Fianzas (CNSF). La organización Bank Security difundió que una persona había puesto a subasta accesos de

---

[6] Federal Bureau Investigation (FBI), "2023 Internet Crime Report", Publicado en diciembre de 2023, disponible en: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf, consultado el 28 de febrero 2025.

[7] Banco de México, "Estrategia de Ciberseguridad del Banco de México 2024-2027", 2024, disponible en la siguiente dirección electrónica: https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf, consultado el 28 de febrero 2025.

[8] Secretaría de Hacienda y Crédito Público, "Fortalecer la ciberseguridad, relevante para el desarrollo de México.", 29 de octubre de 2017, https://www.gob.mx/shcp/prensa/informe-semanal-del-vocero-132251?idiom=es, consultado el 28 de febrero 2025.

[9] BANCOMEXT. "Acción oportuna de BANCOMEXT salvaguarda intereses de clientes y la institución". 10 de enero de 2018. https://www.bancomext.com/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion/, consultado el 28 de febrero 2025.

[10] Banco de México, Comunicado de prensa "El Banco de México informa sobre el estado operativo de su página web", 7 de julio de 2020, disponible en https://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B8A57A6F9-E0F8-969E-202E-64EF6394EBD3%7D.pdf, consultado el 28 de febrero 2025.

[11] Banco de México. "Información sobre los ataques a los Participantes del SPEI", mayo 2018, disponible en: https://www.banxico.org.mx/spei/d/%7BFFC53F5A-CA04-3098-EBF6-B0F17E533183%7D.pdf, consultado el 28 de febrero 2025.

[12] Banco de México, "Puntos importantes sobre la situación actual del SPEI", 22 de mayo de 2018, https://www.banxico.org.mx/spei/d/%7BB806F1E8-686D-B9F1-0452-EC375543C801%7D.pdf, consultado el 28 de febrero 2025.

[13] R3D: Red en Defensa de los Derechos Digitales, "Secretaría de la Función Pública sufrió robo de información; falló en proteger datos personales, alerta el INAI", 16 de diciembre de 2020, disponible en: https://r3d.mx/2020/12/16/secretaria-de-la-funcion-publica-sufrio-robo-de-informacion-fallo-en-proteger-datos-personales-alerta-el-inai/, consultado el 28 de febrero 2025.

administración de red y 10 GB de datos confidenciales de la CNSF, esto como consecuencia del ataque denominado "Lockbit", una de las más recientes formas de "ransomware" que los cibercriminales usan para encriptar la información de los sistemas infectados y pedir rescate, y que en caso de no pagarlo extraen la información con el fin de hacerla pública. Posteriormente, el 28 de noviembre del 2020, la CNSF anunció, vía Twitter, que sufrió un ataque cibernético que afectó su continuidad operativa.[14]

vi. El ataque cibernético a los sistemas informáticos de la Secretaría de la Defensa Nacional, mejor conocida como Sedena,[15] realizado por los ciberactivistas Guacamaya, el cual hasta 2022, es el mayor ciberataque en la historia del país porque da a conocer miles de documentos confidenciales del gobierno federal. De dicho acontecimiento el ahora extinto Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) mencionó que "compromete la seguridad de la información sensible y los datos personales de personas servidoras públicas y particulares que resguarda esa institución, así como información de seguridad nacional".[16]

vii. La Comisión Nacional Bancaria y de Valores (CNBV), declara que a septiembre de 2024 recibió 15 reportes de incidentes de ciberseguridad por parte de las entidades financieras, la misma cantidad de incidentes que se tuvieron en 2023, no obstante, señalan que es posible que falte información necesaria de los incidentes de seguridad en instituciones bancarias porque, incluso estando obligadas a reportarlos, no informan de manera oportuna sobre los percances de los que son víctimas.[17]

viii. El incidente que afectó el proceso de operaciones con tarjetas de crédito y débito durante el sábado 10 de agosto de 2019, tanto en terminales punto de venta como en cajeros automáticos, el cual se debió a problemas relacionados con la infraestructura eléctrica de la cámara de compensación para pagos que ofrece la empresa privada Promoción y Operación S.A. de C.V. (Prosa), afectando a 25 millones de usuarios.[18]

ix. El incidente de ciberseguridad que experimentó la empresa Coca-Cola FEMSA, por el cual implementó sus protocolos de protección y respuesta de ciberseguridad para evitar un impacto adverso en sus aplicaciones de tecnologías de la información. La empresa comunicó que se encuentra trabajando con expertos en medidas para evitar un impacto adverso en sus aplicaciones de tecnologías de la información.[19]

x. Las fallas presentadas en los servicios financieros proporcionados por Caja Popular Mexicana, S.C. de A.P. de R.L. de C.V., durante el seguimiento la sociedad manifestó a la Comisión Nacional

---

[14] Riquelme, Rodrigo, *"Esto es todo lo que sabemos del hackeo a la Comisión Nacional de Seguros y Fianzas"*, El economista, 08 de diciembre de 2020, https://www.eleconomista.com.mx/sectorfinanciero/Esto-es-todo-lo-que-sabemos-del-hackeo-a-la-Comision-Nacional-de-Seguros-y-Fianzas-20201208-0048.html, consultado el 28 de febrero 2025.

[15] Bravo, Jorge, ""Hackeo" a la Sedena y desidia en ciberseguridad", Proceso, octubre 2022, disponible en: https://www.proceso.com.mx/opinion/2022/10/12/hackeo-la-sedena-desidia-en-ciberseguridad-294998.html, consultado el 28 de febrero 2025.

[17] R3D: Red en Defensa de los Derechos Digitales, *"La CNBV señala que las instituciones financieras ocultan incidentes de ciberseguridad"*, 23 de septiembre de 2024, disponible en: https://r3d.mx/2024/09/23/la-cnbv-senala-que-las-instituciones-financieras-ocultan-incidentes-de-ciberseguridad/, consultado el 28 de febrero 2025.

[18] Morales, Yolanda, *"Problemas en infraestructura eléctrica de Prosa provocó los fallos en pagos con tarjetas: Banxico"*, El economista, 13 de agosto de 2019, disponible en: https://www.eleconomista.com.mx/sectorfinanciero/Problemas-en-infraestructura-electrica-de-Prosa-provoco-los-fallos-en-pagos-con-tarjetas-Banxico-20190813-0022.html, consultado el 28 de febrero 2025.

[19] Coca-Cola FEMSA, Coca-*Cola FEMSA Anuncia Incidente de Ciberseguridad*, Ciudad de México, México - 26 de abril de 2023, disponible en: https://www.bmv.com.mx/docs-pub/eventemi/eventemi_1273871_1.pdf, consultado el 28 de febrero 2025.

Bancaria y de Valores que las fallas en los servicios financieros se debieron a un incidente de ciberseguridad.[20]

xi. El incidente de ciberseguridad al Fondo Monetario Internacional detectado el 16 de febrero de 2024 en el cual manifestaron que se vieron comprometidas once cuentas de correo electrónico de dicho organismo.[21]

xii. La Presidencia de la República del Gobierno de México informó sobre el ingreso no autorizado a un archivo que contenía información parcial de periodistas acreditados de la fuente presidencial, viéndose afectados 263 periodistas de los cuales existían datos personales en su conjunto, es decir, 168 credenciales de elector que tenían domicilio completo, 63 pasaportes, uno más, ilegible; dos currículums; una licencia de conducir de Estados Unidos; una Clave Única de Registro de Población y 10 documentos expedidos por el Instituto Nacional de Migración; hay cuatro personas de las que sólo aparece su fotografía, sin ningún dato más.[22]

xiii. Grupo Coppel reportó un incidente de ciberseguridad que generó fallas en sus sistemas el lunes 15 de abril de 2024, cuando sus clientes reportaron que no podían ingresar a su página web para realizar diversos trámites.[23]

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[24] consideran que la obtención de información técnica de especificaciones, es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

Inclusive, uno de los modus operandi de los ciberataques es precisamente a través de la obtención de **información pública**, información fácilmente accesible o información inaccesible, lo cual puede ocurrir mediante solicitudes de acceso a la información, o bien, a través de las organizaciones que operan o tienen acceso a los sistemas, en complicidad o no, con el único objeto de **conocer las vulnerabilidades en las instituciones, empresas, sistemas e infraestructura de tecnologías de la información**.[25]

---

[20] Comisión Nacional Bancaria y de Valores, *"CNBV realiza seguimiento a Caja Popular Mexicana"*, 22 de julio de 2023, disponible a través de la liga de electrónica: https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/SECTOR-POPULAR/Difusi%C3%B3n/Prensa%20%20Sociedades%20Cooperativas%20de%20Ahorro%20y%20Prstam/Comunicado%20de%20Prensa%2024%20CPM.pdf; y *"CNBV continúa con el seguimiento y vigilancia a Caja Popular Mexicana (CPM)"*, con fecha del 31 de agosto de 2023, disponible a través de la liga de electrónica: https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/SECTOR-POPULAR/Difusi%C3%B3n/Prensa%20%20Sociedades%20Cooperativas%20de%20Ahorro%20y%20Prstam/Comunicado%20de%20Prensa%2029%20CNBV%20contin%C3%BAa%20con%20el%20seguimiento%20y%20vigilancia%20a%20CPM.-2.pdf, consultado el 28 de febrero 2025.

[21] Fondo Monetario Internacional, *"El FMI investiga un incidente de ciberseguridad"*, 15 de marzo de 2024, disponible a través de la liga electrónica: https://www.imf.org/es/News/Articles/2024/03/15/pr2488-imf-investigates-cyber-security-incident, consultado el 28 de febrero 2025.

[22] Presidencia de la República, *"Gobierno de México denunciará ante FGR por sustracción ilegal externa de datos de periodistas"*. 29 de enero de 2024, disponible a través de la liga electrónica: https://www.gob.mx/segob/prensa/gobierno-de-mexico-denunciara-ante-fgr-por-sustraccion-ilegal-externa-de-datos-de-periodistas-356608?state=published#:~:text=El%20subsecretario%20de%20Derechos%20Humanos,localicen%20a%20quienes%20resulten%20responsables, consultado el 28 de febrero 2025.

[23] Redacción El Economista, *"Coppel reporta incidente de ciberseguridad en sus sistemas; garantiza protección de datos de sus clientes"*, El Economista, 20 de abril de 2024, disponible a través de la liga electrónica: https://www.eleconomista.com.mx/sectorfinanciero/Coppel-reporta-incidente-de-ciberseguridad-en-sus-sistemas-garantiza-proteccion-de-datos-de-sus-clientes-20240420-0015.html, consulado el 28 de febrero 2025.

[24] Offensive Security, INFORMATION GATHERING IN METASPLOIT, disponible en: https://www.offensive-security.com/metasploit-unleashed/information-gathering/, consultado el 28 de febrero 2025.

[25] El Economista, *El sistema financiero mexicano fue víctima de una campaña de ciberataques*, 15 de mayo de 2018. https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html consultado el 28 de febrero 2025.

Por otro lado, es de destacar que **los cibercriminales han utilizado técnicas de ingeniería social para obtener información y con ello acceder o vulnerar incluso los sistemas más seguros**. Una de las formas más comunes de vulnerar los sistemas es mediante la obtención de información a través de diversas fuentes y mecanismos que les permita diseñar ataques informáticos encaminados a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros elementos, con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes. Las corporaciones multinacionales y las agencias de noticias han sido víctimas de sofisticados ataques dirigidos contra sus sistemas de información derivado de la aplicación de técnicas de ingeniería social.[26]

Por lo anterior, **los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuyo rol no esté autorizado,**[27] en el entendido de que dicha información, al estar en posesión de personas no autorizadas, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central de la nación, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

3. **Identificable**, puesto que, a la fecha de realización de la presente prueba de daño, es un hecho notorio que el sector financiero a nivel mundial, incluyendo bancos centrales y diversas instituciones financieras, están siendo objeto de ciberataques dirigidos a vulnerar sistemas que resguardan información, incluso información personal, como quedó demostrado en la sección anterior. Si bien dichos ataques no han logrado irrumpir en los sistemas del Banco de México, resulta claramente que se debe de prever la protección de la información.

   En ese sentido, **un ataque informático derivado de divulgar la información materia de la presente prueba de daño, podría resultar en la vulneración o sustracción de la información de los sistemas de pagos y aplicaciones diseñadas por el Banco de México en su función de promover el sano desarrollo del sistema financiero.**

   Adicionalmente, una disrupción en los servicios provistos por los sistemas de pagos o de sus participantes, producto de un ataque contra estos o sus tecnologías de la información y de comunicaciones, tendría repercusiones directas para **una gran cantidad de empresas y comercios**, cuyas obligaciones a cubrir a través de pagos electrónicos interbancarios se verían afectadas durante el tiempo de la interrupción de estos servicios. Asimismo, **la población en general** que utiliza estos medios de pago, vería afectada su capacidad para realizar o cumplir con el pago de bienes y servicios, y **las instituciones bancarias y no bancarias participantes de los sistemas de pagos**, que obtienen parte de sus ingresos del cobro de comisiones por la prestación del servicio de pagos a través de estos, también resultarían gravemente perjudicadas, lo cual provocaría una seria afectación al sistema financiero. Finalmente, **las personas que reciben pagos del Gobierno Federal** mismos que son dispersados por este Instituto Central en su carácter de Agente Financiero de la Tesorería de la Federación, se verían seriamente comprometidos.

---

[26] Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, 18 de diciembre de 2001., disponible en: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=891b1f29-e2e7-4484-89c0-a2137ee82f8b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments, consultado el 28 de febrero 2025.

[27] Ver por ejemplo las 10 medidas básicas de ciberseguridad de la Security Information Center, en particular la relacionada con "Implementar un programa de capacitación en seguridad cibernética para empleados "en donde recomiendan sensibilizar sobre los temas de ingeniería social que buscan obtener información mediante diversos canales de comunicación solicitando información sensible. https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_0.pdf, consultado el 28 de febrero 2025.

Por lo anterior, es posible identificar que **el riesgo de perjuicio que supondría la divulgación de la información materia de esta prueba de daño, supera el interés público general de que se difunda**, pues el interés público se centra en que no se comprometa la efectividad en las medidas implementadas en los sistemas financiero y económico, que propician el buen funcionamiento de esos sistemas y del sistema financiero. Por lo que, **la información, no satisface un interés público, por el contrario, es información que pone en riesgo las medidas implementadas por este Instituto Central para la efectividad del sistema financiero**. Asimismo, al realizar una interpretación sobre la alternativa que más satisface dicho interés, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México, los sistemas administrados y las aplicaciones implementadas por éste.

En consecuencia, **proporcionar la información en cuestión, no aporta un beneficio mayor a la transparencia y rendición de cuentas que sea comparable con el perjuicio que implicaría el hecho de divulgarla**, esto es, que permita planear y perpetrar ataques dirigidos específicamente a los sistemas de pagos administrados, operados y supervisados por el Banco de México y a sus aplicaciones, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información - como datos personales referente a sus usuarios y las operaciones que realizan, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción en éstos.

Adicionalmente, **el riesgo de perjuicio que supondría la divulgación de la información, supera el interés público general de que se difunda,** ya que dar a conocer ***información referente a los resultados de consultorías en seguridad informática realizadas a los sistemas de pagos y/o aplicaciones que diseña, administra y opera el Banco de México en su función de promover el sano desarrollo de sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos,*** no aporta un beneficio a la transparencia que sea comparable con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento o dejar inoperantes a los sistemas.

Al respecto, debe destacarse que la información materia de la presente prueba de daño no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, **beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México las cuales, entre otras, se advierten la de promover el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.**

Por otra parte, **la limitación se adecua al principio de proporcionalidad, toda vez que** debe prevalecer el interés que más beneficie a la colectividad, y como se ha dicho, proteger la información materia de la presente prueba de daño **evitará poner en riesgo el buen funcionamiento de los sistemas de pagos del sistema financiero y de la economía nacional en su conjunto.**

En razón de lo anterior, y vistas las consideraciones expuestas en la presente prueba de daño, se solicita la reserva de dicha información, por el **plazo de 5 años más, contados a partir de la fecha de vencimiento del actual plazo de reserva**, en virtud de que esta acción atiende a la protección de las medidas de seguridad informática y especificaciones técnicas con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de pagos y las aplicaciones diseñadas por el Banco de México, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos.

En consecuencia, con fundamento en lo establecido en los artículos 6o., párrafo cuarto, apartado A, fracciones I y VIII, párrafo cuarto, 28, párrafos séptimo y octavo, de la CPEUM; 1, 102, 103, 104, párrafo tercero, 106, 107, 108, 109, 112, fracciones IV y VII, y 113 de la LGTAIP; 1o., 2o. y 3o., fracción I, de la Ley del Banco de México; así como 4o., párrafo primero, 8o., párrafos primero, y tercero, y 10, párrafo primero, del Reglamento Interior del Banco de México, es de clasificarse como reservada la ***información referente a los resultados de consultorías en seguridad informática realizadas a los sistemas de pagos y/o aplicaciones que diseña, administra y opera el Banco de México en su función de promover el sano desarrollo de sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos***, toda vez que la divulgación de dicha información menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto; comprometería las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero o el buen funcionamiento de los sistemas de pagos; generaría incumplimiento de las obligaciones de un participante en un sistema de pagos que dé lugar a que otros participantes incumplan, a su vez, con sus respectivas obligaciones que pueda afectar seriamente al sistema financiero, así como se vería obstruida la prevención de delitos.

"ANEXO 5"

BANCO DE MÉXICO®

"2025, Año de la Mujer Indígena"

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DEL PERIODO DE RESERVA

VISTOS, para resolver sobre la ampliación del periodo de reserva de información determinada por la unidad administrativa solicitante, y:

RESULTANDO

I. Que, con la finalidad de cumplir con las obligaciones de transparencia comunes, los sujetos obligados pondrán a disposición del público, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, la información de los temas, documentos y políticas que se señalan en el artículo 65 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

II. Que, del análisis realizado a la información que en su momento fue clasificada como reservada, se han puesto a consideración de este Órgano Colegiado los motivos y fundamentos para ampliar el periodo de reserva próximo a concluir.

III. Que considerando lo anterior, se solicitó al Comité de Transparencia aprobar la ampliación del plazo de reserva de la información, como se indica enseguida:

FECHA O REFERENCIA DEL OFICIO	UNIDAD(ES) ADMINISTRATIVA(S) SOLICITANTE(S) Y NOMBRE(S) DE SU(S) TITULAR(ES)	SOLICITUD DEL OFICIO	INFORMACIÓN CLASIFICADA	PLAZO DE CLASIFICACIÓN
Oficio con número de referencia D20-016/2025, de fecha 25 de marzo de 2025.	Ángel Salazar Sotelo (Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México.)	Ampliación del plazo de reserva de la información referida en el citado oficio.	**Información reservada** en términos de lo señalado en el oficio y en la prueba de daño correspondiente. "*Información referente a los resultados de consultorías en seguridad informática realizadas a los sistemas de pagos y/o aplicaciones que diseña, administra y opera el Banco de México, en su función de promover el sano desarrollo de sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos.*"	**Plazo de reserva inicial:** 5 años, a partir del 25 de junio de 2020. **Plazo de reserva con ampliación:** 5 años, a partir del 26 de junio de 2025.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva de la información que soliciten los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 40, fracción VII, y 104, párrafo tercero, de la LGTAIP; así como 31, fracción IX, del Reglamento Interior del Banco de México (RIBM).

SEGUNDO. Este Comité de Transparencia, tomando en cuenta que en términos del artículo 106, párrafo segundo, de la LGTAIP, advierte que las razones, motivos y circunstancias especiales que llevaron a concluir que en el caso particular se actualiza la necesidad de ampliar el periodo de reserva de la información señalada, se contienen en el oficio referido en el resultando III, así como en la prueba de daño correspondiente, los cuales se tienen aquí por reproducidos como si a la letra se insertasen.[1]

Al respecto, de conformidad con lo expresado en el oficio señalado en el resultando III, se llevó a cabo una debida ponderación de los intereses en conflicto y se acreditó que el riesgo de perjuicio rebasa el interés público; se acreditó también el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trata; se precisaron las razones por las que la divulgación de la información generaría una afectación a través de los elementos de un riesgo real, demostrable e identificable; y se acreditaron las circunstancias de modo, tiempo y lugar del daño.

En consecuencia, y considerando que, conforme a lo manifestado en la prueba de daño respectiva, la divulgación de la información correspondiente representa un **riesgo al interés público,** toda vez que: *"(…) posibilitaría la creación de mecanismos que faciliten el acceso indebido a los propios sistemas de pagos y de las aplicaciones desarrolladas, generaría vulnerabilidades y riesgos en los propios sistemas, la substracción de información técnica y datos que en ellas se resguardan, lo cual disminuiría la efectividad y eficacia de las medidas implementadas por este Instituto Central en los sistemas de pagos y aplicaciones que diseña, poniendo en riesgo el funcionamiento de dichos sistemas; o bien, podría obstruir la prevención de delitos, (…)"*, **este Comité de Transparencia aprueba la ampliación al periodo de reserva de la información señalada** de conformidad con lo expresado en el oficio citado en el resultando III de la presente determinación, así como en términos de la prueba de daño correspondiente, **y toma conocimiento del nuevo plazo de reserva determinado por la unidad administrativa.**

Por lo expuesto con fundamento en los artículos 40, fracción VII, y 104, párrafo tercero, de la LGTAIP; 31, fracción IX, del RIBM; y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

[1] Sirven de referencia los principios de elaboración de sentencias en materia civil, contenidos en la tesis *"SENTENCIA. CUANDO EL JUEZ CITA UNA TESIS PARA FUNDARLA, HACE SUYOS LOS ARGUMENTOS CONTENIDOS EN ELLA. Cuando en una sentencia se cita y transcribe un precedente o una tesis de jurisprudencia, como apoyo de lo que se está resolviendo, el Juez propiamente hace suyos los argumentos de esa tesis que resultan aplicables al caso que se resuelve, sin que se requiera que lo explicite, pues resulta obvio que al fundarse en la tesis recoge los diversos argumentos contenidos en ella."* (Suprema Corte de Justicia de la Nación; Registro digital: 192898; Instancia: Pleno; Novena Época; Materias(s): Común; Tesis: P./J. 126/99; Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo X, Noviembre de 1999, página 35; Tipo: Jurisprudencia).

RESUELVE

ÚNICO. Se aprueba la ampliación al periodo de reserva de la información clasificada como reservada señalada en el oficio mencionado en el resultando III de la presente determinación, conforme a la fundamentación y motivación expresada en el mismo, así como en la prueba de daño correspondiente, en términos del considerando Segundo de la presente resolución.

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en sesión celebrada el 19 de junio de 2025.----------

COMITÉ DE TRANSPARENCIA

_____

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente
Dirección de Seguridad y Organización de la Información

_____ _____

RODRIGO VILLA COLLINS
Integrante Suplente
Unidad de Transparencia

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente
Dirección Jurídica

PAJC
NMDS
MDF

Documento firmado digitalmente, su validación requiere hacerse electrónicamente.
Información de las firmas:

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
23/06/2025 11:22:09	Rodrigo Villa Collins	2e65db5644a854da5ec772e4a91b0974f90077ce2158b6d136159849a58a7b2b
23/06/2025 11:55:22	JOSE RAMON RODRIGUEZ MANCILLA	3ab7816efb14d1fe2da7770fb8c0a98cd46d93c7f255802e6eac5c0ff59d5c47
23/06/2025 12:23:35	Edgar Miguel Salas Ortega	aaca2669a8365cad688b6714b38b1e337564aeb0ee828ddd795363102422f536

"ANEXO 6"

BANCO DE MÉXICO®

Se recibe oficio y prueba de daño
JIS 383 25 marzo 2025
12:04

"2025, Año de la mujer indígena"

Ciudad de México, 25 de marzo de 2025
Ref: D20-017/2025

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
P r e s e n t e.

Me refiero a la clasificación de reserva realizada, en su momento, para el cumplimiento de las obligaciones de transparencia señaladas en el Título Quinto de la Ley General de Transparencia y Acceso a la Información Pública por la Subgerencia de Tecnologías Innovadoras de Sistemas de Pagos e Infraestructuras de Mercados y la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A, respecto de la información contenida en los documentos que se señalan a continuación:

TÍTULO DEL DOCUMENTO CLASIFICADO
Manual de operación para usuarios Base de Datos de Transferencias versión 1.3

Al respecto, me permito resaltar que dicha clasificación fue confirmada por el Comité de Transparencia mediante resolución de 25 de junio de 2020, emitida en la sesión Especial 17/2020, en términos de la fundamentación y motivación expresadas en el oficio de 19 de junio de 2020, suscrito por la Subgerencia de Tecnologías Innovadoras de Sistemas de Pagos e Infraestructuras de Mercados y la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A, y en la prueba de daño correspondiente.

Dicha clasificación se realizó por el periodo de 5 años contados a partir de la confirmación de la misma, lo cual ocurrió el 25 de junio de 2020 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **25 de junio de 2025.**

Sobre el particular, con fundamento en los artículos 104, párrafo tercero, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 2o., 3o. y 4o., de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, y tercero, 10, 12 Bis y 20, del Reglamento Interior del Banco de México (RIBM); así como Segundo, fracción XVII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, me permito informarles que esta unidad administrativa **estima que las causas para mantener clasificada como reservada la información referida en el presente oficio subsisten a la fecha, y lo seguirán al menos por los próximos 5 años, contados a partir de la citada fecha de expiración del plazo de reserva,** referida en el párrafo precedente.

Lo anterior, **en términos de la fundamentación y motivación expresadas en la prueba de daño correspondiente, que se pone a disposición de ese Comité de Transparencia.**

Por lo expuesto, y con fundamento en el artículo 104, párrafo tercero, de la LGTAIP; **solicito atentamente a ese Comité de Transparencia confirme la ampliación del plazo de reserva de la**

información referida en el presente oficio, por 5 años más, contados a partir de la fecha de expiración del plazo de reserva respectivo.

Asimismo, informo que el personal que por la naturaleza de sus atribuciones tiene acceso a la referida información clasificada es el adscrito a: Dirección General de Sistemas de Pagos e Infraestructuras de Mercados (Director General), Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructura de Mercados (Director), Gerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados (Gerente), Gerencia de Tecnologías Innovadoras de Sistemas de Pagos e Infraestructuras de Mercados (Gerente), Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A (Subgerente), Subgerencia de Tecnologías Innovadoras de Sistemas de Pagos e Infraestructuras de Mercados (Subgerente), Dirección de Política y Estudios de Sistemas de Pagos e Infraestructuras de Mercados (Director), Gerencia de Política Regulatoria de Sistemas de Pagos e Infraestructuras de Mercados (Gerente) y Subgerencia de Cámaras de Compensación, Tarjetas y Sistemas de Información (Subgerente).

Atentamente

Ángel Salazar Sotelo
Director de Desarrollo e Innovación de Sistemas
de Pagos e Infraestructuras de Mercados

PRUEBA DE DAÑO

INFORMACIÓN RELACIONADA CON SEGURIDAD INFORMÁTICA, ELEMENTOS OPERATIVOS Y ESPECIFICACIONES TÉCNICAS, IMPLEMENTADAS EN LA OPERACIÓN DE LA PLATAFORMA TECNOLÓGICA QUE PERMITE EL INTERCAMBIO DE INFORMACIÓN ENTRE INSTITUCIONES DE CRÉDITO, QUE ADMINISTRA EL BANCO DE MÉXICO EN SU FUNCIÓN DE PROMOVER EL SANO DESARROLLO DEL SISTEMA FINANCIERO.

En términos de lo dispuesto en los artículos 6, párrafo cuarto, apartado A, fracciones I y VIII, cuarto párrafo, 28, párrafos séptimo y octavo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM); 112, fracciones IV y VII, de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP), es de clasificarse como información reservada aquella que:

- Menoscabe la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país.
- Obstruya la prevención de delitos.

Al establecer los parámetros de la información cuya divulgación pueda afectar considerablemente la instrumentación y por ende la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, y dañar el buen funcionamiento del sistema de pagos, es indispensable identificar los objetivos de protección de la información, por tanto, es preciso dar a conocer los riesgos a los cuales puede estar expuesta la información que nos atañe.

Al tener el Banco de México, por mandato de Ley, la facultad de promover el sano desarrollo del sistema financiero y, en un mundo globalizado y digital, el ejercicio de estas funciones no puede ser concebida sin el uso de herramientas de tecnologías de la información y comunicaciones eficientes, confiables y seguras; en efecto, la secrecía, sigilo y cuidado de la información que mantiene la estabilidad y buen funcionamiento del sistema financiero, de los sistemas de pagos, y de la economía nacional en su conjunto, debe ser tratada de manera cautelosa. En este tenor, la presente prueba de daño constituye los **límites al principio de máxima publicidad**, misma que permite la reserva de la información, con la única intención de proteger el **interés público sobre el interés individual de dar a conocer la información motivo de la presente prueba de daño.**

El dar a conocer la ***información relacionada con seguridad informática, elementos operativos y especificaciones técnicas, implementadas en la operación de la plataforma tecnológica que permite el intercambio de información entre instituciones de crédito, que administra el Banco de México en su función de promover el sano desarrollo del sistema financiero***, entre las cuales se advierte la referente a protocolos de comunicación, formatos de mensajes, protocolos tecnológicos, de seguridad informática, procedimientos de continuidad operativa y de contingencia, requisitos de seguridad informática y de gestión del riesgo operacional, así como toda información que de forma aislada o agrupada, permita vincular directa o indirectamente, algún elemento específico en la operación de la plataforma tecnológica que permite el intercambio de información entre instituciones de crédito, que administra el Banco de México en su función de promover el sano desarrollo del sistema financiero, podría disminuir la efectividad de las medidas implementadas en los sistemas financiero o económico del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto; o bien, podía obstruir la prevención de delitos, por lo que dicha información se clasifica como reservada, toda vez que el riesgo es:

1. **Real**, en razón de revelar o divulgar la información motivo de la presente prueba de daño, **facilita a una persona o grupo de personas con intenciones delincuenciales identificar, de manera directa o a través de técnicas de ingeniería social, los aspectos de seguridad informática, las especificaciones técnicas en materia de seguridad,** especificaciones operativas, y, en general, información

relacionada con la infraestructura de la plataforma tecnológica que opera el Banco de México a través de la cual se realiza el intercambio de información entre instituciones de crédito sobre las transferencias de fondos nacionales en moneda extranjera, así como de transferencias de fondos internacionales que envíen o reciban las mismas, posibilita la realización de acciones hostiles en contra de las tecnologías de la información de este Banco Central, así como de las infraestructuras que éste administra y opera lo cual, podría menoscabar la efectividad de las infraestructuras a tal grado, que su destrucción o inhabilitación afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero y económico, del país, arriesgando el buen funcionamiento de esos sistemas y, en consecuencia, de la economía nacional en su conjunto.

Los riesgos aludidos tienen mayor probabilidad de materializarse con la divulgación de la información citada, debido a que **los delincuentes podrían diseñar estrategias para llevar a cabo ataques dirigidos específicamente a la plataforma tecnológica que trata información relacionada con las transferencias de fondos nacionales en moneda extranjera, así como de transferencias de fondos internacionales que envíen o reciban las instituciones de crédito a nombre o por cuenta propia o de sus clientes y usuarios, plataforma que administra el Banco Central, dichos ataques focalizados podrían tener mayor probabilidad de éxito debido a que los delincuentes tendrían la posibilidad de dedicar todos sus recursos a ataques específicos identificados con base en la información en cuestión**.

Incluso, los ataques cibernéticos pueden provocar la disrupción de los servicios de esa plataforma, y de lograr un ataque exitoso se pondría en riesgo la información que en ella se almacena, y como consecuencia poner en riesgo el buen funcionamiento del sistema financiero y de la economía nacional en su conjunto, así como alterar, extraer o suprimir la información transaccional que en ella se trata.

En efecto, revelar la información materia de la presente prueba de daño, **facilitaría que terceros logren acceder a información personal y financiera descrita en las operaciones,** modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a dichas tecnologías.

Asimismo, es de suma importancia destacar **que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas**. Estos ataques se fundamentan en descubrir y aprovechar supuestas vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, seguridad informática, especificaciones técnicas en materia de seguridad, procesos de continuidad operativa y, en general, información relacionada con los sistemas correspondientes e infraestructura informática.

Está documentado en la literatura especializada en la materia que **los principales elementos de información que requiere conocer un cibercriminal son**: la **arquitectura de los sistemas**, sus **especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad informática instrumentados, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir** en estos elementos y atacar a los sistemas.[1]

En el caso en concreto, **la información materia de esta prueba de daño posibilita que de manera directa o indirecta se puedan identificar especificaciones técnicas, especificaciones en materia de**

[1] Wilshusen, G. C., & Powner, D. A. (2009). Cybersecurity: Continued efforts are needed to protect information systems from evolving threats (No. GA0-10-230T). GOVERNMENT ACCOUNTABILITY OFFICE WASHINGTON DC.

seguridad, particularidades técnicas de su operación y ejecución, especificaciones respecto de los servicios prestados así como las condiciones de los mismos, entre otros, por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales identificar, analizar y posteriormente aprovechar los supuestos puntos débiles de la plataforma, y en consecuencia llevar a cabo ataques informáticos más certeros con la finalidad de causar daños o disrupción de servicios, obtener datos personales e información financiera o incluso modificar información que pudiera ser de tal relevancia, como aquellas operaciones que pudieran estar vinculadas con recursos de procedencia ilícita o financiamiento al terrorismo.

Por lo anterior, mantener clasificada con carácter de reservada la información materia de esta prueba de daño, permite reducir sustancialmente ataques que pudieran resultar efectivos en contra de la Plataforma tecnológica que permite el intercambio de información entre instituciones de crédito, que administra el Banco de México.

2. **Demostrable,** ya que es un hecho notorio que durante los últimos años se ha observado un incremento sostenido de ataques informáticos en el sector financiero a nivel mundial, incluyendo Bancos Centrales y diversas instituciones financieras. Las investigaciones realizadas señalan que estos ataques han sido orquestados por organizaciones criminales internacionales con herramientas y técnicas sofisticadas que, además de dañar la reputación de las instituciones afectadas, han generado cuantiosas pérdidas económicas.[2]

   En relación con lo anterior, es importante señalar que **a 2023 México ocupó el primer lugar en ciberataques en Latinoamérica y el cuarto a nivel global**[3] y se encuentra en el en el top 3 de países con más ataques a servicios financieros.[4] Asimismo, **recibió la mayor cantidad de intentos de ciberataques con 187 mil millones**, seguido por Brasil con 103 mil millones de ciberataques, Colombia con 103 mil millones y Perú con 15 mil millones.[5]

   Adicionalmente, se citan algunos de los ataques más relevantes que se han identificado:

   i. El ataque que se perpetró a BANCOMEXT el 9 de enero de 2018 a través de una afectación en su plataforma de pagos internacionales provocada por un tercero. Dicho ataque es similar a intromisiones ocurridas en otras instituciones en México y América Latina.[6]

   ii. El ataque ocurrido a las instituciones financieras participantes del SPEI®, el cual consistió en la alteración de sus aplicativos para conectarse a esta IMF, mediante código malicioso, el cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios

---

[2] Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Congressional Research Service Documents, CRS RL32331 (Washington DC).

[3] Redacción el Heraldo de México, "México ocupa el primer lugar en ciberataques en Latinoamérica y el cuarto a nivel global", El Heraldo, 24 de febrero 2023, disponible en: https://heraldodemexico.com.mx/tecnologia/2023/2/24/mexico-ocupa-el-primer-lugar-en-ciberataques-en-latinoamerica-el-cuarto-nivel-global-484179.html, Consultado el 03 de marzo 2025.

[4] Ramírez, Selene, "México en el top 3 de países con más ataques a servicios financieros", Expansión, 23 agosto 2023, disponible en: https://expansion.mx/tecnologia/2023/08/23/mexico-en-el-top-3-de-paises-con-mas-ataques-a-servicios-financieros#:~:text=A%20nivel%20global%2C%20M%C3%A9xico%20es,el%20mayor%20productor%20de%20malware, Consultado el 03 de marzo 2025.

[5] Forninet, "Fortinet informa que América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en 2022", Forninet , 27 de febrero de 2023, Florida, disponible en: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent, consultado el 03 de marzo 2025.

[6] BANCOMEXT. "Acción oportuna de BANCOMEXT salvaguarda intereses de clientes y la institución". 10 de enero de 2018. https://www.bancomext.com/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion/, consultado el 03 de marzo 2025.

específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero.[7] A la fecha de publicación de dicho comunicado, se estimó un daño a los participantes del SPEI® de aproximadamente 300 millones de pesos.[8]

iii. El intento de degradación de servicio al que fue expuesto el Banco de México en su página principal el 7 de julio del 2020 en el cual se reportó que hubo intermitencias en la página web principal durante aproximadamente 30 minutos. Asimismo, se informó que, los mecanismos y protocolos de protección establecidos por el Banco de México para este tipo de circunstancias evitaron afectaciones a sus procesos en los mercados financieros y sistemas de pagos.[9]

iv. El robo de información que sufrió la entonces Secretaría de la Función Pública, entre mayo y junio de 2020, en la que la Secretaría explicó que el grupo de atacantes detectó una vulnerabilidad en la configuración de una base de datos que permitió *"un ataque técnico en el que se accedió a los índices de la base de datos, pudiéndose haberse realizado una copia de la información y se introdujo un aviso de extorsión"*. Asimismo, una investigación reveló que la base de datos, con información de más de 830 mil funcionarios, estuvo disponible en internet, más de un mes.[10]

v. El incidente se seguridad que sufrió la Comisión Nacional de Seguros y Fianzas (CNSF). La organización Bank Security difundió que una persona había puesto a subasta accesos de administración de red y 10 GB de datos confidenciales de la CNSF, esto como consecuencia del ataque denominado "Lockbit", una de las más recientes formas de "ransomware" que los cibercriminales usan para encriptar la información de los sistemas infectados y pedir rescate, y que en caso de no pagarlo extraen la información con el fin de hacerla pública. Posteriormente, el 28 de noviembre del 2020, la CNSF anunció, vía twitter, que sufrió un ataque cibernético que afectó su continuidad operativa.[11]

vi. El ataque cibernético a los sistemas informáticos de la Secretaría de la Defensa Nacional, mejor conocida como Sedena,[12] realizado por los ciberactivistas Guacamaya, el cual hasta 2022, es el mayor ciberataque en la historia del país porque da a conocer miles de documentos confidenciales del gobierno federal. De dicho acontecimiento el ahora extinto Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) mencionó que "compromete la seguridad de la información sensible y los datos personales de personas servidoras públicas y particulares que resguarda esa institución, así como información de seguridad nacional".

---

[7] Banco de México. "Información sobre los ataques a los Participantes del SPEI", mayo 2018, disponible en: https://www.banxico.org.mx/spei/d/%7BFFC53F5A-CA04-3098-EBF6-B0F17E533183%7D.pdf, consultado el 03 de marzo 2025.

[8] Banco de México, "Puntos importantes sobre la situación actual del SPEI", 22 de mayo de 2018, disponible en: https://www.banxico.org.mx/spei/d/%7BB806F1E8-686D-B9F1-0452-EC375543C801%7D.pdf, consultado el 03 de marzo 2025.

[9] Banco de México, Comunicado de prensa "El Banco de México informa sobre el estado operativo de su página web", 7 de julio de 2020, disponible en https://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B8A57A6F9-E0F8-969E-202E-64EF6394EBD3%7D.pdf, consultado el 03 de marzo 2025.

[10] R3D: Red en Defensa de los Derechos Digitales, "Secretaría de la Función Pública sufrió robo de información; falló en proteger datos personales, alerta el INAI", 16 de diciembre de 2020, disponible en: https://r3d.mx/2020/12/16/secretaria-de-la-funcion-publica-sufrio-robo-de-informacion-fallo-en-proteger-datos-personales-alerta-el-inai/, consultado el 03 de marzo 2025.

[11] Riquelme, Rodrigo, *"Esto es todo lo que sabemos del hackeo a la Comisión Nacional de Seguros y Fianzas"*, El economista, 08 de diciembre de 2020, https://www.eleconomista.com.mx/sectorfinanciero/Esto-es-todo-lo-que-sabemos-del-hackeo-a-la-Comision-Nacional-de-Seguros-y-Fianzas-20201208-0048.html, consultado el 03 de marzo 2025.

[12] Bravo, Jorge, ""Hackeo" a la Sedena y desidia en ciberseguridad", Proceso, octubre 2022, disponible en: https://www.proceso.com.mx/opinion/2022/10/12/hackèo-la-sedena-desidia-en-ciberseguridad-294998.html, consultado el 03 de marzo 2025.

vii. La Comisión Nacional Bancaria y de Valores (CNBV), declara que a septiembre de 2024 recibió 15 reportes de incidentes de ciberseguridad por parte de las entidades financieras, la misma cantidad de incidentes que se tuvieron en 2023, no obstante, señalan que es posible que falte información necesaria de los incidentes de seguridad en instituciones bancarias porque, incluso estando obligadas a reportarlos, no informan de manera oportuna sobre los percances de los que son víctimas.[13]

viii. El incidente que afectó el proceso de operaciones con tarjetas de crédito y débito durante el sábado 10 de agosto de 2019, tanto en terminales punto de venta como en cajeros automáticos, el cual se debió a problemas relacionados con la infraestructura eléctrica de la cámara de compensación para pagos que ofrece la empresa privada Promoción y Operación S.A. de C.V. (Prosa), afectando a 25 millones de usuarios.[14]

ix. El incidente de ciberseguridad que experimentó la empresa Coca-Cola FEMSA por el cual implementó sus protocolos de protección y respuesta de ciberseguridad para evitar un impacto adverso en sus aplicaciones de tecnologías de la información. La empresa comunicó que se encuentra trabajando con expertos en medidas para evitar un impacto adverso en sus aplicaciones de tecnologías de la información.[15]

x. Las fallas presentadas en los servicios financieros proporcionados por Caja Popular Mexicana, S.C. de A.P. de R.L. de C.V., durante el seguimiento la sociedad manifestó a la Comisión Nacional Bancaria y de Valores que las fallas en los servicios financieros se debieron a un incidente de ciberseguridad.[16]

xi. El incidente de ciberseguridad al Fondo Monetario Internacional detectado el 16 de febrero de 2024 en el cual manifestaron que se vieron comprometidas once cuentas de correo electrónico de dicho organismo.[17]

xii. La Presidencia de la República del Gobierno de México informó sobre el ingreso no autorizado a un archivo que contenía información parcial de periodistas acreditados de la fuente presidencial, viéndose afectados 263 periodistas de los cuales existían datos personales en su conjunto, es decir, 168 credenciales de elector que tenían domicilio completo, 63 pasaportes, uno más, ilegible; dos currículums; una licencia de conducir de Estados Unidos; una Clave Única de Registro

---

[13] R3D: Red en Defensa de los Derechos Digitales, *"La CNBV señala que las instituciones financieras ocultan incidentes de ciberseguridad"*, 23 de septiembre de 2024, disponible en: https://r3d.mx/2024/09/23/la-cnbv-senala-que-las-instituciones-financieras-ocultan-incidentes-de-ciberseguridad/, , consultado el 03 de marzo 2025.

[14] Morales, Yolanda, *"Problemas en infraestructura eléctrica de Prosa provocó los fallos en pagos con tarjetas: Banxico"*, El economista, 13 de agosto de 2019, disponible en: https://www.eleconomista.com.mx/sectorfinanciero/Problemas-en-infraestructura-electrica-de-Prosa-provoco-los-fallos-en-pagos-con-tarjetas-Banxico-20190813-0022.html, consultado el 03 de marzo 2025.

[15] Coca-Cola FEMSA, "Coca-*Cola FEMSA Anuncia Incidente de Ciberseguridad*", Ciudad de México, México - 26 de abril de 2023, disponible en: https://www.bmv.com.mx/docs-pub/eventemi/eventemi_1273871_1.pdf, consultado del 03 de marzo 2025.

[16] Comisión Nacional Bancaria y de Valores, *"CNBV realiza seguimiento a Caja Popular Mexicana"*, 22 de julio de 2023, disponible a través de la liga de electrónica: https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/SECTOR-POPULAR/Difusi%C3%B3n/Prensa%20%20Sociedades%20Cooperativas%20de%20Ahorro%20y%20Prstam/Comunicado%20de%20Prensa%2024%20CPM.pdf; y *"CNBV continúa con el seguimiento y vigilancia a Caja Popular Mexicana (CPM)"*, con fecha del 31 de agosto de 2023, disponible a través de la liga de electrónica: https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/SECTOR-POPULAR/Difusi%C3%B3n/Prensa%20%20Sociedades%20Cooperativas%20de%20Ahorro%20y%20Prstam/Comunicado%20de%20Prensa%2029%20CNBV%20contin%C3%BAa%20con%20el%20seguimiento%20y%20vigilancia%20a%20CPM.-2.pdf, consultado del 03 de marzo 2025.

[17] Fondo Monetario Internacional, *"El FMI investiga un incidente de ciberseguridad"*, 15 de marzo de 2024, disponible a través de la liga electrónica: https://www.imf.org/es/News/Articles/2024/03/15/pr2488-imf-investigates-cyber-security-incident, consultado el 03 de marzo 2025.

de Población y 10 documentos expedidos por el Instituto Nacional de Migración; hay cuatro personas de las que sólo aparece su fotografía, sin ningún dato más.[18]

xiii. Grupo Coppel reportó un incidente de ciberseguridad que generó fallas en sus sistemas el lunes 15 de abril de 2024, cuando sus clientes reportaron que no podían ingresar a su página web para realizar diversos trámites.[19]

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[20] consideran que la obtención de información técnica de especificaciones, es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

Inclusive, uno de los *modus operandi* de los atacantes es precisamente a través de la obtención de **información pública**, información fácilmente accesible o información inaccesible, lo cual puede ocurrir mediante solicitudes de acceso a la información, o bien, a través de las organizaciones que operan o tienen acceso a los sistemas, en complicidad o no, con el único objeto de **conocer las probables vulnerabilidades en las instituciones, empresas, sistemas e infraestructura de tecnologías**.[21]

Por otro lado, es de destacar que los criminales han utilizado técnicas de ingeniería social para obtener información y con ello acceder o vulnerar incluso los sistemas más seguros. **Una de las formas más comunes de vulnerar los sistemas es mediante la obtención de información a través de diversas fuentes y mecanismos que les permita diseñar ataques informáticos encaminados a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros elementos, con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes**. Las corporaciones multinacionales y las agencias de noticias han sido víctimas de sofisticados ataques dirigidos contra sus sistemas de información derivado de la aplicación de técnicas de ingeniería social.[22]

Por lo anterior, **los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuyo rol no esté autorizado**,[23] en el entendido de que dicha información, al estar en posesión de personas no autorizadas, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del

---

[18] Presidencia de la República, *"Gobierno de México denunciará ante FGR por sustracción ilegal externa de datos de periodistas"*. 29 de enero de 2024, disponible a través de la liga electrónica: https://www.gob.mx/segob/prensa/gobierno-de-mexico-denunciara-ante-fgr-por-sustraccion-ilegal-externa-de-datos-de-periodistas-356608?state=published#:~:text=El%20subsecretario%20de%20Derechos%20Humanos,localicen%20a%20quienes%20resulten%20responsables, consultado el 03 de marzo 2025.

[19] Redacción El Economista, *"Coppel reporta incidente de ciberseguridad en sus sistemas; garantiza protección de datos de sus clientes"*, El Economista, 20 de abril de 2024, disponible a través de la liga electrónica: https://www.eleconomista.com.mx/sectorfinanciero/Coppel-reporta-incidente-de-ciberseguridad-en-sus-sistemas-garantiza-proteccion-de-datos-de-sus-clientes-20240420-0015.html, consulado el 03 de marzo 2025.

[20] Offensive Security, INFORMATION GATHERING IN METASPLOIT, disponible en: https://www.offensive-security.com/metasploit-unleashed/information-gathering/, consultado el 03 de marzo 2025.

[21] Riquelme, Rodrigo, *"El sistema financiero mexicano fue victima de una campaña de ciberataques"*, El Economista, 15 de mayo de 2018, https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html, consultado el 03 de marzo 2025.

[22] Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, 18 de diciembre de 2001., disponible en: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=891b1f29-e2e7-4484-89c0-a2137ee82f8b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments, consultado el 03 de marzo 2025.

[23] Ver por ejemplo las 10 medidas básicas de ciberseguridad de la Security Information Center, en particular la relacionada con "Implementar un programa de capacitación en seguridad cibernética para empleados "en donde recomiendan sensibilizar sobre los temas de ingeniería social que buscan obtener información mediante diversos canales de comunicación solicitando información sensible, https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_0.pdf, consultado el 03 de marzo 2025.

Banco Central de la Nación, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

3. **Identificable,** ya que, a la fecha de realización de la presente prueba de daño, es un hecho notorio que en el mundo se han realizado ciberataques dirigidos a vulnerar los sistemas de pagos y los sistemas que resguardan información, incluso información personal. Si bien dichos ataques no han logrado irrumpir en los sistemas del Banco de México, resulta claramente identificable que el objeto final de dichos ataques son la infraestructura que maneja el Banco de México, cuya seguridad depende de la reserva de la información materia de la presente prueba de daño.

   En ese sentido, **un ataque informático derivado de divulgar la información materia de la presente prueba de daño, podría resultar en la vulneración de la información relacionada con las** operaciones que las Instituciones de crédito envíen o reciban a nombre o por cuenta propia o de sus clientes y usuarios, obtener información o incluso modificar información que pudiera ser de tal relevancia, como aquellas operaciones que pudieran estar vinculadas con recursos de procedencia ilícita o financiamiento al terrorismo, en beneficio o perjuicio de estas obstruyendo la prevención de delitos.

   Finalmente, una disrupción en los servicios provistos por la plataforma tecnológica, producto de un ataque contra esta o sus tecnologías de la información y de comunicaciones, tendría repercusiones directas para los Participantes, y el sistema financiero en general, ya que imposibilitaría que las Instituciones de Crédito puedan observar la información transaccional de sus clientes y potenciales usuarios, lo cual está directamente relacionado con la detección de operaciones que pudieran estar vinculadas con recursos de procedencia ilícita o financiamiento al terrorismo, impidiendo que este Instituto Central cumpla con su función de promover el sano desarrollo del sistema financiero, al no poder proveer de manera oportuna este servicio.

Adicionalmente, **el riesgo de perjuicio que supondría la divulgación de la información materia de esta prueba de daño, supera el interés público general de que se difunda**, pues el interés público se centra en que no se comprometa la efectividad en las medidas implementadas en los sistemas financiero y económico, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto. Por lo que, **la información, no satisface un interés público, por el contrario, es información que pone en riesgo las medidas implementadas por este Instituto Central para la efectividad del sistema financiero.** Asimismo, al realizar una interpretación sobre la alternativa que más satisface dicho interés, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México, los sistemas administrados y las plataformas implementadas por éste.

En consecuencia, **proporcionar la información en cuestión, no aporta un beneficio mayor a la transparencia y rendición de cuentas que sea comparable con el perjuicio que implicaría el hecho de divulgarla**, esto es, que permita planear y perpetrar ataques cibernéticos dirigidos específicamente a la plataforma tecnológica al Banco de México y a la infraestructura relacionada con estos, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información - como datos personales referente a sus usuarios y las operaciones que realizan -, o la disrupción en éstos. En este sentido, el riesgo de perjuicio antes señalado supera claramente el interés general de que se difunda la información.

Por otra parte, la limitación se adecua al principio de proporcionalidad, toda vez que debe prevalecer el interés que más beneficie a la colectividad, y como se ha dicho, proteger la información **evitará poner en riesgo el buen funcionamiento del sistema financiero y de la economía nacional en su conjunto.**

Asimismo, **reservar la información en cuestión representa el medio menos restrictivo disponible para evitar el perjuicio**, en aras salvaguardar la estabilidad y el buen funcionamiento del sistema financiero, **puesto que el propio legislador determinó que el medio menos restrictivo es la clasificación de la información cuando actualice las causales previstas en la Leyes aplicables**, tal y como se demostró en el presente caso. Por lo tanto, la reserva de la información es proporcional y resulta la forma menos restrictiva disponible para evitar un perjuicio mayor.

En razón de lo anterior, y vistas las consideraciones expuestas en la presente prueba de daño, se solicita la reserva de dicha información, por el **plazo de 5 años más, contados a partir de la fecha de vencimiento del actual plazo de reserva**, ya que como se ha mencionada a lo largo de la presente prueba de daño, esta acción atiende preservación de las medidas de seguridad informática necesarias, con la finalidad de evitar el desarrollo de estrategias para la realización de ataques informáticos más certeros y dirigidos específicamente a la plataforma que opera y administra actualmente este Instituto Central. Asimismo, el Banco Central continuará utilizando la infraestructura tecnológica protegida por la presente prueba de daño para el ejercicio de sus funciones, y continuará operando indefinidamente, por lo que la información materia de la presente clasificación seguirá siendo utilizada durante este periodo de tiempo e incluso más allá del mismo.

En consecuencia, con fundamento en lo establecido en los artículos 6o., párrafo cuarto, apartado A, fracciones I y VIII, párrafo cuarto, 28, párrafos séptimo y octavo, de la CPEUM; 1, 102, 103, 104, párrafo tercero, 106, 107, 108, 109, 112, fracciones IV y VII, y 113 de la LGTAIP; 1o., 2o. y 3o., fracción I, de la Ley del Banco de México; así como 4o., párrafo primero, 8o., párrafos primero, y tercero, y 10, párrafo primero del Reglamento Interior del Banco de México; es de clasificarse como reservada ***la información relacionada con seguridad informática, elementos operativos y especificaciones técnicas, implementadas en la operación de la plataforma tecnológica que permite el intercambio de información entre instituciones de crédito, que administra el Banco de México en su función de promover el sano desarrollo del sistema financiero,*** toda vez que su divulgación menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto, así como la obstrucción en prevención de delitos.

"ANEXO 7"

BANCO DE MÉXICO®

"2025, Año de la Mujer Indígena"

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DEL PERIODO DE RESERVA

VISTOS, para resolver sobre la ampliación del periodo de reserva de información determinada por la unidad administrativa solicitante, y:

RESULTANDO

I. Que, con la finalidad de cumplir con las obligaciones de transparencia comunes, los sujetos obligados pondrán a disposición del público, en sus respectivos medios electrónicos y en la Plataforma Nacional de Transparencia, de acuerdo con sus facultades, atribuciones, funciones u objeto social, la información de los temas, documentos y políticas que se señalan en el artículo 65 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

II. Que, del análisis realizado a la información que en su momento fue clasificada como reservada, se han puesto a consideración de este Órgano Colegiado los motivos y fundamentos para ampliar el periodo de reserva próximo a concluir.

III. Que considerando lo anterior, se solicitó al Comité de Transparencia aprobar la ampliación del plazo de reserva de la información, como se indica enseguida:

FECHA O REFERENCIA DEL OFICIO	UNIDAD(ES) ADMINISTRATIVA(S) SOLICITANTE(S) Y NOMBRE(S) DE SU(S) TITULAR(ES)	SOLICITUD DEL OFICIO	INFORMACIÓN CLASIFICADA	PLAZO DE CLASIFICACIÓN
Oficio de referencia: D20-017/2025, de fecha 25 de marzo de 2025.	Ángel Salazar Sotelo (Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México).	Ampliación del plazo de reserva de la información referida en el citado oficio.	**Información reservada** en términos de lo señalado en el oficio y en la prueba de daño correspondiente. "*INFORMACIÓN RELACIONADA CON SEGURIDAD INFORMÁTICA, ELEMENTOS OPERATIVOS Y ESPECIFICACIONES TÉCNICAS, IMPLEMENTADAS EN LA OPERACIÓN DE LA PLATAFORMA TECNOLÓGICA QUE PERMITE EL INTERCAMBIO DE INFORMACIÓN ENTRE INSTITUCIONES DE CRÉDITO, QUE ADMINISTRA EL BANCO DE MÉXICO EN SU FUNCIÓN DE PROMOVER EL SANO DESARROLLO DEL SISTEMA FINANCIERO.*"	**Plazo de reserva inicial:** 5 años, a partir del 25 de junio de 2020. **Plazo de reserva con ampliación:** 5 años, a partir del 26 de junio de 2025.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva de la información que soliciten los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 40, fracción VII, y 104, párrafo tercero, de la LGTAIP; 31, fracción IX, del Reglamento Interior del Banco de México (RIBM).

SEGUNDO. Este Comité de Transparencia, tomando en cuenta que en términos del artículo 106, párrafo segundo, de la LGTAIP, advierte que las razones, motivos y circunstancias especiales que llevaron a concluir que en el caso particular se actualiza la necesidad de ampliar el periodo de reserva de la información señalada, se contienen en el oficio referido en el resultando III, así como en la prueba de daño correspondiente, los cuales se tienen aquí por reproducidos como si a la letra se insertasen.[1]

Al respecto, de conformidad con lo expresado en el oficio señalado en el resultando III, se llevó a cabo una debida ponderación de los intereses en conflicto y se acreditó que el riesgo de perjuicio rebasa el interés público; se acreditó también el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trata; se precisaron las razones por las que la divulgación de la información generaría una afectación a través de los elementos de un riesgo real, demostrable e identificable; y se acreditaron las circunstancias de modo, tiempo y lugar del daño.

En consecuencia, y considerando que, conforme a lo manifestado en la prueba de daño respectiva, la divulgación de la información correspondiente: *"(…) podría disminuir la efectividad de las medidas implementadas en los sistemas financiero o económico del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto; o bien, podía obstruir la prevención de delitos (…)"*, **este Comité de Transparencia aprueba la ampliación al periodo de reserva de la información señalada** de conformidad con lo expresado en el oficio citado en el resultando III de la presente determinación, así como en términos de la prueba de daño correspondiente, **y toma conocimiento del nuevo plazo de reserva determinado por la unidad administrativa.**

Por lo expuesto con fundamento en los artículos 40, fracción VII, y 104, párrafo tercero, de la LGTAIP; 31, fracción IX, del RIBM; y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este Órgano Colegiado:

RESUELVE

ÚNICO. Se aprueba la ampliación al periodo de reserva de la información clasificada como reservada señalada en el oficio mencionado en el resultando III de la presente determinación,

[1] Sirven de referencia los principios de elaboración de sentencias en materia civil, contenidos en la tesis *"SENTENCIA. CUANDO EL JUEZ CITA UNA TESIS PARA FUNDARLA, HACE SUYOS LOS ARGUMENTOS CONTENIDOS EN ELLA. Cuando en una sentencia se cita y transcribe un precedente o una tesis de jurisprudencia, como apoyo de lo que se está resolviendo, el Juez propiamente hace suyos los argumentos de esa tesis que resultan aplicables al caso que se resuelve, sin que se requiera que lo explicite, pues resulta obvio que al fundarse en la tesis recoge los diversos argumentos contenidos en ella."* (Suprema Corte de Justicia de la Nación; Registro digital: 192898; Instancia: Pleno; Novena Época; Materias(s): Común; Tesis: P./J. 126/99; Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo X, Noviembre de 1999, página 35; Tipo: Jurisprudencia).

conforme a la fundamentación y motivación expresadas en el mismo, así como en la prueba de daño correspondiente, en términos del considerando Segundo de la presente resolución.

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en sesión celebrada el 19 de junio de 2025.----------

COMITÉ DE TRANSPARENCIA

_____

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente
Dirección de Seguridad y Organización de la Información

_____	_____
RODRIGO VILLA COLLINS	**EDGAR MIGUEL SALAS ORTEGA**
Integrante Suplente	**Integrante Suplente**
Unidad de Transparencia	Dirección Jurídica

URD
AMR
MDF

Documento firmado digitalmente, su validación requiere hacerse electrónicamente.
Información de las firmas:

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
23/06/2025 11:22:09	Rodrigo Villa Collins	2e65db5644a854da5ec772e4a91b0974f90077ce2158b6d136159849a58a7b2b
23/06/2025 11:55:23	JOSE RAMON RODRIGUEZ MANCILLA	6f0ff1853948dc55e9d5a1f8f7173bff39053d333c1b2f9048c3e79b9d3aad31
23/06/2025 12:23:38	Edgar Miguel Salas Ortega	030d61226f35d251ab5c5e6c5e6353854f5105971d598d4ead175d6b0c601ae1

"ANEXO 8"

BANCO DE MÉXICO®

"2025, Año de la Mujer Indígena"

Se recibe oficio y prueba de daño.
J15383 20 marzo de 2025
12:00

Ciudad de México, 20 de marzo de 2025

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente.

Me refiero a la clasificación de reserva realizada, en su momento, para el cumplimiento de las obligaciones de transparencia señaladas en el Título Quinto de la Ley General de Transparencia y Acceso a la Información Pública por esta unidad administrativa, respecto de diversa información contenida en el documento que se señala en el siguiente cuadro:

TÍTULO DEL DOCUMENTO CLASIFICADO
MPO Envío y Recepción de billete a/de Cajas Regionales y Corresponsales 12junio2020 – O

Al respecto, me permito resaltar que dicha clasificación fue confirmada por ese Comité mediante resolución de 25 de junio de 2020, emitida en la sesión Especial 17/2020, en términos de la fundamentación y motivación expresadas en el oficio de 19 de junio de 2020, suscrito por esta unidad administrativa y en la prueba de daño correspondiente.

Dicha clasificación se realizó por el periodo de 5 años contados a partir de la confirmación de la misma, lo cual ocurrió el 25 de junio de 2020 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **25 de junio de 2025.**

Sobre el particular, con fundamento en los artículos 104, párrafo tercero, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 2o., 3o. y 4o., de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, y tercero, 10, y 16 Bis del Reglamento Interior del Banco de México (RIBM); así como Segundo, fracción III, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; me permito informarles que esta unidad administrativa **estima que las causas para mantener clasificada como reservada la información referida en el presente oficio subsisten a la fecha, y lo seguirán al menos por los próximos 5 años, contados a partir de la citada fecha de expiración del plazo de reserva,** referida en el párrafo precedente.

Lo anterior, **en términos de la fundamentación y motivación expresadas en la prueba de daño correspondiente, que se pone a disposición de ese Comité de Transparencia.**

Por lo expuesto, y con fundamento en el artículo 104, párrafo tercero, de la LGTAIP, **solicito atentamente a ese Comité de Transparencia confirme la ampliación del plazo de reserva de la información referida en el presente oficio, por 5 años más,** contados a partir de la fecha de expiración del plazo de reserva respectivo.

Uso Público

Información de acceso público.

Asimismo, informo que el personal que por la naturaleza de sus atribuciones tiene acceso a la referida información clasificada es el adscrito a: Dirección General de Emisión (Director general), Dirección de Seguridad (Director), Gerencia de Protección y Traslado de Valores (Gerente), Gerencia de Prevención y Planeación de Seguridad (Gerente), Subgerencia de Resguardo y Traslado de Valores Jalisco (Subgerente), Subgerencia de Resguardo y Traslado de Valores Ciudad de México (Subgerente), Subgerencia de Transportes Aéreos (Subgerente), Oficina de Operaciones de Vuelo (Jefe), Dirección Programación y Distribución de Efectivo (Director), Cajero Regional Centro (Cajero), Subgerencia de Custodia de Efectivo (Subgerente), Subgerencia de Distribución y Proceso de Efectivo (Subgerente), Cajero Regional Guadalajara (Cajero), Cajero Regional Monterrey (Cajero), Cajero Regional Hermosillo (Cajero), Cajero Regional Veracruz (Cajero), Cajero Regional Mérida (Cajero), Dirección de Administración de Emisión (Director).

Atentamente

MTRA. ISABEL MORALES PASANTES
Directora de Programación y Distribución de Efectivo

PRUEBA DE DAÑO

Actividades de operación referentes al envío y recepción de billete a/de Cajas Regionales y Corresponsales.

En términos de lo dispuesto en los artículos 6º., párrafo cuarto, apartado A, fracciones I y VIII, párrafo cuarto, 28, párrafos séptimo y octavo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), 112, fracciones I, IV y V, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), es de clasificarse como información reservada aquella cuya publicación pueda, entre otras cosas:

- Comprometer la seguridad nacional.
- Comprometer la seguridad en la provisión de moneda nacional al país.
- Poner en riesgo la vida, seguridad o salud de una persona física.

Por lo que la información relativa a las ***"Actividades de operación referentes al envío y recepción de billete a/de Cajas Regionales y Corresponsales"***, es clasificada como reservada, ya que la divulgación de la citada información representa un riesgo de perjuicio significativo al interés público, compromete la seguridad nacional, la seguridad en la provisión de moneda nacional al país, y pone en riesgo la vida, seguridad y salud de personas físicas, toda vez que dicho riesgo es:

1) **Real**, ya que revelar o divulgar información relativa a las actividades de envío y recepción de billete a/de Cajas Regionales y Corresponsales así como la logística para realizar el envío de billetes a Cajas Regionales y Corresponsales de Banco de México, así como los diferentes responsables de ejecutar dicha tarea haría vulnerable la seguridad del efectivo que resguarda el Banco Central, a sus empleados, a sus instalaciones y, en consecuencia, el cumplimiento de la finalidad establecida en el artículo 2o. de la Ley del Banco de México, en el sentido de proveer a la economía del país de moneda nacional.

La divulgación de la información referente al envío y recepción de billete a/de Cajas Regionales y Corresponsales, compromete la seguridad nacional que refiere el artículo 112, fracción I, de la LGTAIP, y, por lo tanto, se podría destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos, como es la provisión de moneda nacional al país.

Asimismo, revelar la citada información compromete la seguridad en la provisión de moneda nacional al país que prevé el artículo 112, fracción IV, de la LGTAIP, toda vez que un eventual ataque a las instalaciones del Banco Central de la Nación, a los vehículos propios o de empresas de traslado de

valores, afectaría el cumplimiento de la finalidad establecida en el artículo 2o. de la Ley del Banco de México, en el sentido de proveer a la economía del país de moneda nacional.

Por otra parte, de conformidad con lo establecido en el artículo 112, fracción V, de la LGTAIP, divulgar las actividades de operación referentes al envío y recepción de billete a/de Cajas Regionales y Corresponsales, pone en inminente riesgo la vida, seguridad o salud del personal que labora en el Banco de México, destinado a realizar los traslados de efectivo desde el sitio de origen hasta el de destino, del personal de empresas de traslado de valores, así como de las personas que pudieran encontrase cerca de algún punto de ataque por parte de la delincuencia organizada. Por tal motivo, es indispensable salvaguardar la vida, seguridad y salud de todo el personal del Banco Central y de las personas que pudieran estar involucradas.

En efecto, de conformidad con los artículos 28, párrafo octavo de la Constitución Política de los Estados Unidos Mexicanos, así como 2o. y 4o. de la Ley del Banco de México, el Estado ejerce de manera exclusiva, a través del Banco de México, funciones en las áreas estratégicas de acuñación de moneda y emisión de billetes, por lo que resulta evidente que divulgar información contenida en las actividades de envío y recepción de billete a/de Cajas Regionales y Corresponsales, representaría una amenaza a la Seguridad Nacional al ponerse en riesgo el cumplimiento de la finalidad del Instituto Central de proveer a la economía del país de moneda nacional. Lo anterior, debido a que le corresponde privativamente emitir billetes y ordenar la acuñación de moneda metálica, así como poner ambos signos en circulación a través de las operaciones que dicha Ley le autoriza realizar.

En este sentido, el artículo 5, fracción XII, de la Ley de Seguridad Nacional establece que son amenazas a la seguridad nacional, los actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos. A su vez, el artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública dispone que se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, entre las que se encuentran las áreas estratégicas de acuñación de moneda y emisión de billetes citadas.

Por lo expuesto con antelación, es evidente que al divulgar información contenida en las actividades del envío y recepción de billete a/de Cajas Regionales y Corresponsales, se facilitaría conocer los métodos

que utiliza el Banco de México para la distribución de efectivo y los procedimientos detallados de envío de remesas de efectivo.

En ese mismo sentido, conforme a la experiencia en el contexto de seguridad y robo, un modo de operación común de los grupos de delincuencia organizada es el asalto a las empresas de traslado de valores, lo cual se facilitaría o lograría con la divulgación de la información contenida en las actividades de envío y recepción de billete a/de Cajas Regionales y Corresponsales, por lo que el hecho de hacerla del dominio público, implicaría un riesgo y una amenaza inminente en la distribución de efectivo, así como para el personal involucrado en esta actividad, ya que dicha información puede ser utilizada por la delincuencia organizada para planear un asalto a los vehículos que custodian y trasladan efectivo.

En cumplimiento de tal función, el Banco de México se encarga de proporcionar billetes y monedas en cantidad suficiente al Estado Mexicano con las medidas de seguridad y calidad adecuadas, a fin de preservar y fortalecer tanto la confianza del público usuario en los mismos, como procurar la estabilidad en la economía nacional.

Tomando en consideración lo anterior, conforme a la experiencia en el contexto de seguridad y asaltos a instalaciones bancarias a nivel internacional, un modo de operación común de los grupos de delincuencia organizada es la penetración a las bóvedas, lo cual se logra con información como la que se pretende hacer del conocimiento público, por lo que el hecho de otorgarla implicaría un riesgo y una posible amenaza a las instalaciones del Banco de México en dónde se encuentra el efectivo, así como para el personal que labora dentro del propio Banco Central, ya que dicha información puede ser utilizada por diversos grupos delincuenciales para planear una intrusión a las bóvedas de Banco de México.

Adicionalmente, es importante destacar que de conformidad con el artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública, se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, por lo tanto, no deben ser revelados.

2) Demostrable existen varios casos de asalto por grupos de la delincuencia organizada en el traslado de valores, y por tal motivo, es importante mencionar que el actuar de estos grupos, normalmente conlleva a la pérdida de vidas humanas, y en la actualidad, ésta mantiene una constante actividad delictiva tanto a nivel nacional como internacional, y como ejemplos de dicha actividad delictiva, se citan algunos casos de robos que destacaron en su planeación, cabe mencionar que los casos más vulnerables se presentan cuando los valores son transferidos de un vehículo terrestre a un aéreo:

a. En el territorio nacional:

1. En abril de 2019, en el Aeropuerto Internacional de Guanajuato, seis hombres encapuchados y armados asaltaron una camioneta de valores del Servicio Panamericano de Protección cuando se encontraba en una plataforma para cargar valores a una aeronave cuyo destino era la Ciudad de México. Los delincuentes utilizaron una camioneta con logotipos falsos de la aerolínea Aeroméxico para pasar hasta la zona restringida. Entre moneda nacional y dólares estadounidenses, el botín se estimó en 46 millones de pesos.[1]
2. En noviembre de 2020, en Guanajuato, se llevó a cabo un intento de robo a través de un túnel a las instalaciones de SEPSA, el cual fue construido de forma diagonal desde un predio cercano, atravesando la calle y el estacionamiento de diversos negocios, para así poder llegar a la bóveda de SEPSA[2].
3. En diciembre de 2024, en Tabasco, cinco sujetos armados interceptaron una camioneta de traslado de valores de la empresa Cometra, cuando se encontraba justo afuera de la sede de dicha empresa en Villahermosa. Los presuntos delincuentes dispararon contra la camioneta de valores en ocho ocasiones; lograron someter a los custodios y los obligaron a descender de la unidad para poder sustraer varias bolsas con efectivo[3].
4. En febrero de 2025, en Estado de México, un grupo conformado por 30 sujetos uniformados como policías irrumpieron en el Instituto Mexicano de Proceso y Traslado de Valores, ubicado en la calle Huatzin, de la colonia Pescadores. Los presuntos delincuentes arribaron a las instalaciones de la empresa con mazos, armas de fuego y camionetas con estrobos y simularon un cateo en el edificio. Se llevaron decenas de bolsas con monedas y efectivo por un monto aproximado de dos millones de pesos[4].

---

[1] Fuente: Verónica Espinosas (04 de abril de 2019). "Comando irrumpe en pista del aeropuerto de Guanajuato y roba 20 mdp de camión de valores". Consultado el 06 de marzo de 2025 en PROCESO. Sitio web: https://www.proceso.com.mx/nacional/estados/2019/4/4/comando-irrumpe-en-pista-del-aeropuerto-de-guanajuato-roba-20-mdp-de-camion-de-valores-222769.html

[2] Fuente: LC Camargo (17/11/2020). "Cavan túnel a bóveda de Sepsa; falla intento". Consultado el 06 de marzo de 2025 en PERIÓDICO CORREO. Sitio web: https://periodicocorreo.com.mx/cavan-tunel-a-boveda-de-sepsa-falla-intento/

[3] Fuente: Roberto Gómez (16/12/2024). "Hombres armados asaltan unidad de valores en Lindavista". Consultado el 06 de marzo de 2025 en EL HERALDO DE TABASCO. Sitio web: https://oem.com.mx/elheraldodetabasco/policiaca/hombres-armados-asaltan-unidad-de-valores-en-villahermosa-20527867

[4] Fuente: Claudia Flores (19/02/2025). "Supuestos policías robaron cerca de 3 toneladas de morralla del Instituto Mexicano de Proceso y Traslado de Valores en Chimalhuacán". Consultado el 06 de marzo de 2025 en INFOBAE. Sitio web: https://www.infobae.com/mexico/2025/02/19/supuestos-policias-robaron-cerca-de-3-toneladas-de-morralla-del-instituto-mexicano-de-proceso-y-traslado-de-valores-en-chimalhuacan/

b. En el ámbito internacional:

1. En marzo de 2018, en Brasil, hombres armados robaron cinco millones de dólares estadounidenses cuando eran descargados de un avión de la empresa Lufthansa a una camioneta de valores de la empresa Brink's en el Aeropuerto Internacional de la ciudad de Campinas. Mientras se realizaba la descarga de valores, los asaltantes sometieron a los custodios y sustrajeron los valores para colocarlos dentro del vehículo en el que viajaban. Huyeron embistiendo los portones de salida de la terminal aérea.[5]
2. En marzo de 2019, en Brasil, 2022, un comando de ocho personas realizó un ataque contra tres camionetas de traslado de valores de la empresa Brink's cuando se encontraban descargando valores de un avión en el Aeropuerto de Blumenau. Los asaltantes se movilizaban en dos vehículos, con uno de los cuales arrollaron el portón de acceso a la pista de aterrizaje y posterior a ello lanzaron una granada a la cubierta del avión[6].
3. En octubre de 2019, en Brasil, una camioneta de traslado de valores Brink's fue asaltada por un grupo formado por 20 personas en la zona de carga del Aeropuerto Internacional de Viracopos; el grupo delincuencial ingreso al aeropuerto a bordo de dos camionetas que tenían adhesivos propios de la aeronáutica brasileña. Los asaltantes se aproximaron a la unidad de Brink's, la cual estaba por cargar de valores a una aeronave[7].
4. En mayo de 2020, en Chile, la Brigada de Robos de la Policía de Investigaciones descubrió en un cobertizo abandonado del Barrio Industrial de Coquimbo, un túnel de 42 metros de largo, el cual tenía como destino las instalaciones de la empresa de traslado de valores Brink's[8].
5. En diciembre de 2022, en Chile, se produjo un intento de robo a una de las bodegas del Banco Central de Chile, en las que se resguardan monedas. Los dueños de un inmueble

---

[5] Fuente: María Camila Torres Cepeda (05/03/2018). "Cinematográfico robo de dólares en un aeropuerto en Brasil". Consultado el 06 de marzo de 2025 en RCN RADIO. Sitio web: https://www.rcnradio.com/internacional/cinematografico-robo-de-dolares-en-un-aeropuerto-en-brasil

[6] Fuente: Redacción G1 (14/03/2019). "Robo en aeropuerto con bandidos armados con rifles en Carolina del Sur deja una persona muerta y dos heridas". Consultado el 06 de marzo de 2025 en G1 GLOBO. Sitio web: https://g1.globo.com/sc/santa-catarina/noticia/2019/03/14/assalto-com-criminosos-fortemente-armados-em-blumenau-deixa-feridos.ghtml

[7] Fuente: Redacción G1 Campinas (17/10/2019). "Robo en el aeropuerto de Viracopos deja dos personas baleadas y cierra carretera en el interior de SP". Consultado el 06 de marzo de 2025 en G1 GLOBO. Sitio web: https://g1.globo.com/sp/campinas-regiao/noticia/2019/10/17/suspeita-de-assalto-ao-aeroporto-internacional-de-viracopos-em-campinas-mobiliza-pf-ha-informacoes-de-tiroteio.ghtml

[8] Fuente: Redacción La Tercera (19/05/2020). "Coquimbo: PDI detecta túnel subterráneo tras intento de robo a empresa de valores". Consultado el 06 de marzo de 2025 en LA TERCERA. Sitio web: https://www.latercera.com/nacional/noticia/coquimbo-pdi-detecta-tunel-subterraneo-tras-intento-de-robo-a-empresa-de-valores/Y6HUPCLFHJFL5J6HN43NDTKLPU/

colindante a la bodega alertaron a las autoridades sobre un grupo de personas que intentaban realizar un boquete por la pared, hecho que provocó la activación de las alarmas instaladas en la bodega[9].

6. En marzo de 2024, en Estados Unidos, un grupo de delincuentes sustrajo 30 millones de dólares de las instalaciones de la empresa de custodia de valores GardaWorld; en esta instalación se maneja y almacena efectivo de la empresa de toda la región de Los Ángeles. Los ladrones lograron entrar por el techo y por un costado del inmueble, con ello pudieron ingresar hasta la bóveda[10].
7. En junio de 2024, en Brasil, se registró un intento de robo a un vehículo blindado en el aeropuerto de Caxias do Sul que dejó como saldo un policía y un delincuente muerto tras un intercambio de disparos. Los delincuentes estaban armados con rifles y disfrazados de policías federales para ingresar al aeropuerto Hugo Cantergiani y atacar al vehículo blindado[11].
8. En agosto de 2024, en Chile, la sede de la empresa de transportes de valores Brink's en Rancagua fue objeto de un planificado asalto que incluyó autos quemados, corte de rutas y lanzamiento de "miguelitos" (dispositivo de cuatro puntas metálicas afiladas utilizado para detener el avance de diversos vehículos) para impedir la persecución policial. El asalto fue realizado por al menos 20 sujetos armados que llegaron en cuatro vehículos. El monto de lo robado superó los 12 millones de dólares[12].

En México, desde el año 2018 y hasta 2025 se registran al menos 41 pérdidas de vidas humanas como consecuencia de asaltos o tentativas de asaltos a empresas de traslado de valores.

De la información referida, se desprende que las empresas de traslado de valores enfrentan un riesgo latente de sufrir asaltos durante los traslados como en la entrega y resguardo de valores. Aunado a esto,

---

[9] Fuente: CNN Chile (26/12/2022). "Desconocidos intentaron realizar forado cercano a la bodega del Banco Central". Consultado el 06 de marzo de 2025 en CNN CHILE. Sitio web: https://www.cnnchile.com/pais/forado-bodega-banco-central_20221226/

[10] Fuente: Melissa Alonso y Josh Campbell (04/04/2024). "Ladrones roban 30 millones de dólares en efectivo de un depósito de dinero en Los Ángeles: uno de los robos de efectivo más grandes de la ciudad". Consultado el 06 de marzo de 2025 en CNN. Sitio web: https://edition.cnn.com/2024/04/04/us/la-bank-heist-money-storage-facility/index.html

[11] Fuente: Redacción G1 RS (19/06/2024). "Intento de robo a vehículo blindado en el aeropuerto de Caxias do Sul deja policía y sospechoso muertos, dice PM". Consultado el 06 de marzo de 2025 en CNN. Sitio web: https://g1.globo.com/rs/rio-grande-do-sul/noticia/2024/06/19/tentativa-de-assalto-em-carro-forte-no-aeroporto-de-caxias-do-sul-deixa-policial-e-suspeito-mortos-diz-pm.ghtml

[12] Fuente: Mauricio Palazzo (19/08/2024). "Detuvieron a 18 personas tras un espectacular robo a una transportadora de caudales en Chile: se llevaron más de USD 27 millones". Consultado el 06 de marzo de 2025 en INFOBAE. Sitio web: https://www.infobae.com/america/america-latina/2024/08/19/detuvieron-a-18-personas-tras-un-espectacular-robo-a-una-transportadora-de-caudales-en-chile-se-llevaron-mas-de-usd-27-millones/

la delincuencia generalmente busca implementar nuevos mecanismos a través de los cuales vulnerar las medidas de seguridad existentes.

3) Identificable, ya que al tomar en consideración los casos antes expuestos, la delincuencia organizada cuenta con el desarrollo, sofisticación y capacidades operativas avanzadas que pueden realizar este tipo de ataques, y el hecho de hacer pública las actividades de operación referentes al envío y recepción de billete a/de Cajas Regionales y Corresponsales, pondría al alcance de estos grupos las herramientas necesarias para la planeación y ejecución de los mismos.

En efecto, respecto de este rubro, es importante mencionar que en términos del artículo 63, fracción II, de la Ley del Banco de México, este Instituto Central se encuentra obligado a mantener los inmuebles estrictamente indispensables para el desempeño de sus funciones, por lo que la ubicación de estos para llevar a cabo actividades estratégicas del Estado Mexicano, tales como el resguardo, depósito y abastecimiento de valores, así como las operaciones para su puesta en circulación, son fácilmente identificables.

El riesgo de perjuicio que supondría la divulgación de la información supera el interés público general de que se difunda, ya que dar a conocer las actividades de operación referentes al envío y recepción de billete a/de Cajas Regionales y Corresponsales, no aporta un beneficio a la sociedad comparable con el perjuicio de comprometer la seguridad de las instalaciones del Banco Central de la Nación, la vida o salud del personal que participa en las operaciones de traslado del efectivo, la Seguridad Nacional, y el cumplimiento de una actividad estratégica del Estado Mexicano.

En efecto, revelar esta información situaría a las instalaciones y bienes del Banco de México como un blanco fácil de la delincuencia organizada, lo que ocasionaría, como se ha señalado, poner en riesgo la integridad física de los trabajadores del Banco de México, de las autoridades y las Fuerzas Armadas que contribuyen a la seguridad y resguardado de un área considerada estratégica por nuestra Constitución Política, con lo que se perturbaría en forma directa e inmediata a la colectividad.

Así las cosas, es indispensable destacar el grado de importancia que tienen las instalaciones de este Instituto Central y sobre todo, aquellas en donde se encuentra almacenado el efectivo con el que se provee a la economía del Estado Mexicano, por lo que una afectación o interrupción del proceso normal de operación en la distribución y almacenamiento del efectivo, implica un riesgo desestabilizador directo para la Seguridad de la Nación.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que debe prevalecer el interés público de preservar la seguridad en la provisión de moneda nacional al país y evitar cualquier riesgo o amenaza a la seguridad nacional

respecto al beneficio de hacer pública las actividades de operación referentes al envío y recepción de billete a/de Cajas Regionales y Corresponsales, así como su logística. Adicionalmente, el hecho de reservar esta información resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, ya que proporcionarla conlleva el alto riesgo de comprometer la seguridad nacional, asaltos, pérdidas de vidas humanas, alteración de la seguridad en la provisión de moneda nacional y el rediseño de las medidas de seguridad reveladas, costos claramente mayores a los que representaría el beneficio de hacerla del dominio público.

En razón de lo anterior, toda vez que se continuarán empleando por un tiempo indefinido las actividades de operación referentes al envío y recepción de billete a/de Cajas Regionales y Corresponsales materia de la presente prueba de daño, y vistas las consideraciones expuestas en este documento, la clasificación de la información como reservada por un plazo de **cinco años adicionales, contados a partir de la fecha de vencimiento del plazo de reserva actual.**

Por lo antes expuesto, con fundamento en lo dispuesto por los artículos 6, párrafo cuarto, apartado A, fracciones I y VIII, párrafo cuarto, y 28, párrafos séptimo y octavo, de la CPEUM; 1, 2 fracción I, 102, 104, tercer párrafo, 106, 107, 108, 109, 110, 112, fracciones I, IV y V, y 113, de la LGTAIP; 146 de la Ley General del Sistema de Seguridad Nacional; 5, fracción XII, de la Ley de Seguridad Nacional; 2o. y 4o., de la Ley del Banco de México; 4, párrafo primero, 8, párrafos primero y tercero del Reglamento Interior del Banco de México, divulgar las actividades de operación referentes al envío y recepción de billete a/de Cajas Regionales y Corresponsales, está clasificada como **reservada**, toda vez que su divulgación compromete la seguridad nacional, la seguridad en la provisión de moneda nacional al país, además de que pone en riesgo la vida, seguridad y salud de personas físicas.

"ANEXO 9"

BANCO DE MÉXICO®

"2025, Año de la Mujer Indígena"

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DEL PERIODO DE RESERVA

VISTOS, para resolver sobre la ampliación del periodo de reserva de información determinada por la unidad administrativa solicitante, y:

RESULTANDO

I. Que, con la finalidad de cumplir con las obligaciones de transparencia comunes, los sujetos obligados pondrán a disposición del público, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, la información de los temas, documentos y políticas que se señalan en el artículo 65 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

II. Que, del análisis realizado a la información que en su momento fue clasificada como reservada, se han puesto a consideración de este Órgano Colegiado los motivos y fundamentos para ampliar el periodo de reserva próximo a concluir.

III. Que considerando lo anterior, se solicitó al Comité de Transparencia aprobar la ampliación del plazo de reserva de la información, como se indica enseguida:

FECHA O REFERENCIA DEL OFICIO	UNIDAD(ES) ADMINISTRATIVA(S) SOLICITANTE(S) Y NOMBRE(S) DE SU(S) TITULAR(ES)	SOLICITUD DEL OFICIO	INFORMACIÓN CLASIFICADA	PLAZO DE CLASIFICACIÓN
Oficio de fecha 20 de marzo de 2025.	Isabel Morales Pasantes (Dirección de Programación y Distribución de Efectivo del Banco de México.)	Ampliación del plazo de reserva de la información referida en el citado oficio.	**Información reservada** en términos de lo señalado en el oficio y en la prueba de daño correspondiente. *"Actividades de operación referentes al envío y recepción de billete a/de Cajas Regionales y Corresponsales"*	**Plazo de reserva inicial:** 5 años, a partir del 25 de junio de 2020. **Plazo de reserva con ampliación:** 5 años, a partir del 26 de junio de 2025.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva de la información que soliciten los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 40, fracción VII, y 104, párrafo tercero, de la LGTAIP; así como 31, fracción IX, del Reglamento Interior del Banco de México (RIBM).

SEGUNDO. Este Comité de Transparencia, tomando en cuenta que en términos del artículo 106, párrafo segundo de la LGTAIP, advierte que las razones, motivos y circunstancias especiales que llevaron a concluir que en el caso particular se actualiza la necesidad de ampliar el periodo de reserva de la información señalada, se contienen en el oficio referido en el resultando III, así como en la prueba de daño correspondiente, los cuales se tienen aquí por reproducidos como si a la letra se insertasen.[1]

[1] Sirven de referencia los principios de elaboración de sentencias en materia civil, contenidos en la tesis *"SENTENCIA. CUANDO EL JUEZ CITA UNA TESIS PARA FUNDARLA, HACE SUYOS LOS ARGUMENTOS CONTENIDOS EN ELLA. Cuando en una sentencia se cita y transcribe un precedente o una tesis de jurisprudencia, como apoyo de lo que se está resolviendo, el Juez propiamente hace suyos los argumentos de esa tesis que resultan aplicables al caso que se resuelve, sin que se requiera que lo explicite, pues resulta obvio que al fundarse en la tesis recoge los diversos argumentos contenidos en ella."* (Suprema Corte de Justicia de

Al respecto, de conformidad con lo expresado en el oficio señalado en el resultando III, se llevó a cabo una debida ponderación de los intereses en conflicto y se acreditó que el riesgo de perjuicio rebasa el interés público; se acreditó también el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trata; se precisaron las razones por las que la divulgación de la información generaría una afectación a través de los elementos de un riesgo real, demostrable e identificable; y se acreditaron las circunstancias de modo, tiempo y lugar del daño.

En consecuencia, y considerando que, conforme a lo manifestado en la prueba de daño respectiva, la divulgación de la información correspondiente representa: *"(…) un riesgo de perjuicio significativo al interés público, compromete la seguridad nacional, la seguridad en la provisión de moneda nacional al país, y pone en riesgo la vida, seguridad y salud de personas físicas (…)"*, **este Comité de Transparencia aprueba la ampliación al periodo de reserva de la información señalada** de conformidad con lo expresado en el oficio citado en el resultando III de la presente determinación, así como en términos de la prueba de daño correspondiente, **y toma conocimiento del nuevo plazo de reserva determinado por la unidad administrativa.**

Por lo expuesto con fundamento en los artículos 40, fracción VII, y 104, párrafo tercero, de la LGTAIP; 31, fracción IX, del RIBM; y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este Órgano Colegiado:

RESUELVE

ÚNICO. Se aprueba la ampliación al periodo de reserva de la información clasificada como reservada señalada en el oficio mencionado en el resultando III de la presente determinación, conforme a la fundamentación y motivación expresadas en el mismo, así como en la prueba de daño correspondiente, en términos del considerando Segundo de la presente resolución.

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en sesión celebrada el 19 de junio de 2025. ----------

COMITÉ DE TRANSPARENCIA
COMITÉ DE TRANSPARENCIA

_____
JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente
Dirección de Seguridad y Organización de la Información

_____
RODRIGO VILLA COLLINS
Integrante Suplente
Unidad de Transparencia

_____
EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente
Dirección Jurídica

NMDS
PAJC
MDF

la Nación; Registro digital: 192898; Instancia: Pleno; Novena Época; Materias(s): Común; Tesis: P./J. 126/99; Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo X, noviembre de 1999, página 35; Tipo: Jurisprudencia).

Documento firmado digitalmente, su validación requiere hacerse electrónicamente.
Información de las firmas:

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
23/06/2025 11:22:07	Rodrigo Villa Collins	9d310338a465003797e22c4c39b541d3b87cdb541bbfbb9c450e48a47e117701
23/06/2025 11:55:19	JOSE RAMON RODRIGUEZ MANCILLA	b8171a06a391a0d6de670aba05e8afb8bdb3709ec62d33c7750fa63ebd01c924
23/06/2025 12:23:28	Edgar Miguel Salas Ortega	ab85caf2c2654a903825acda24dd224ef84584aa5cceb3ac00e9690362f9b919

"ANEXO 10"

BANCO DE MÉXICO®

"2025, Año de la Mujer Indígena"

Ciudad de México, a 09 de junio de 2025

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
P r e s e n t e.

Me refiero a la obligación prevista en el artículo 56 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), en el sentido de poner a disposición de los particulares la información a que se refiere el Título Quinto de dicho ordenamiento (obligaciones de transparencia) en los respectivos medios electrónicos.

Sobre el particular, en relación con las referidas obligaciones de transparencia, me permito informar que esta unidad administrativa, de conformidad con los artículos 102, y 103, fracción III, de la LGTAIP, ha determinado clasificar diversa información contenida en el documento que se indica en el cuadro siguiente, de conformidad con la fundamentación y motivación señaladas en la carátula y en la prueba de daño correspondiente.

TÍTULO DEL DOCUMENTO CLASIFICADO	TIPO DE CLASIFICACIÓN
NAI Mantenimiento y Administración de equipos e instalaciones en A1, Complejo Jalisco, Hangar y Cajas Regionales del Banco de México (4 de julio de 2025).	Reservada

Por lo expuesto, en términos de los artículos 40, fracción II, de la LGTAIP; y 31, fracción III, del Reglamento Interior del Banco de México, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa.

Asimismo, informo que el personal que por la naturaleza de sus atribuciones tienen acceso al documento referido es el adscrito a:

- Dirección de Infraestructura de Tecnologías de la Información (todo el personal)
- Subgerencia de Operación de Inmuebles (todo el personal)
- Subgerencia de Coordinación de Obras (todo el personal)
- Dirección de Seguridad (Director)
- Gerencia de Prevención y Planeación de Seguridad (Gerente)
- Subgerencia de Prevención y Protección Civil (Subgerente)
- Oficina de Protección Civil (todo el personal).
- Dirección de Fabricación de Billetes (Todo el personal)

Uso Público

Información de acceso público.

- Cajero Regional Guadalajara (Todo el personal)
- Cajero Regional Centro (Todo el personal)
- Subgerencia de Ingeniería Industrial (Todo el personal)
- Subgerencia de Mantenimiento Ciudad de México (Todo el personal)

Atentamente

_____

MARCOS PÉREZ HERNÁNDEZ
Director de Infraestructura de Tecnologías
de la Información

Documento firmado digitalmente, su validación requiere hacerse electrónicamente.
Información de las firmas:

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
09/06/2025 16:23:55	MARCOS PEREZ HERNANDEZ	9180f9c1dbf8416a302898525c9904c333c52c1ec226839bfbdb203d757e847c

"ANEXO 11"

BANCO DE MÉXICO®

"2025, Año de la Mujer Indígena"

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

OBLIGACIONES DE TRANSPARENCIA

Unidad Administrativa: Dirección de Infraestructura de Tecnologías de la Información del Banco de México.

VISTOS, para resolver sobre la clasificación de información determinada por la unidad administrativa al rubro indicada, y:

RESULTANDO

I. Que, con la finalidad de cumplir con las obligaciones de transparencia comunes, los sujetos obligados pondrán a disposición del público, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, la información de los temas, documentos y políticas que se señalan en el artículo 65 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

II. SOLICITUD DE LA UNIDAD ADMINISTRATIVA

Se solicitó al Comité de Transparencia la confirmación de la clasificación de la información, como se indica a continuación:

FECHA O REFERENCIA DEL OFICIO	UNIDAD(ES) ADMINISTRATIVA(S) SOLICITANTE(S) Y NOMBRE(S) DE SU(S) TITULAR(ES)	SOLICITUD DEL OFICIO	INFORMACIÓN CLASIFICADA	VERSIONES PÚBLICAS	PLAZO DE CLASIFICACIÓN
Oficio de fecha 09 de junio de 2025.	Marcos Pérez Hernández (Dirección de Infraestructura de Tecnologías de la Información del Banco de México).	Confirmación de clasificación de información.	**Información reservada** en términos de lo señalado en el oficio y en la prueba de daño correspondiente. *"Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México."*	1 versión pública señalada en el oficio correspondiente.	**Información reservada:** 5 años, a partir de la presente resolución (vencimiento: 19 de junio de 2030).

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las unidades administrativas del Banco de México, de conformidad con lo previsto en los artículos 40, fracción II, de la LGTAIP; y 31, fracción III, del Reglamento Interior del Banco de México (RIBM).

SEGUNDO. Este Comité de Transparencia, tomando en cuenta que en términos del artículo 102, párrafo tercero, de la LGTAIP, corresponde a las personas titulares de las áreas de los sujetos obligados clasificar la información, advierte que las razones, motivos y circunstancias especiales que llevaron a concluir que en el caso particular se actualiza la necesidad de clasificar la información señalada, se contienen en el oficio referido en el resultando II, así como en la prueba de daño correspondiente, los cuales se tienen aquí por reproducidos como si a la letra se insertasen.[1]

De igual manera, de conformidad con lo expresado en el oficio señalado en el resultando II, se llevó a cabo una debida ponderación de los intereses en conflicto y se acreditó que el riesgo de perjuicio rebasa el interés público; se acreditó también el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trata; se precisaron las razones por las que la divulgación de la información generaría una afectación a través de los elementos de un riesgo real, demostrable e identificable; y se acreditaron las circunstancias de modo, tiempo y lugar del daño.

En consecuencia, y considerando que conforme a lo manifestado en la prueba de daño respectiva, la divulgación de la información representa un riesgo: *"(…)* ***de perjuicio significativo al interés público****, ya que con ello se compromete la seguridad nacional; así como la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y comprometería la seguridad en la provisión de moneda nacional al país; toda vez que la divulgación de la información posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional, así como menoscabar la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto; y obstruiría la prevención de delitos informáticos en contra del Banco de México cuya planeación y ejecución se facilitarían (…)",* **este Comité de Transparencia confirma la clasificación de la información señalada como reservada,** de conformidad con lo expresado en el oficio referido en el resultando II de la presente resolución, así como en la prueba de daño correspondiente, y **toma conocimiento del plazo de reserva determinado por la unidad administrativa.**

Por lo expuesto, con fundamento en los artículos 40, fracción II, y 139, párrafo segundo, fracción I, de la LGTAIP; 31, fracción III, del RIBM; así como Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este Órgano Colegiado:

RESUELVE

ÚNICO. Se **confirma la clasificación de la información referida como reservada,** señalada en el oficio citado en el resultando II de la presente determinación, conforme a la fundamentación y

[1] Sirven de referencia los principios de elaboración de sentencias en materia civil, contenidos en la tesis *"SENTENCIA. CUANDO EL JUEZ CITA UNA TESIS PARA FUNDARLA, HACE SUYOS LOS ARGUMENTOS CONTENIDOS EN ELLA. Cuando en una sentencia se cita y transcribe un precedente o una tesis de jurisprudencia, como apoyo de lo que se está resolviendo, el Juez propiamente hace suyos los argumentos de esa tesis que resultan aplicables al caso que se resuelve, sin que se requiera que lo explicite, pues resulta obvio que al fundarse en la tesis recoge los diversos argumentos contenidos en ella."* (Suprema Corte de Justicia de la Nación; Registro digital: 192898; Instancia: Pleno; Novena Época; Materias(s): Común; Tesis: P./J. 126/99; Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo X, noviembre de 1999, página 35; Tipo: Jurisprudencia).

motivación expresadas en el mismo, así como en la prueba de daño correspondiente, en términos del considerando Segundo de la presente resolución.

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en la sesión celebrada el 19 de junio de 2025.----------

COMITÉ DE TRANSPARENCIA

_____

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente
Dirección de Seguridad y Organización de la Información

_____	_____
RODRIGO VILLA COLLINS	**EDGAR MIGUEL SALAS ORTEGA**
Integrante Suplente	**Integrante Suplente**
Unidad de Transparencia	Dirección Jurídica

AMR
URD
MDF

Documento firmado digitalmente, su validación requiere hacerse electrónicamente.
Información de las firmas:

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
23/06/2025 11:22:10	Rodrigo Villa Collins	e8c0d0612b20f98730f37c0eb8e0f2b483f615e30b232e7c446213d88c315833
23/06/2025 11:55:25	JOSE RAMON RODRIGUEZ MANCILLA	6cfa8709081f69ac71fba73b461ecc3822324e72f5fd2b83fdaba02120a6c2d4
23/06/2025 12:23:41	Edgar Miguel Salas Ortega	ff236c0f005b9d7e9d51497b820522e88daab9ee95ab5bf72fd4a6c4472667dc