COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ORDINARIA 23/2025
DEL 26 DE JUNIO DE 2025

A las trece horas del 26 de junio de 2025, participan en la presente sesión a través de medios electrónicos de comunicación, Claudia Tapia Rangel, Titular de la Unidad de Transparencia; Víctor Manuel De La Luz Puebla, Director de Seguridad y Organización de la Información; 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 29 de abril de 2025 (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 del Banco de México, 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 QUIENES SON TITULARES DE LA GERENCIA DE CONTINUIDAD, CONTROL Y SOPORTE DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS Y DE LA SUBGERENCIA DE SOPORTE DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, AMBAS UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE OPERACIÓN Y CONTINUIDAD DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, A SU VEZ ADSCRITA A LA DIRECCIÓN GENERAL DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO 6110000014020. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura a los dos oficios de fecha 16 de abril de 2025, suscritos por quienes son titulares de la Gerencia de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados y de la Subgerencia de Soporte de Sistemas de Pagos e Infraestructuras de Mercados, ambas unidades administrativas adscritas a la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, a su vez adscrita a la Dirección General de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, los cuales se agregan en un solo legajo a la presente Acta como **"ANEXO 2",** por medio de los cuales hicieron del conocimiento de este Comité de Transparencia la determinación de ampliar el periodo de reserva de la información señalada en dichos oficios, de conformidad con la fundamentación y motivación expresadas en los mismos, así como en las pruebas de daño correspondientes, y solicitaron a este órgano colegiado aprobar dicha 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 QUIENES SON TITULARES DE LA GERENCIA DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA SUBGERENCIA DEL CENTRO DE DEFENSA DE CIBERSEGURIDAD, AMBAS UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE SEGURIDAD Y ORGANIZACIÓN DE LA INFORMACIÓN, A SU VEZ ADSCRITA A LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO 6110000028220.----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de fecha 29 de abril de 2025, suscrito por quienes son titulares de la Gerencia de Seguridad de Tecnologías de la Información y de la Subgerencia del Centro de Defensa de Ciberseguridad, ambas unidades administrativas adscritas a la Dirección de Seguridad y Organización de la Información, a su vez adscrita a la Dirección General de Tecnologías de la Información del Banco de México, el cual se agrega a la presente Acta como **"ANEXO 4",** por medio del cual hicieron del conocimiento de este Comité de Transparencia la determinación de ampliar el periodo de reserva de la información señalada en dicho oficio, de conformidad con la fundamentación y motivación expresadas en el mismo, así como en la prueba de daño correspondiente, y solicitaron a este órgano colegiado aprobar dicha 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 QUIENES SON TITULARES DE LA GERENCIA DE CONTINUIDAD, CONTROL Y SOPORTE DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS Y DE LA SUBGERENCIA DE SOPORTE DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, AMBAS UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE OPERACIÓN Y CONTINUIDAD DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, A SU VEZ ADSCRITA A LA DIRECCIÓN GENERAL DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO CTC-BM-30250. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de fecha 16 de abril de 2025, suscrito por quienes son titulares de la Gerencia de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados y de la Subgerencia de Soporte de Sistemas de Pagos e Infraestructuras de Mercados, ambas unidades administrativas adscritas a la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, a su vez adscrita a la Dirección General 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 hicieron del conocimiento de este Comité de Transparencia la determinación de ampliar el periodo de reserva de la información señalada en dicho oficio, de conformidad con la fundamentación y motivación expresadas en el mismo, así como en la prueba de daño correspondiente, y solicitaron a este órgano colegiado aprobar dicha 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 QUIENES SON TITULARES DE LA GERENCIA DE CONTINUIDAD, CONTROL Y SOPORTE DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN DE OPERACIÓN Y CONTINUIDAD DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, DE LA GERENCIA DE TECNOLOGÍAS INNOVADORAS DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN DE DESARROLLO E INNOVACIÓN DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, A SU VEZ ADSCRITAS A LA DIRECCIÓN GENERAL DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS; ASÍ COMO DE LA GERENCIA DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA SUBGERENCIA DEL CENTRO DE DEFENSA DE CIBERSEGURIDAD, AMBAS UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE SEGURIDAD Y ORGANIZACIÓN DE LA INFORMACIÓN, A SU VEZ ADSCRITA A LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN, TODAS ELLAS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO 6110000014620.----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de fecha 21 de mayo de 2025, suscrito por quienes son titulares de la Gerencia de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados, unidad administrativa adscrita a la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, de la Gerencia de Tecnologías Innovadoras de Sistemas de Pagos e Infraestructuras de Mercados, unidad administrativa adscrita a la Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructuras de Mercados, a su vez adscritas a la Dirección General de Sistemas de Pagos e Infraestructuras de Mercados; así como de la Gerencia de Seguridad de Tecnologías de la Información y de la Subgerencia del Centro de Defensa de Ciberseguridad, ambas unidades administrativas adscritas a la Dirección de Seguridad y Organización de la Información, a su vez adscrita a la Dirección General de Tecnologías de la Información, todas ellas del Banco de México, el cual se agrega a la presente Acta como **"ANEXO 8",** por medio del cual hicieron del conocimiento de este Comité de Transparencia la determinación de ampliar el periodo de reserva de la información señalada en dicho oficio, de conformidad con la fundamentación y motivación expresadas en el mismo, así como en las pruebas de daño correspondientes, y solicitaron a este órgano colegiado aprobar dicha 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. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE OPERACIONES INTERNACIONALES, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN GENERAL DE OPERACIONES DE BANCA CENTRAL DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO 6110000013320.----------

Quien ejerce en este acto las funciones de Secretariado dio lectura a los dos oficios de fecha 28 de mayo de 2025, suscritos por quien es titular de la Dirección de Operaciones Internacionales, unidad administrativa adscrita a la Dirección General de Operaciones de Banca Central del Banco de México, los cuales se agregan en un solo legajo a la presente Acta como **"ANEXO 10",** por medio de los cuales

hicieron del conocimiento de este Comité de Transparencia la determinación de ampliar el periodo de reserva de la información señalada en dichos oficios, de conformidad con la fundamentación y motivación expresadas en los mismos, así como en la prueba de daño correspondiente, y solicitaron a este órgano colegiado aprobar dicha 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 11"**.

SEXTO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA GERENCIA DE TECNOLOGÍAS INNOVADORAS DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS Y DE LA GERENCIA DE DESARROLLO TECNOLÓGICO DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE DESARROLLO E INNOVACIÓN DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, A SU VEZ ADSCRITA A LA DIRECCIÓN GENERAL DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS; ASÍ COMO DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN, DE LA GERENCIA DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA SUBGERENCIA DEL CENTRO DE DEFENSA DE CIBERSEGURIDAD, AMBAS UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE SEGURIDAD Y ORGANIZACIÓN DE LA INFORMACIÓN, A SU VEZ ADSCRITAS A LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN, TODAS ELLAS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO 6110000028120. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de fecha 21 de mayo de 2025, suscrito por quienes son titulares de la Gerencia de Tecnologías Innovadoras de Sistemas de Pagos e Infraestructuras de Mercados y de la Gerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados, ambas unidades administrativas adscritas a la Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructuras de Mercados, a su vez adscrita a la Dirección General de Sistemas de Pagos e Infraestructuras de Mercados; así como de la Dirección de Infraestructura de Tecnologías de la Información, de la Gerencia de Seguridad de Tecnologías de la Información y de la Subgerencia del Centro de Defensa de Ciberseguridad, ambas unidades administrativas adscritas a la Dirección de Seguridad y Organización de la Información, a su vez adscritas a la Dirección General de Tecnologías de la Información, todas ellas del Banco de México, el cual se agrega a la presente Acta como **"ANEXO 12",** por medio del cual hicieron del conocimiento de este Comité de Transparencia la determinación de ampliar el periodo de reserva de la información señalada en dicho oficio, de conformidad con la fundamentación y motivación expresadas en el mismo, así como en las pruebas de daño correspondientes, y solicitaron a este órgano colegiado aprobar dicha 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 13"**.

Al no haber más asuntos que tratar, se da por terminada la sesión a las trece horas con veinte 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

_____

CLAUDIA TAPIA RANGEL
Integrante
Unidad de Transparencia

_____

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante
Dirección de Seguridad y Organización de la Información

_____

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente
Dirección Jurídica

_____

SERGIO ZAMBRANO HERRERA
Secretario

AMR
URD
MDF

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
27/06/2025 18:31:13	SERGIO ZAMBRANO HERRERA	faaa30efc51699cb920b234733f0e04789f06c5df95e36d2988b6bcb2da6361a
27/06/2025 19:15:04	Edgar Miguel Salas Ortega	9ac196a76e74c5dcfa8bd952608d394dead5f29c4485c967e36536d20b360c2e
27/06/2025 20:20:53	VICTOR MANUEL DE LA LUZ PUEBLA	ba37fd8e950fc82a41ebad1d30a9896abf8408627ed6e20744f1b4dca9e6a8fe
30/06/2025 09:26:51	Claudia Tapia Rangel	165d88d122d8a962a12b45361b8fe7bb04c6caa8544e326517b1a9375ea0a2e6

"ANEXO 1"

BANCO DE MÉXICO®

"2025, Año de la Mujer Indígena"

COMITÉ DE TRANSPARENCIA

ORDEN DEL DÍA

SESIÓN ORDINARIA 23/2025
26 DE JUNIO DE 2025

PRIMERO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA GERENCIA DE CONTINUIDAD, CONTROL Y SOPORTE DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS Y DE LA SUBGERENCIA DE SOPORTE DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, AMBAS UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE OPERACIÓN Y CONTINUIDAD DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, A SU VEZ ADSCRITA A LA DIRECCIÓN GENERAL DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO **6110000014020.**

SEGUNDO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA GERENCIA DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA SUBGERENCIA DEL CENTRO DE DEFENSA DE CIBERSEGURIDAD, AMBAS UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE SEGURIDAD Y ORGANIZACIÓN DE LA INFORMACIÓN, A SU VEZ ADSCRITA A LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO **6110000028220.**

TERCERO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA GERENCIA DE CONTINUIDAD, CONTROL Y SOPORTE DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS Y DE LA SUBGERENCIA DE SOPORTE DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, AMBAS UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE OPERACIÓN Y CONTINUIDAD DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, A SU VEZ ADSCRITA A LA DIRECCIÓN GENERAL DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO **CTC-BM-30250.**

CUARTO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA GERENCIA DE CONTINUIDAD, CONTROL Y SOPORTE DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN DE OPERACIÓN Y CONTINUIDAD DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, DE LA GERENCIA DE TECNOLOGÍAS INNOVADORAS DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN DE DESARROLLO E INNOVACIÓN DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, A SU VEZ ADSCRITAS A LA DIRECCIÓN GENERAL DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS; ASÍ COMO DE LA GERENCIA DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA SUBGERENCIA DEL CENTRO DE DEFENSA DE CIBERSEGURIDAD, AMBAS UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE SEGURIDAD Y ORGANIZACIÓN DE LA INFORMACIÓN, A SU VEZ ADSCRITA A LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN, TODAS ELLAS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO **6110000014620.**

QUINTO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE OPERACIONES INTERNACIONALES, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN GENERAL DE OPERACIONES DE BANCA CENTRAL DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO **6110000013320.**

SEXTO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA GERENCIA DE TECNOLOGÍAS INNOVADORAS DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS Y DE LA GERENCIA DE DESARROLLO TECNOLÓGICO DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE DESARROLLO E INNOVACIÓN DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS, A SU VEZ ADSCRITA A LA DIRECCIÓN GENERAL DE SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS; ASÍ COMO DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN, DE LA GERENCIA DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA SUBGERENCIA DEL CENTRO DE DEFENSA DE CIBERSEGURIDAD, AMBAS UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE SEGURIDAD Y ORGANIZACIÓN DE LA INFORMACIÓN, A SU VEZ ADSCRITAS A LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN, TODAS ELLAS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON NÚMERO DE FOLIO **6110000028120.**

"ANEXO 2"

BANCO DE MÉXICO®

"2025, Año de la mujer indígena"

Ciudad de México, 16 de abril de 2025

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

Nos referimos a la clasificación de reserva realizada, en su momento, para la atención de una solicitud de acceso a la información por la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, respecto de diversa información contenida en los documentos que se señalan a continuación:

TÍTULO DEL DOCUMENTO CLASIFICADO
Correo CASP Oficio: D50/1107-2018
Correo CASP Oficio: D50/1028-2018
Correo CASP Oficio: D50/1029-2018
Correo CASP Oficio: D50/1108-2018
Correo CASP Oficio: D50/1272-2018
Correo CASP Oficio: D50/1485-2018

Al respecto, nos permitimos resaltar que dicha clasificación fue confirmada por el Comité de Transparencia mediante resolución de 20 de agosto de 2020, emitida en la sesión ordinaria 27/2020, en términos de la fundamentación y motivación expresadas en el oficio con referencia D40-040-2020 del 14 de agosto de 2020, suscrito por la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, 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 20 de agosto de 2020 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **20 de agosto 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 Ter, del Reglamento Interior del Banco de México (RIBM); Segundo, fracción XVII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; nos permitimos informarles que estas unidades administrativas **estiman 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 las pruebas de daño correspondientes, que se ponen a disposición de ese Comité de Transparencia.**

Por lo expuesto, y con fundamento en el artículo 104, párrafo tercero, de la LGTAIP; **solicitamos 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, informamos 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 Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados (Director), Gerencia de Operación de Sistemas de Pagos e Infraestructuras de Mercados (Gerente), Gerencia de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados (Gerente) y Subgerencia de Continuidad y Gestión de Sistemas de Pagos e Infraestructuras de Mercados (Subgerente).

Atentamente

ANA LAURA MORALES GUZMÁN
Gerente de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados

VICTOR ENRIQUE TAPIA TEC
Subgerente de Soporte de Sistemas de Pagos e Infraestructuras de Mercados

BANCO DE MÉXICO®
RECIBIDO
16 ABR 2025
Comité de Transparencia
Por: E19807 Hora: 12:00

PRUEBA DE DAÑO

INFORMACIÓN QUE PUEDE HACER IDENTIFICABLE A LOS PARTICIPANTES DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS (SPEI®) QUE ESTUVIERON INVOLUCRADOS DE MANERA DIRECTA O INDIRECTA EN LOS EVENTOS DE ABRIL DE 2018 Y CON LOS CUALES SE INTERCAMBIARON COMUNICACIONES EN EL PERIODO DE ABRIL 2018 AL 31 DE DICIEMBRE DE 2018.

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 (en adelante, CPEUM); 112, fracciones IV y VII, de la Ley General de Transparencia y Acceso a la información Pública (en adelante, LGTAIP); es de clasificarse como información reservada aquella que pueda:

- Afectar la efectividad de 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 sistémico 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, 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.

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.

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, necesita mantener el cuidado de la información que pudiera afectar el buen funcionamiento de los sistemas de pagos. En ese sentido, 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 que puede hacer identificable a los Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI®) y que estuvieron involucrados de manera directa o indirecta en los eventos de abril de 2018 y con los cuales se intercambiaron comunicaciones en el periodo de abril 2018 al 31 de diciembre 2018,** podría disminuir la efectividad de las medidas que en su caso fueron adoptadas dificultando la consecución de su objetivo, podría menoscabar la efectividad de las medidas implementadas en el sistema financiero y económico del país, poniendo en riesgo el funcionamiento de esos sistemas; o bien, otorgaría una ventaja indebida, generando distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pagos; toda vez que dicho riesgo es:

1) **Real**, ya que revelar o divulgar información que puede hacer identificable a los Participantes del SPEI® que estuvieron involucrados de manera directa o indirecta en los eventos de abril de 2018, permitiría inferir brechas en la operación de los Participantes o vulnerabilidades que podrían ser utilizadas para diseñar estrategias operativas o tecnológicas que pudieran afectar la infraestructura de la entidad, o en un caso extremo la infraestructura del Banco de México, lo que podría derivar en la detección de posibles debilidades en los procesos de los participantes y, por ende, impactar en el buen funcionamiento del sistema, o bien podría posibilitar la realización de acciones hostiles por parte de una persona o grupo con intenciones delincuenciales en contra de dichos participantes.

   Adicionalmente, al identificar a los participantes del SPEI® que estuvieron involucrados de manera directa o indirecta en los eventos de abril de 2018, se podrían relacionar los mecanismos de operación con el participante, lo cual podría ser utilizado por otro participante, un cliente o un usuario mal intencionado para obtener una ventaja del proceso o detección de vulnerabilidades identificadas en el Participante en concreto, permitiendo a cibercriminales la realización de acciones hostiles en contra de estos participantes, aprovechando los puntos débiles identificados y enfocar ataques en contra de esos elementos.

   En consecuencia, la información referida actualiza las causales de reserva previstas en el artículo 112, fracciones IV y VII, de la LGTAIP, toda vez que su divulgación podría afectar las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, o bien podría obstruir en la prevención de delitos.

2) **Demostrable.** ya que se considera **demostrable que los sistemas de pagos de bancos centrales han sufrido ataques cibernéticos a través de estas infraestructuras**, que los sistemas de pagos están siendo víctimas de ciberataques sin precedente, de forma constante y organizada. Dichos ataques tienen por objeto el robo de recursos económicos a través del empleo de vulnerabilidades en las instituciones, aplicativos e infraestructura tecnológica de los sistemas. Lo anterior se puede ejemplificar con el ataque ocurrido a las instituciones financieras participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI®), el cual consistió en la fabricación o inyección de órdenes de transferencia apócrifas en los sistemas de los participantes donde se procesan las instrucciones de pago de los participantes, los atacantes vulneraron la infraestructura tecnológica de los participantes y generaron órdenes de transferencias ilegitimas.[1] Al 22 de mayo de 2018, se estimó un daño a los participantes del SPEI® de aproximadamente 300 millones de pesos.[2]

[1] Banco de México. "Información sobre los ataques a los Participantes del SPEI". https://www.banxico.org.mx/spei/d/%7BFFC53F5A-CA04-3098-EBF6-B0F17E533183%7D.pdf, consultado el 09 de abril de 2025.

[2] Acorde con los "Puntos importantes sobre la situación actual del SPEI" publicados en la página de internet del Banco de. http://www.banxico.org.mx/spei/d/%7BB806F1E8-686D-B9F1-0452-EC375543C801%7D.pdf, consultado el 09 de abril de 2025.

En ese sentido, también es de destacar que una afectación a la reputación de cualquier entidad tiene un impacto moral y económico, si no es controlado de manera correcta, puede terminar impactando su entorno. Tratándose de entidades financieras, la afectación en la reputación de un participante que se podría ocasionar por proporcionar la información que se está clasificando podría representar una ventaja indebida para un competidor malintencionado que, dependiendo del alcance de su interpretación, podría tener un impacto en el participante, SPEI® o en mayor escala, en el sistema financiero mexicano.

Por otra parte, en los últimos años se ha observado un incremento sostenido de ataques informáticos en el sector financiero, **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.[3]

En este sentido, la divulgación de la información materia de la presente prueba de daño, al estar en posesión de personas no autorizadas, puede facilitar que sea utilizada para impactar la operación de los participantes del SPEI® en la infraestructura y como institución financiera, en beneficio de terceros y en perjuicio del patrimonio de los participantes, generando distorsiones en la estabilidad del sistema de pagos denominado SPEI®.

3) Identificable, ya que, a la fecha de realización de la presente prueba de daño, es un hecho notorio que los sistemas de pagos atraen la atención del público en general ya que están siendo objeto de ciberataques a gran escala; una disrupción en los servicios provistos por los sistemas de pagos o de sus participantes, tendría repercusiones directas para una gran cantidad de empresas y comercios, que podrían ser utilizadas por terceros para impactar el funcionamiento de los sistemas de pagos.

Por lo anterior, un ataque perpetrado directamente al SPEI® o a sus participantes, ocasionado por dar a conocer el nombre de los participantes que se vieron involucrados en los eventos de abril de 2018 a que refiere la presente prueba de daño, representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues de acuerdo con la información del Banco de México, de febrero de 2024 a enero de 2025 se realizaron aproximadamente 5,155 millones de pagos electrónicos interbancarios por un monto de aproximadamente 329 billones de pesos; ahora bien y específicamente para el mes de enero de 2025 se realizaron aproximadamente 481 millones de operaciones en un mes, por un monto promedio de 60 mil pesos por operación, únicamente para lo que respecta a este sistema.[4]

Con base en estas cifras, es evidente que un ataque al SPEI® o a sus Participantes, sin importar la duración de la disrupción, puede llegar a tener efectos cuantiosos sobre la actividad económica del país y sobre el patrimonio de los usuarios de estos servicios.

Adicionalmente, **el riesgo de perjuicio que supondría la divulgación de la información, supera el interés público general de que se difunda**, pues el interés público se centra en que no se comprometa la efectividad

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

[4] Banco de México. Sistemas de pago de bajo valor, Transferencias SPEI por monto operado (CF620), https://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=21&accion=consultarCuadro&idCuadro=CF620&locale=es, consultado el 09 de abril 2025.

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, la estabilidad en los mercados financieros y en los sistemas de pagos. Por lo que, la información, no satisface un interés público, por el contrario, es información que pone en riesgo el buen funcionamiento de los sistemas de pagos y de la economía nacional en su conjunto. 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 y los sistemas de pagos administrados por éste, en particular el SPEI®.

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 obtener una ventaja indebida sobre otros participantes del sistema o se menoscabe la efectividad de las medidas implementadas en los sistemas financiero, así como permitir planear y perpetrar ataques cibernéticos dirigidos en contra de dichos participantes, lo cual tenga como resultado la creación de mecanismos que faciliten el acceso indebido, la sustracción de información – como datos personales referente a sus usuarios y las operaciones que realizan-, la alteración de las órdenes de transferencias de dichos participantes y que son enviadas a otros participantes del SPEI®. 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 adecúa 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 de los sistemas de pagos, del sistema financiero y de la economía nacional en su conjunto, así como prevención de delitos.**

Asimismo, **reservar la información en cuestión representa el medio menos restrictivo disponible para evitar el perjuicio**, en aras salvaguardar el buen funcionamiento de los sistemas de pagos, así como la estabilidad 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.

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 a la protección de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de los participantes, o en un caso extremo los sistemas de pagos del Banco de México, por lo que, en caso de revelarse, podría derivar en la detección de posibles debilidades en los procesos de los participantes y, por ende, impactar en el buen funcionamiento del sistema, o bien podría posibilitar la realización de acciones hostiles por parte de una persona o grupo con intenciones delincuenciales en contra de dichos participantes. Asimismo, y dada la importancia sistémica de los sistemas de pagos, estos continuarán 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, 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 que puede hacer identificable a los Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI®) que estuvieron involucrados de***

manera directa o indirecta en los eventos de abril de 2018 y con los cuales se intercambiaron comunicaciones en el periodo de abril 2018 al 31 de diciembre de 2018, toda vez que, como se ha manifestado esta acción atiende a la protección de la información de saber a quién de los participantes en el sistema de pagos se le compartió dicha información, con la finalidad de evitar utilizar la información contenida en las comunicaciones de manera errónea sin conocer el contexto de dicha información y que como consecuencia de su mal uso otorgue una ventaja indebida, generando distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pagos, o bien, en caso de revelarse, permitiría afectar 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 y comprometería las acciones encaminadas a la prevención de delitos.

PRUEBA DE DAÑO

INFORMACIÓN RELACIONADA CON PROCESOS DE CONTINUIDAD OPERATIVA Y DE CONTINGENCIA, ESPECIFICACIONES TÉCNICAS Y DE SEGURIDAD INFORMÁTICA QUE SOPORTAN EL FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS QUE ADMINISTRA, OPERA Y SUPERVISA EL BANCO DE MÉXICO.

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 (en adelante, CPEUM); así como 112, fracciones IV y VII, de la Ley General de Transparencia y Acceso a la información Pública (en adelante LGTAIP); es de clasificarse como información reservada aquella que pueda:

- Afectar la efectividad de 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 sistémico 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 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.

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.

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.**

El dar a conocer la ***información relacionada con procesos de continuidad operativa y de contingencia, especificaciones técnicas y de seguridad informática que soportan el funcionamiento de los sistemas de pagos que administra, opera y supervisa el Banco de México***, 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, aspectos de especificaciones técnicas, así como toda información que de forma aislada o agrupada, permita vincular directa o indirectamente, algún elemento específico de los sistemas de pagos que administra, opera y supervisa el Banco de México, podría disminuir la efectividad de las medidas que en su caso fueran adoptadas dificultando la consecución de su objetivo, retrasando la estabilización en los mercados financieros, dañando el funcionamiento de los sistemas de pagos e inclusive generando una mayor inestabilidad.

En ese orden de ideas, se precisa que la divulgación de la citada información representa un riesgo de perjuicio significativo al interés público ya que, menoscabaría 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; generaría incumplimiento en 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; 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**, en razón de revelar o divulgar la información, **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, procesos de continuidad operativa y de contingencia y, en general, información relacionada con la infraestructura informática de los sistemas de pago administrados por este Instituto Central, lo cual posibilita la realización de acciones hostiles en contra de las tecnologías de la información y protocolos de comunicación que establece este Banco Central** en los sistemas de pagos que éste administra, opera y supervisa, 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, debido a **que los delincuentes podrían diseñar estrategias para llevar a cabo ataques cibernéticos** dirigidos específicamente a los sistemas de pagos que administra el Banco Central, así como sabotajes a la estructura y elementos físicos, 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.

   Por lo anterior, exponer a los participantes de las Infraestructuras de los Mercados Financieros (IMF) así como al Banco Central que las administra, opera y supervisa, a estos riesgos cibernéticos **puede perturbar considerablemente al sistema financiero por su efecto directo en la información y operaciones relativas a los usuarios de los sistemas de pagos -tanto de las instituciones financieras como de las personas físicas y morales-.**

   Incluso, los ataques cibernéticos pueden provocar la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de estos sistemas, lo cual pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de las IMF, entre ellas los sistemas de pagos.

En efecto, revelar la información materia de la presente prueba de daño**, facilitaría que terceros logren acceder a información financiera o personal**, 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 vulnerabilidades de dichos sistemas, 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]

Sea cual fuere el origen o motivación del ataque en contra de la infraestructura utilizada para operar los sistemas de pagos, éste puede conducir al incumplimiento de las obligaciones del Banco Central hacia el sistema financiero y provocar **un colapso nacional de los sistemas de pagos, lo que actualizaría una contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.**

En el caso en concreto, la información materia de esta prueba de daño contiene información **relacionada con especificaciones técnicas en materia de seguridad, procesos de continuidad operativa, información sobre los componentes de los sistemas informáticos así como especificaciones de equipos de cómputo y telecomunicaciones, especificaciones respecto de los servicios prestados en materia de seguridad informática así como las condiciones de los mismos, horarios de operación, protocolos de comunicación, entre otros,** por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales aprovechar los aparentes puntos débiles y en consecuencia llevar a cabo ataques más certeros con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes a través de estas infraestructuras.

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]

---

[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.

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

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, en 2022 **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 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 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.[9]

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 específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero.[10] A la fecha de publicación de dicho comunicado, se estimó un daño a los participantes del SPEI® de aproximadamente 300 millones de pesos.[11]

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.[12]

---

[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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 2025.

[10] 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 09 de abril 2025.

[11] 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 09 de abril 2025.

[12] 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 09 de abril 2025.

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, 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 entonces 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

[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 09 de abril 2025.

[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 09 de abril 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 09 de abril 2025.

[16] INAI, Comunicado INAI/296/22 "Datos personales en riesgo de estar comprometidos por ataque cibernético a Sedena: INAI", 30 septiembre 2022, disponible en: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-296-22.pdf, consultado el 09 de abril 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 09 de abril 2025.

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 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]

---

[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 09 de abril 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 del 09 de abril 2025.

[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 del 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 2025.

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 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**.[25]

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.[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, ya que, a la fecha de realización de la presente prueba de daño, es un hecho notorio que los sistemas de pagos están siendo objeto de ciberataques a gran escala, como quedó demostrado en la sección anterior. 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 los sistemas de pagos 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 proporcionar la información materia de la presente prueba de daño, podría resultar en la afectación de las órdenes de transferencia en las**

---

[24] Offensive Security, INFORMATION GATHERING IN METASPLOIT, disponible en: https://www.offensive-security.com/metasploit-unleashed/information-gathering/, consultado el 09 de abril 2025.

[25] Riquelme, Rodrigo, "*El sistema financiero mexicano fue víctima 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 09 de abril 2025.

[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 09 de abril 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 09 de abril 2025.

cuentas bancarias de los distintos participantes y de los usuarios del sistema en comento. A su vez, estas afectaciones en las órdenes de transferencia podrían derivar en una pérdida de patrimonio no sólo para las instituciones financieras del país y demás participantes de los sistemas de pagos, sino en perjuicio de la población usuaria de los pagos electrónicos interbancarios, es decir **millones de personas físicas y morales, incluyendo aquellos empleados del sector público o privado que reciben su pago de salario vía transferencia electrónica que realizan sus patrones.**

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, un ataque perpetrado directamente a alguno de los sistemas de pagos administrados y operados por este Banco Central, ocasionado por dar a conocer la información objeto de la presente prueba de daño, representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues, por ejemplo, de acuerdo con la información disponible respecto del SPEI®, de febrero de 2024 a enero de 2025 se realizaron aproximadamente 5,155 millones de pagos electrónicos interbancarios por un monto de aproximadamente 329 billones de pesos; ahora bien y específicamente para el mes de enero de 2025 se realizaron aproximadamente 481 millones de operaciones en un mes, por un monto promedio de 60 mil pesos por operación, únicamente para lo que respecta a este sistema.[28]

Con base en estas cifras, es evidente que un ataque cibernético que vulnere la operación de los sistemas de pagos, sus tecnologías de la información y de comunicaciones, o la de sus participantes, sin importar la duración de la disrupción, puede llegar a tener efectos cuantiosos sobre la actividad económica del país y sobre el patrimonio de los usuarios de estos servicios; en especial, si este ocurre en alguno de los días de mayor actividad económica en el año, fechas particulares en que el número y monto de las operaciones se incrementa considerablemente.

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, la estabilidad en los mercados financieros y en los sistemas de pagos. Por lo que, **la información, no satisface un interés público, por el contrario, es información que pone en riesgo el buen funcionamiento de los sistemas de pagos y de la economía nacional en su conjunto.** 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

[28] Banco de México. Sistemas de pago de bajo valor, Transferencias SPEI por monto operado (CF620), https://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=21&accion=consultarCuadro&idCuadro=CF620&locale=es, consultado el 09 de abril 2025.

personas, esto es, **beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste, en particular el SPEI®.**

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 los sistemas de pagos administrados, operados y supervisados por el 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 -, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes 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 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.**

Asimismo, **reservar la información en cuestión representa el medio menos restrictivo disponible para evitar el perjuicio**, en aras salvaguardar el buen funcionamiento de los sistemas de pagos, así como la estabilidad 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.

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 a la protección de las medidas de seguridad informática, continuidad operativa y de contingencia, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques. Asimismo, y dada la importancia sistémica de los sistemas de pagos, estos continuarán 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, 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 procesos de continuidad operativa y de contingencia, especificaciones técnicas y de seguridad informática que soportan el funcionamiento de los sistemas de pagos que administra, opera y supervisa el Banco de México,** toda vez que, como se ha manifestado esta acción atiende a la protección de las medidas de seguridad informática, procedimientos de continuidad operativa y de contingencia, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos, no solo de las supuestas vulnerabilidades identificadas sino de aquellas que no se encuentran reconocidas provocando afectaciones a las IMF que opera y administra este Instituto Central, entre ellas los sistemas de pagos, lo cual menoscabaría 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; así como

podría generar incumplimiento en 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 y comprometería las acciones encaminadas a la prevención de delitos.

BANCO DE MÉXICO®

"2025, Año de la mujer indígena"

Ciudad de México, 16 de abril de 2025

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

Nos referimos a la clasificación de reserva realizada, en su momento, para la atención de una solicitud de acceso a la información por la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, respecto de diversa información contenida en los documentos que se señalan a continuación:

TÍTULO DEL DOCUMENTO CLASIFICADO
Oficio 24 de abril de 2018
Oficio: D50/1029-2018
Oficio D50/1107-2018
Antecedente: oficio: D50/1107-2018 de fecha 20 de junio de 2018
Oficio: D50/1272-2018
Antecedente: oficio: D50/1272-2018 de fecha 03 de julio de 2018
Antecedentes: Of. N° D50/1029-2018, de 14 Jun. 2018 y Of. N°D50/1272-2018, de 03 Jul. 2018
Oficio 21 de noviembre 2018 en respuesta al oficio D50/1029-2018
Oficio: D50/2219-2018
Antecedente; Oficio No. D50/2219-2018 de 21 de noviembre de 2018
Oficio: D50/2252-2018
Oficio de fecha 26 de abril 2018
Oficio: D50/1028-2018
Oficio: D50/1108-2018
Respuesta a Oficio: D50/1108-2018
Oficio: D50/1485-2018

Respuesta a Oficio No. D50/1028-2018
Oficio: D50/1655-2018
Respuesta a Oficio Ref.: D50/1655-2018
Oficio: D50/1750-2018
Informe de inicio de operaciones de conformidad con el Oficio D50/1750-2018
Oficio: D50/1882-2018
Informe de inicio de operaciones SPEI de conformidad con el Oficio D50/1750-2018
Oficio: D50/1932-2018
Comunicado CASP del 17 abril 2018
Alcance Comunicado CASP 24 de abril 2018
Comunicado CASP 26 abril 2018

Al respecto, nos permitimos resaltar que dicha clasificación fue confirmada por el Comité de Transparencia mediante resolución de 23 de julio de 2020, emitida en la sesión ordinaria 24/2020, en términos de la fundamentación y motivación expresadas en el oficio con referencia D40-033-2020 del 17 de julio de 2020, suscrito por la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, 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 23 de julio de 2020 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **23 de julio 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 Ter, del Reglamento Interior del Banco de México (RIBM); Segundo, fracción XVII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; nos permitimos informarles que estas unidades administrativas **estiman 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 las pruebas de daño correspondientes, que se ponen a disposición de ese Comité de Transparencia.**

Por lo expuesto, y con fundamento en el artículo 104, párrafo tercero, de la LGTAIP; **solicitamos 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, informamos 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 Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados (Director), Gerencia de Operación de Sistemas de Pagos e Infraestructuras de Mercados (Gerente), Gerencia de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados (Gerente) y Subgerencia de Continuidad y Gestión de Sistemas de Pagos e Infraestructuras de Mercados (Subgerente).

Atentamente

ANA LAURA MORALES GUZMÁN
Gerente de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados

VICTOR ENRIQUE TAPIA TEC
Subgerente de Soporte de Sistemas de Pagos e Infraestructuras de Mercados

BANCO DE MÉXICO®
RECIBIDO
16 ABR 2025
Comité de Transparencia
Por: E/9807 Hora: 12:00

PRUEBA DE DAÑO

INFORMACIÓN QUE PUEDE HACER IDENTIFICABLE A LOS PARTICIPANTES DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS (SPEI®) QUE ESTUVIERON INVOLUCRADOS DE MANERA DIRECTA O INDIRECTA EN LOS EVENTOS DE ABRIL DE 2018 Y CON LOS CUALES SE INTERCAMBIARON COMUNICACIONES EN EL PERIODO DE ABRIL 2018 AL 31 DE DICIEMBRE DE 2018.

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 (en adelante, CPEUM); 112, fracciones IV y VII, de la Ley General de Transparencia y Acceso a la información Pública (en adelante, LGTAIP); es de clasificarse como información reservada aquella que pueda:

- Afectar la efectividad de 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 sistémico 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, 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.

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.

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, necesita mantener el cuidado de la información que pudiera afectar el buen funcionamiento de los sistemas de pagos. En ese sentido, 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 que puede hacer identificable a los Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI®) y que estuvieron involucrados de manera directa o indirecta en los eventos de abril de 2018 y con los cuales se intercambiaron comunicaciones en el periodo de abril 2018 al 31 de diciembre 2018,** podría disminuir la efectividad de las medidas que en su caso fueron adoptadas dificultando la consecución de su objetivo, podría menoscabar la efectividad de las medidas implementadas en el sistema financiero y económico del país, poniendo en riesgo el funcionamiento de esos sistemas; o bien, otorgaría una ventaja indebida, generando distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pagos; toda vez que dicho riesgo es:

1) **Real**, ya que revelar o divulgar información que puede hacer identificable a los Participantes del SPEI® que estuvieron involucrados de manera directa o indirecta en los eventos de abril de 2018, permitiría inferir brechas en la operación de los Participantes o vulnerabilidades que podrían ser utilizadas para diseñar estrategias operativas o tecnológicas que pudieran afectar la infraestructura de la entidad, o en un caso extremo la infraestructura del Banco de México, lo que podría derivar en la detección de posibles debilidades en los procesos de los participantes y, por ende, impactar en el buen funcionamiento del sistema, o bien podría posibilitar la realización de acciones hostiles por parte de una persona o grupo con intenciones delincuenciales en contra de dichos participantes.

   Adicionalmente, al identificar a los participantes del SPEI® que estuvieron involucrados de manera directa o indirecta en los eventos de abril de 2018, se podrían relacionar los mecanismos de operación con el participante, lo cual podría ser utilizado por otro participante, un cliente o un usuario mal intencionado para obtener una ventaja del proceso o detección de vulnerabilidades identificadas en el Participante en concreto, permitiendo a cibercriminales la realización de acciones hostiles en contra de estos participantes, aprovechando los puntos débiles identificados y enfocar ataques en contra de esos elementos.

   En consecuencia, la información referida actualiza las causales de reserva previstas en el artículo 112, fracciones IV y VII, de la LGTAIP, toda vez que su divulgación podría afectar las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, o bien podría obstruir en la prevención de delitos.

2) **Demostrable.** ya que se considera **demostrable que los sistemas de pagos de bancos centrales han sufrido ataques cibernéticos a través de estas infraestructuras**, que los sistemas de pagos están siendo víctimas de ciberataques sin precedente, de forma constante y organizada. Dichos ataques tienen por objeto el robo de recursos económicos a través del empleo de vulnerabilidades en las instituciones, aplicativos e infraestructura tecnológica de los sistemas. Lo anterior se puede ejemplificar con el ataque ocurrido a las instituciones financieras participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI®), el cual consistió en la fabricación o inyección de órdenes de transferencia apócrifas en los sistemas de los participantes donde se procesan las instrucciones de pago de los participantes, los atacantes vulneraron la infraestructura tecnológica de los participantes y generaron órdenes de transferencias ilegitimas.[1] Al 22 de mayo de 2018, se estimó un daño a los participantes del SPEI® de aproximadamente 300 millones de pesos.[2]

[1] Banco de México. "Información sobre los ataques a los Participantes del SPEI". https://www.banxico.org.mx/spei/d/%7BFFC53F5A-CA04-3098-EBF6-B0F17E533183%7D.pdf, consultado el 09 de abril de 2025.

[2] Acorde con los "Puntos importantes sobre la situación actual del SPEI" publicados en la página de internet del Banco de. http://www.banxico.org.mx/spei/d/%7BB806F1E8-686D-B9F1-0452-EC375543C801%7D.pdf, consultado el 09 de abril de 2025.

En ese sentido, también es de destacar que una afectación a la reputación de cualquier entidad tiene un impacto moral y económico, si no es controlado de manera correcta, puede terminar impactando su entorno. Tratándose de entidades financieras, la afectación en la reputación de un participante que se podría ocasionar por proporcionar la información que se está clasificando podría representar una ventaja indebida para un competidor malintencionado que, dependiendo del alcance de su interpretación, podría tener un impacto en el participante, SPEI® o en mayor escala, en el sistema financiero mexicano.

Por otra parte, en los últimos años se ha observado un incremento sostenido de ataques informáticos en el sector financiero, **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.[3]

En este sentido, la divulgación de la información materia de la presente prueba de daño, al estar en posesión de personas no autorizadas, puede facilitar que sea utilizada para impactar la operación de los participantes del SPEI® en la infraestructura y como institución financiera, en beneficio de terceros y en perjuicio del patrimonio de los participantes, generando distorsiones en la estabilidad del sistema de pagos denominado SPEI®.

3) Identificable, ya que, a la fecha de realización de la presente prueba de daño, es un hecho notorio que los sistemas de pagos atraen la atención del público en general ya que están siendo objeto de ciberataques a gran escala; una disrupción en los servicios provistos por los sistemas de pagos o de sus participantes, tendría repercusiones directas para una gran cantidad de empresas y comercios, que podrían ser utilizadas por terceros para impactar el funcionamiento de los sistemas de pagos.

Por lo anterior, un ataque perpetrado directamente al SPEI® o a sus participantes, ocasionado por dar a conocer el nombre de los participantes que se vieron involucrados en los eventos de abril de 2018 a que refiere la presente prueba de daño, representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues de acuerdo con la información del Banco de México, de febrero de 2024 a enero de 2025 se realizaron aproximadamente 5,155 millones de pagos electrónicos interbancarios por un monto de aproximadamente 329 billones de pesos; ahora bien y específicamente para el mes de enero de 2025 se realizaron aproximadamente 481 millones de operaciones en un mes, por un monto promedio de 60 mil pesos por operación, únicamente para lo que respecta a este sistema.[4]

Con base en estas cifras, es evidente que un ataque al SPEI® o a sus Participantes, sin importar la duración de la disrupción, puede llegar a tener efectos cuantiosos sobre la actividad económica del país y sobre el patrimonio de los usuarios de estos servicios.

Adicionalmente, **el riesgo de perjuicio que supondría la divulgación de la información, supera el interés público general de que se difunda**, pues el interés público se centra en que no se comprometa la efectividad

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

[4] Banco de México. Sistemas de pago de bajo valor, Transferencias SPEI por monto operado (CF620), https://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=21&accion=consultarCuadro&idCuadro=CF620&locale=es, consultado el 09 de abril 2025.

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, la estabilidad en los mercados financieros y en los sistemas de pagos. Por lo que, la información, no satisface un interés público, por el contrario, es información que pone en riesgo el buen funcionamiento de los sistemas de pagos y de la economía nacional en su conjunto. 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 y los sistemas de pagos administrados por éste, en particular el SPEI®.

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 obtener una ventaja indebida sobre otros participantes del sistema o se menoscabe la efectividad de las medidas implementadas en los sistemas financiero, así como permitir planear y perpetrar ataques cibernéticos dirigidos en contra de dichos participantes, lo cual tenga como resultado la creación de mecanismos que faciliten el acceso indebido, la sustracción de información – como datos personales referente a sus usuarios y las operaciones que realizan-, la alteración de las órdenes de transferencias de dichos participantes y que son enviadas a otros participantes del SPEI®. 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 adecúa 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 de los sistemas de pagos, del sistema financiero y de la economía nacional en su conjunto, así como prevención de delitos.**

Asimismo, **reservar la información en cuestión representa el medio menos restrictivo disponible para evitar el perjuicio**, en aras salvaguardar el buen funcionamiento de los sistemas de pagos, así como la estabilidad 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.

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 a la protección de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de los participantes, o en un caso extremo los sistemas de pagos del Banco de México, por lo que, en caso de revelarse, podría derivar en la detección de posibles debilidades en los procesos de los participantes y, por ende, impactar en el buen funcionamiento del sistema, o bien podría posibilitar la realización de acciones hostiles por parte de una persona o grupo con intenciones delincuenciales en contra de dichos participantes. Asimismo, y dada la importancia sistémica de los sistemas de pagos, estos continuarán 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, 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 que puede hacer identificable a los Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI®) que estuvieron involucrados de***

manera directa o indirecta en los eventos de abril de 2018 y con los cuales se intercambiaron comunicaciones en el periodo de abril 2018 al 31 de diciembre de 2018, toda vez que, como se ha manifestado esta acción atiende a la protección de la información de saber a quién de los participantes en el sistema de pagos se le compartió dicha información, con la finalidad de evitar utilizar la información contenida en las comunicaciones de manera errónea sin conocer el contexto de dicha información y que como consecuencia de su mal uso otorgue una ventaja indebida, generando distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pagos, o bien, en caso de revelarse, permitiría afectar 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 y comprometería las acciones encaminadas a la prevención de delitos.

PRUEBA DE DAÑO

INFORMACIÓN RELACIONADA CON PROCESOS DE CONTINUIDAD OPERATIVA Y DE CONTINGENCIA, ESPECIFICACIONES TÉCNICAS Y DE SEGURIDAD INFORMÁTICA QUE SOPORTAN EL FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS QUE ADMINISTRA, OPERA Y SUPERVISA EL BANCO DE MÉXICO.

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 (en adelante, CPEUM); así como 112, fracciones IV y VII, de la Ley General de Transparencia y Acceso a la información Pública (en adelante LGTAIP); es de clasificarse como información reservada aquella que pueda:

- Afectar la efectividad de 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 sistémico 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 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.

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.

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.**

El dar a conocer la ***información relacionada con procesos de continuidad operativa y de contingencia, especificaciones técnicas y de seguridad informática que soportan el funcionamiento de los sistemas de pagos que administra, opera y supervisa el Banco de México***, 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, aspectos de especificaciones técnicas, así como toda información que de forma aislada o agrupada, permita vincular directa o indirectamente, algún elemento específico de los sistemas de pagos que administra, opera y supervisa el Banco de México, podría disminuir la efectividad de las medidas que en su caso fueran adoptadas dificultando la consecución de su objetivo, retrasando la estabilización en los mercados financieros, dañando el funcionamiento de los sistemas de pagos e inclusive generando una mayor inestabilidad.

En ese orden de ideas, se precisa que la divulgación de la citada información representa un riesgo de perjuicio significativo al interés público ya que, menoscabaría 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; generaría incumplimiento en 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; 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**, en razón de revelar o divulgar la información, **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, procesos de continuidad operativa y de contingencia y, en general, información relacionada con la infraestructura informática de los sistemas de pago administrados por este Instituto Central, lo cual posibilita la realización de acciones hostiles en contra de las tecnologías de la información y protocolos de comunicación que establece este Banco Central** en los sistemas de pagos que éste administra, opera y supervisa, 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, debido a **que los delincuentes podrían diseñar estrategias para llevar a cabo ataques cibernéticos** dirigidos específicamente a los sistemas de pagos que administra el Banco Central, así como sabotajes a la estructura y elementos físicos, 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.

   Por lo anterior, exponer a los participantes de las Infraestructuras de los Mercados Financieros (IMF) así como al Banco Central que las administra, opera y supervisa, a estos riesgos cibernéticos **puede perturbar considerablemente al sistema financiero por su efecto directo en la información y operaciones relativas a los usuarios de los sistemas de pagos -tanto de las instituciones financieras como de las personas físicas y morales-.**

   Incluso, los ataques cibernéticos pueden provocar la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de estos sistemas, lo cual pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de las IMF, entre ellas los sistemas de pagos.

En efecto, revelar la información materia de la presente prueba de daño**, facilitaría que terceros logren acceder a información financiera o personal**, 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 vulnerabilidades de dichos sistemas, 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]

Sea cual fuere el origen o motivación del ataque en contra de la infraestructura utilizada para operar los sistemas de pagos, éste puede conducir al incumplimiento de las obligaciones del Banco Central hacia el sistema financiero y provocar **un colapso nacional de los sistemas de pagos, lo que actualizaría una contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.**

En el caso en concreto, la información materia de esta prueba de daño contiene información **relacionada con especificaciones técnicas en materia de seguridad, procesos de continuidad operativa, información sobre los componentes de los sistemas informáticos así como especificaciones de equipos de cómputo y telecomunicaciones, especificaciones respecto de los servicios prestados en materia de seguridad informática así como las condiciones de los mismos, horarios de operación, protocolos de comunicación, entre otros,** por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales aprovechar los aparentes puntos débiles y en consecuencia llevar a cabo ataques más certeros con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes a través de estas infraestructuras.

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]

---

[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.

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

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, en 2022 **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 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 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.[9]

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 específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero.[10] A la fecha de publicación de dicho comunicado, se estimó un daño a los participantes del SPEI® de aproximadamente 300 millones de pesos.[11]

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.[12]

---

[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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 2025.

[10] 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 09 de abril 2025.

[11] 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 09 de abril 2025.

[12] 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 09 de abril 2025.

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, 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 entonces 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

[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 09 de abril 2025.

[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 09 de abril 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 09 de abril 2025.

[16] INAI, Comunicado INAI/296/22 "Datos personales en riesgo de estar comprometidos por ataque cibernético a Sedena: INAI", 30 septiembre 2022, disponible en: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-296-22.pdf, consultado el 09 de abril 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 09 de abril 2025.

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 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]

---

[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 09 de abril 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 del 09 de abril 2025.

[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 del 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 2025.

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 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**.[25]

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.[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, ya que, a la fecha de realización de la presente prueba de daño, es un hecho notorio que los sistemas de pagos están siendo objeto de ciberataques a gran escala, como quedó demostrado en la sección anterior. 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 los sistemas de pagos 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 proporcionar la información materia de la presente prueba de daño, podría resultar en la afectación de las órdenes de transferencia en las**

---

[24] Offensive Security, INFORMATION GATHERING IN METASPLOIT, disponible en: https://www.offensive-security.com/metasploit-unleashed/information-gathering/, consultado el 09 de abril 2025.

[25] Riquelme, Rodrigo, "*El sistema financiero mexicano fue víctima 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 09 de abril 2025.

[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 09 de abril 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 09 de abril 2025.

cuentas bancarias de los distintos participantes y de los usuarios del sistema en comento. A su vez, estas afectaciones en las órdenes de transferencia podrían derivar en una pérdida de patrimonio no sólo para las instituciones financieras del país y demás participantes de los sistemas de pagos, sino en perjuicio de la población usuaria de los pagos electrónicos interbancarios, es decir **millones de personas físicas y morales, incluyendo aquellos empleados del sector público o privado que reciben su pago de salario vía transferencia electrónica que realizan sus patrones.**

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, un ataque perpetrado directamente a alguno de los sistemas de pagos administrados y operados por este Banco Central, ocasionado por dar a conocer la información objeto de la presente prueba de daño, representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues, por ejemplo, de acuerdo con la información disponible respecto del SPEI®, de febrero de 2024 a enero de 2025 se realizaron aproximadamente 5,155 millones de pagos electrónicos interbancarios por un monto de aproximadamente 329 billones de pesos; ahora bien y específicamente para el mes de enero de 2025 se realizaron aproximadamente 481 millones de operaciones en un mes, por un monto promedio de 60 mil pesos por operación, únicamente para lo que respecta a este sistema.[28]

Con base en estas cifras, es evidente que un ataque cibernético que vulnere la operación de los sistemas de pagos, sus tecnologías de la información y de comunicaciones, o la de sus participantes, sin importar la duración de la disrupción, puede llegar a tener efectos cuantiosos sobre la actividad económica del país y sobre el patrimonio de los usuarios de estos servicios; en especial, si este ocurre en alguno de los días de mayor actividad económica en el año, fechas particulares en que el número y monto de las operaciones se incrementa considerablemente.

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, la estabilidad en los mercados financieros y en los sistemas de pagos. Por lo que, **la información, no satisface un interés público, por el contrario, es información que pone en riesgo el buen funcionamiento de los sistemas de pagos y de la economía nacional en su conjunto.** 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

[28] Banco de México. Sistemas de pago de bajo valor, Transferencias SPEI por monto operado (CF620), https://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=21&accion=consultarCuadro&idCuadro=CF620&locale=es, consultado el 09 de abril 2025.

personas, esto es, **beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste, en particular el SPEI®.**

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 los sistemas de pagos administrados, operados y supervisados por el 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 -, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes 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 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.**

Asimismo, **reservar la información en cuestión representa el medio menos restrictivo disponible para evitar el perjuicio**, en aras salvaguardar el buen funcionamiento de los sistemas de pagos, así como la estabilidad 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.

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 a la protección de las medidas de seguridad informática, continuidad operativa y de contingencia, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques. Asimismo, y dada la importancia sistémica de los sistemas de pagos, estos continuarán 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, 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 procesos de continuidad operativa y de contingencia, especificaciones técnicas y de seguridad informática que soportan el funcionamiento de los sistemas de pagos que administra, opera y supervisa el Banco de México,** toda vez que, como se ha manifestado esta acción atiende a la protección de las medidas de seguridad informática, procedimientos de continuidad operativa y de contingencia, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos, no solo de las supuestas vulnerabilidades identificadas sino de aquellas que no se encuentran reconocidas provocando afectaciones a las IMF que opera y administra este Instituto Central, entre ellas los sistemas de pagos, lo cual menoscabaría 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; así como

podría generar incumplimiento en 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 y comprometería las acciones encaminadas a la prevención de delitos.

"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 relativa a la solicitud cuyos datos se señalan a continuación, y:

RESULTANDO

I. DATOS DE LA SOLICITUD

De conformidad a lo establecido en los artículos 124 y 125 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), el Banco de México recibió, en su oportunidad, la solicitud de acceso a la información cuyos datos se indican en la tabla siguiente:

FOLIO:	**6110000014020**
TRANSCRIPCIÓN PÚBLICA DE LA SOLICITUD:	
"Solicito copia documental en versiones públicas de los documentos generados entre la banca y Banxico (correos electrónicos, oficios, notas informativas, tarjetas informativas, circulares, comunicaciones, oficios) luego de la vulneración en los sistemas de seguridad internos de los bancos, que fue conocido como "hackeo" en abril de 2018. Solo requiero la información en versiones públicas de abril de 2018 (fecha en que ocurrió el suceso) hasta diciembre de 2018."	

II. SOLICITUD DE LA UNIDAD ADMINISTRATIVA

Toda vez que el plazo de clasificación inicial que se llevó a cabo para atender la solicitud citada está por concluir, 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 16 de abril de 2025.	Ana Laura Morales Guzmán (Gerencia de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados) y Víctor Enrique Tapia Tec (Subgerencia de Soporte de Sistemas de Pagos e Infraestructuras de Mercados), ambas unidades administrativas adscritas a la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, a su vez adscrita a la Dirección General 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 las pruebas de daño correspondientes: **A)** *"INFORMACIÓN QUE PUEDE HACER IDENTIFICABLE A LOS PARTICIPANTES DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS (SPEI®) QUE ESTUVIERON INVOLUCRADOS DE MANERA DIRECTA O INDIRECTA EN LOS EVENTOS DE ABRIL DE 2018 Y CON LOS CUALES SE INTERCAMBIARON COMUNICACIONES EN EL PERIODO DE ABRIL 2018 AL 31 DE DICIEMBRE DE 2018."* **B)** *"INFORMACIÓN RELACIONADA CON PROCESOS DE CONTINUIDAD OPERATIVA Y DE CONTINGENCIA, ESPECIFICACIONES TÉCNICAS Y DE SEGURIDAD INFORMÁTICA QUE SOPORTAN EL FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS QUE ADMINISTRA, OPERA Y SUPERVISA EL BANCO DE MÉXICO."*	**Plazo de reserva inicial:** 5 años, a partir del 20 de agosto de 2020. **Plazo de reserva con ampliación:** 5 años, a partir del 21 de agosto de 2025.

Oficio de fecha 16 de abril de 2025.	Ana Laura Morales Guzmán (Gerencia de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados) y Víctor Enrique Tapia Tec (Subgerencia de Soporte de Sistemas de Pagos e Infraestructuras de Mercados), ambas unidades administrativas adscritas a la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, a su vez adscrita a la Dirección General 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: *A*) *"INFORMACIÓN QUE PUEDE HACER IDENTIFICABLE A LOS PARTICIPANTES DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS (SPEI®) QUE ESTUVIERON INVOLUCRADOS DE MANERA DIRECTA O INDIRECTA EN LOS EVENTOS DE ABRIL DE 2018 Y CON LOS CUALES SE INTERCAMBIARON COMUNICACIONES EN EL PERIODO DE ABRIL 2018 AL 31 DE DICIEMBRE DE 2018."* **B)** *"INFORMACIÓN RELACIONADA CON PROCESOS DE CONTINUIDAD OPERATIVA Y DE CONTINGENCIA, ESPECIFICACIONES TÉCNICAS Y DE SEGURIDAD INFORMÁTICA QUE SOPORTAN EL FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS QUE ADMINISTRA, OPERA Y SUPERVISA EL BANCO DE MÉXICO."*	**Plazo de reserva inicial:** 5 años, a partir del 23 de julio de 2020. **Plazo de reserva con ampliación:** 5 años, a partir del 24 de julio de 2025.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva que soliciten las personas titulares de las unidades administrativas 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 los oficios referidos en el resultando II, así como en las correspondientes pruebas de daño, los cuales se tienen aquí por reproducidos como si a la letra se insertasen.[1]

Al respecto, de conformidad con lo expresado en los oficios señalados 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 las pruebas de daño respectivas, la divulgación de la información correspondiente: **A)***"(…) podría disminuir la efectividad de las medidas que en su caso fueron adoptadas dificultando la consecución de su objetivo, podría menoscabar la efectividad de las medidas implementadas en el sistema financiero y económico del país, poniendo en riesgo el funcionamiento de esos sistemas; o bien, otorgaría una ventaja indebida, generando distorsiones en la estabilidad de los*

[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).

mercados, incluyendo los sistemas de pagos (…)" y **B)** *"(…) representa un riesgo de perjuicio significativo al interés público ya que, menoscabaría 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; generaría incumplimiento en 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; o bien, podría obstruir la prevención de delitos (…)", **e**ste* **Comité de Transparencia aprueba la ampliación al periodo de reserva de la información señalada** de conformidad con lo expresado en los oficios citados en el resultando II de la presente determinación, así como en términos de las pruebas de daño correspondientes, **y toma conocimiento del nuevo plazo de reserva determinado por las unidades administrativas.**

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 señalada en los oficios mencionados en el resultando II de la presente determinación, conforme a la fundamentación y motivación expresadas en los mismos y en las pruebas de daño correspondientes, 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 26 de junio de 2025. ----------

COMITÉ DE TRANSPARENCIA

_____

CLAUDIA TAPIA RANGEL
Integrante
Unidad de Transparencia

_____

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante
Dirección de Seguridad y Organización de la Información

_____

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente
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
27/06/2025 19:14:59	Edgar Miguel Salas Ortega	b4ad34ffe8ded0d2d38db52054a3ab3673a57d07f7f8503fc048951951729105
27/06/2025 20:20:59	VICTOR MANUEL DE LA LUZ PUEBLA	34c364ac9921897ea457dbbed890590bea84314b0564f6e15d57e54db79d911f
30/06/2025 09:26:36	Claudia Tapia Rangel	d85082091cc027f5a5491d575a713b0555f897e4a83461d1b2c831bbfb5061ee

"ANEXO 4"

BANCO DE MÉXICO®

"*2025, Año de la Mujer Indígena*"

Ciudad de México, 29 de abril de 2025

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

Nos referimos a la clasificación de reserva realizada, en su momento, para la atención de una solicitud de acceso a la información a, por estas unidades administrativas, respecto de diversa información contenida en el documento que se señala en el siguiente cuadro:

Cons.	TÍTULO DEL DOCUMENTO CLASIFICADO
1	Lineamientos para Borrar Datos en las ETB

Al respecto, nos permitimos resaltar que dicha clasificación fue confirmada por ese Comité mediante resolución del 30 de julio de 2020, emitida en la sesión Ordinaria 25/2020, en términos de la fundamentación y motivación expresadas en el oficio del 22 de julio de 2020, suscrito por estas unidades administrativas, 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 30 de julio de 2020, a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el 30 de julio 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, 19 Bis 1 y 18 Bis del Reglamento Interior del Banco de México (RIBM); así como Segundo, fracciones VI y IX, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; nos permitimos informarles que estas unidades administrativas **estiman 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 ponemos 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 al referido documento clasificado, es el adscrito a:

Por parte de la Dirección General de Tecnologías de la Información:

- Dirección de Infraestructura de Tecnologías de la Información (Director).
- Gerencia de Seguridad de Tecnologías de la Información (Gerente).

- Subgerencia del Centro de Defensa de Ciberseguridad (Todo el personal).
- Subgerencia de Planeación y Regulación (Todo el personal).

Por parte de la Dirección de Recursos Materiales:

- Dirección de Recursos Materiales (Director).
- Gerencia de Abastecimiento de Tecnologías de la Información, Inmuebles y Generales (Todo el personal).
- Gerencia de Abastecimiento a Emisión y Recursos Humanos (Todo el personal).
- Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Todo el personal).

Unidad de Auditoría (Todo el personal).
Dirección de Control Interno (Todo el personal).

Atentamente

ARTURO GARCÍA HERNÁNDEZ
Gerente de Seguridad de Tecnologías de la Información

MARÍA DEL CARMEN PRUDENTE TIXTECO
Subgerente del Centro de Defensa de Ciberseguridad

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
29/04/2025 17:52:38	ARTURO GARCIA HERNANDEZ	64bfb88bfe46775fe4adb8b974ce9499ae172556099fe20ee9fecbe9645842b8
29/04/2025 18:38:25	MARIA DEL CARMEN PRUDENTE TIXTECO	2ec840dea140ac3c33e77d0cfee4aaf78e197e7fc532421eb17b0180525c06a1

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 relativa a la solicitud cuyos datos se señalan a continuación, y:

RESULTANDO

I. DATOS DE LA SOLICITUD

De conformidad a lo establecido en los artículos 124 y 125 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), el Banco de México recibió, en su oportunidad, la solicitud de acceso a la información cuyos datos se indican en la tabla siguiente:

FOLIO:	**6110000028220**
TRANSCRIPCIÓN PÚBLICA DE LA SOLICITUD:	
"Solicito los Lineamientos para Borrar Datos en la ETB (en su caso, la respectiva versión pública) descrito en el documento de seguridad de dicho Sujeto Obligado. En caso de que la respuesta rebase los límites de carga de la Plataforma Nacional de Transparencia, se requiere se remita al correo electrónico descrito en la solicitud de mérito."	

II. SOLICITUD DE LA UNIDAD ADMINISTRATIVA

Toda vez que el plazo de clasificación inicial que se llevó a cabo para atender la solicitud citada está por concluir, 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 29 de abril de 2025.	Arturo García Hernández (Gerencia de Seguridad de Tecnologías de la Información) y María del Carmen Prudente Tixteco (Subgerencia del Centro de Defensa de Ciberseguridad), ambas unidades administrativas adscritas a la Dirección de Seguridad y Organización de la Información, a su vez adscrita a la Dirección General de Tecnologías de la Información 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: *"Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México"*	**Plazo de reserva inicial:** 5 años, a partir del 30 de julio de 2020. **Plazo de reserva con ampliación:** 5 años, a partir del 31 de julio de 2025.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva que soliciten las personas titulares de las unidades administrativas 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 II, así como en la correspondiente prueba de daño, 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 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 correspondiente 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 (…)",* ***es*****te 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 II de la presente determinación, así como en términos de la prueba de daño correspondiente, **y toma conocimiento del nuevo plazo de reserva determinado por las unidades administrativas.**

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 señalada en el oficio mencionado en el resultando II de la presente determinación, conforme a la fundamentación y motivación expresadas en el mismo y 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 26 de junio de 2025.----------

COMITÉ DE TRANSPARENCIA

_____

CLAUDIA TAPIA RANGEL
Integrante
Unidad de Transparencia

_____	_____
VÍCTOR MANUEL DE LA LUZ PUEBLA	**EDGAR MIGUEL SALAS ORTEGA**
Integrante	Integrante Suplente
Dirección de Seguridad y Organización de la Información	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
27/06/2025 19:15:02	Edgar Miguel Salas Ortega	3eef1be2e416f1b7b0b6b887bf564163cf0e4c66d267a12d0ae97d8f55c1721e
27/06/2025 20:20:49	VICTOR MANUEL DE LA LUZ PUEBLA	fdd70fdff84f0fd8ed87f318d36db2d5f7d3aeb3ab315a4da370c2df918b4f25
30/06/2025 09:26:43	Claudia Tapia Rangel	60d0fed001b1f0679b35e9cb00a0ad5afb6dd1b17f5dadac36c1fe55eba45b0d

"ANEXO 6"

BANCO DE MÉXICO®

"2025, Año de la mujer indígena"

Ciudad de México, 16 de abril de 2025

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

Nos referimos a la clasificación de reserva realizada, en su momento, para la atención de una solicitud de acceso a la información por la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, respecto de la información contenida en los documentos que se señalan a continuación:

TÍTULO DEL DOCUMENTO CLASIFICADO
Guía para la evaluación del cumplimiento de los requisitos de seguridad informática y de gestión del riesgo operacional del SPEI

Al respecto, nos permitimos resaltar que dicha clasificación fue confirmada por el Comité de Transparencia mediante resolución de 30 de julio de 2020, emitida en la sesión ordinaria 25/2020, en términos de la fundamentación y motivación expresadas en el oficio con referencia D40-038-2020 del 23 de julio de 2020, suscrito la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, 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 30 de julio de 2020 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **30 de julio 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 Ter, del Reglamento Interior del Banco de México (RIBM); Segundo, fracción XVII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; nos permitimos informarles que estas unidades administrativas **estiman 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; **solicitamos 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, informamos 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 Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados (Director), Gerencia de Operación de Sistemas de Pagos e Infraestructuras de Mercados (Gerente), Gerencia de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados (Gerente), Subgerencia de Continuidad y Gestión de Sistemas de Pagos e Infraestructuras de Mercados (Subgerente) y Subgerencia de Soporte de Sistemas de Pagos e Infraestructuras de Mercados.

Atentamente

ANA LAURA MORALES GUZMÁN
Gerente de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados

VICTOR ENRIQUE TAPIA TEC
Subgerente de Soporte de Sistemas de Pagos e Infraestructuras de Mercados

BANCO DE MÉXICO®
RECIBIDO
16 ABR 2025
Comité de Transparencia
Por: E14807 Hora: 12:00

PRUEBA DE DAÑO

INFORMACIÓN RELACIONADA CON PROCESOS DE CONTINUIDAD OPERATIVA Y DE CONTINGENCIA, ESPECIFICACIONES TÉCNICAS Y DE SEGURIDAD INFORMÁTICA QUE SOPORTAN EL FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS QUE ADMINISTRA, OPERA Y SUPERVISA EL BANCO DE MÉXICO.

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 (en adelante, CPEUM); así como 112, fracciones IV y VII, de la Ley General de Transparencia y Acceso a la información Pública (en adelante LGTAIP); es de clasificarse como información reservada aquella que pueda:

- Afectar la efectividad de 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 sistémico 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 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.

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.

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.**

El dar a conocer la ***información relacionada con procesos de continuidad operativa y de contingencia, especificaciones técnicas y de seguridad informática que soportan el funcionamiento de los sistemas de pagos que administra, opera y supervisa el Banco de México***, 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, aspectos de especificaciones técnicas, así como toda información que de forma aislada o agrupada, permita vincular directa o indirectamente, algún elemento específico de los sistemas de pagos que administra, opera y supervisa el Banco de México, podría disminuir la efectividad de las medidas que en su caso fueran adoptadas dificultando la consecución de su objetivo, retrasando la estabilización en los mercados financieros, dañando el funcionamiento de los sistemas de pagos e inclusive generando una mayor inestabilidad.

En ese orden de ideas, se precisa que la divulgación de la citada información representa un riesgo de perjuicio significativo al interés público ya que, menoscabaría 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; generaría incumplimiento en 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; 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**, en razón de revelar o divulgar la información, **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, procesos de continuidad operativa y de contingencia y, en general, información relacionada con la infraestructura informática de los sistemas de pago administrados por este Instituto Central, lo cual posibilita la realización de acciones hostiles en contra de las tecnologías de la información y protocolos de comunicación que establece este Banco Central** en los sistemas de pagos que éste administra, opera y supervisa, 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, debido a **que los delincuentes podrían diseñar estrategias para llevar a cabo ataques cibernéticos** dirigidos específicamente a los sistemas de pagos que administra el Banco Central, así como sabotajes a la estructura y elementos físicos, 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.

   Por lo anterior, exponer a los participantes de las Infraestructuras de los Mercados Financieros (IMF) así como al Banco Central que las administra, opera y supervisa, a estos riesgos cibernéticos **puede perturbar considerablemente al sistema financiero por su efecto directo en la información y operaciones relativas a los usuarios de los sistemas de pagos -tanto de las instituciones financieras como de las personas físicas y morales-.**

   Incluso, los ataques cibernéticos pueden provocar la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de estos sistemas, lo cual pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de las IMF, entre ellas los sistemas de pagos.

En efecto, revelar la información materia de la presente prueba de daño**, facilitaría que terceros logren acceder a información financiera o personal**, 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 vulnerabilidades de dichos sistemas, 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]

Sea cual fuere el origen o motivación del ataque en contra de la infraestructura utilizada para operar los sistemas de pagos, éste puede conducir al incumplimiento de las obligaciones del Banco Central hacia el sistema financiero y provocar **un colapso nacional de los sistemas de pagos, lo que actualizaría una contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.**

En el caso en concreto, la información materia de esta prueba de daño contiene información **relacionada con especificaciones técnicas en materia de seguridad, procesos de continuidad operativa, información sobre los componentes de los sistemas informáticos así como especificaciones de equipos de cómputo y telecomunicaciones, especificaciones respecto de los servicios prestados en materia de seguridad informática así como las condiciones de los mismos, horarios de operación, protocolos de comunicación, entre otros,** por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales aprovechar los aparentes puntos débiles y en consecuencia llevar a cabo ataques más certeros con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes a través de estas infraestructuras.

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]

---

[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.

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

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, en 2022 **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 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 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.[9]

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 específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero.[10] A la fecha de publicación de dicho comunicado, se estimó un daño a los participantes del SPEI® de aproximadamente 300 millones de pesos.[11]

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.[12]

---

[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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 2025.

[10] 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 09 de abril 2025.

[11] 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 09 de abril 2025.

[12] 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 09 de abril 2025.

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, 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 entonces 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

[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 09 de abril 2025.

[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 09 de abril 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 09 de abril 2025.

[16] INAI, Comunicado INAI/296/22 "Datos personales en riesgo de estar comprometidos por ataque cibernético a Sedena: INAI", 30 septiembre 2022, disponible en: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-296-22.pdf, consultado el 09 de abril 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 09 de abril 2025.

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 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]

---

[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 09 de abril 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 del 09 de abril 2025.

[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 del 09 de abril 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 09 de abril 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 09 de abril 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 09 de abril 2025.

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 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**.[25]

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.[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, ya que, a la fecha de realización de la presente prueba de daño, es un hecho notorio que los sistemas de pagos están siendo objeto de ciberataques a gran escala, como quedó demostrado en la sección anterior. 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 los sistemas de pagos 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 proporcionar la información materia de la presente prueba de daño, podría resultar en la afectación de las órdenes de transferencia en las**

[24] Offensive Security, INFORMATION GATHERING IN METASPLOIT, disponible en: https://www.offensive-security.com/metasploit-unleashed/information-gathering/, consultado el 09 de abril 2025.
[25] Riquelme, Rodrigo, "*El sistema financiero mexicano fue víctima 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 09 de abril 2025.
[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 09 de abril 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 09 de abril 2025.

cuentas bancarias de los distintos participantes y de los usuarios del sistema en comento. A su vez, estas afectaciones en las órdenes de transferencia podrían derivar en una pérdida de patrimonio no sólo para las instituciones financieras del país y demás participantes de los sistemas de pagos, sino en perjuicio de la población usuaria de los pagos electrónicos interbancarios, es decir **millones de personas físicas y morales, incluyendo aquellos empleados del sector público o privado que reciben su pago de salario vía transferencia electrónica que realizan sus patrones.**

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, un ataque perpetrado directamente a alguno de los sistemas de pagos administrados y operados por este Banco Central, ocasionado por dar a conocer la información objeto de la presente prueba de daño, representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues, por ejemplo, de acuerdo con la información disponible respecto del SPEI®, de febrero de 2024 a enero de 2025 se realizaron aproximadamente 5,155 millones de pagos electrónicos interbancarios por un monto de aproximadamente 329 billones de pesos; ahora bien y específicamente para el mes de enero de 2025 se realizaron aproximadamente 481 millones de operaciones en un mes, por un monto promedio de 60 mil pesos por operación, únicamente para lo que respecta a este sistema.[28]

Con base en estas cifras, es evidente que un ataque cibernético que vulnere la operación de los sistemas de pagos, sus tecnologías de la información y de comunicaciones, o la de sus participantes, sin importar la duración de la disrupción, puede llegar a tener efectos cuantiosos sobre la actividad económica del país y sobre el patrimonio de los usuarios de estos servicios; en especial, si este ocurre en alguno de los días de mayor actividad económica en el año, fechas particulares en que el número y monto de las operaciones se incrementa considerablemente.

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, la estabilidad en los mercados financieros y en los sistemas de pagos. Por lo que, **la información, no satisface un interés público, por el contrario, es información que pone en riesgo el buen funcionamiento de los sistemas de pagos y de la economía nacional en su conjunto.** 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

[28] Banco de México. Sistemas de pago de bajo valor, Transferencias SPEI por monto operado (CF620), https://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=21&accion=consultarCuadro&idCuadro=CF620&locale=es, consultado el 09 de abril 2025.

personas, esto es, **beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste, en particular el SPEI®.**

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 los sistemas de pagos administrados, operados y supervisados por el 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 -, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes 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 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.**

Asimismo, **reservar la información en cuestión representa el medio menos restrictivo disponible para evitar el perjuicio**, en aras salvaguardar el buen funcionamiento de los sistemas de pagos, así como la estabilidad 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.

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 a la protección de las medidas de seguridad informática, continuidad operativa y de contingencia, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques. Asimismo, y dada la importancia sistémica de los sistemas de pagos, estos continuarán 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, 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 procesos de continuidad operativa y de contingencia, especificaciones técnicas y de seguridad informática que soportan el funcionamiento de los sistemas de pagos que administra, opera y supervisa el Banco de México,** toda vez que, como se ha manifestado esta acción atiende a la protección de las medidas de seguridad informática, procedimientos de continuidad operativa y de contingencia, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos, no solo de las supuestas vulnerabilidades identificadas sino de aquellas que no se encuentran reconocidas provocando afectaciones a las IMF que opera y administra este Instituto Central, entre ellas los sistemas de pagos, lo cual menoscabaría 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; así como

podría generar incumplimiento en 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 y comprometería las acciones encaminadas a la prevención de delitos.

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 relativa a la solicitud cuyos datos se señalan a continuación, y:

RESULTANDO

I. DATOS DE LA SOLICITUD

De conformidad a lo establecido en los artículos 124 y 125 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), el Banco de México recibió, en su oportunidad, la solicitud de acceso a la información cuyos datos se indican en la tabla siguiente:

FOLIO:	**CTC-BM-30250**
TRANSCRIPCIÓN PÚBLICA DE LA SOLICITUD:	
"Buen día, quisiera su apoyo para obtener la Guía para la evaluación del cumplimiento de los requisitos de seguridad informática y de gestión del riesgo operacional del SPEI, dado que dentro de la página no localizo el documento; o en su caso me puedan indicar en que apartado lo encuentro gracias!"	

II. SOLICITUD DE LA UNIDAD ADMINISTRATIVA

Toda vez que el plazo de clasificación inicial que se llevó a cabo para atender la solicitud citada está por concluir, 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 16 de abril de 2025.	Ana Laura Morales Guzmán (Gerencia de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados) y Víctor Enrique Tapia Tec (Subgerencia de Soporte de Sistemas de Pagos e Infraestructuras de Mercados), ambas unidades administrativas adscritas a la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, a su vez adscrita a la Dirección General 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 PROCESOS DE CONTINUIDAD OPERATIVA Y DE CONTINGENCIA, ESPECIFICACIONES TÉCNICAS Y DE SEGURIDAD INFORMÁTICA QUE SOPORTAN EL FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS QUE ADMINISTRA, OPERA Y SUPERVISA EL BANCO DE MÉXICO."*	**Plazo de reserva inicial:** 5 años, a partir del 30 de julio de 2020. **Plazo de reserva con ampliación:** 5 años, a partir del 31 de julio de 2025.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva que soliciten las personas titulares de las unidades administrativas 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 II, así como en la correspondiente prueba de daño, 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 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 correspondiente representa un riesgo: *"(…) de perjuicio significativo al interés público ya que, menoscabaría 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; generaría incumplimiento en 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; o bien, podría obstruir la prevención de delitos (…)", **es*****te* Comité de Transparencia aprueba la ampliación al periodo de reserva de la información señalada** de conformidad con lo expresado en los oficios citados en el resultando II de la presente determinación, así como en términos de las pruebas de daño correspondientes, **y toma conocimiento del nuevo plazo de reserva determinado por las unidades administrativas.**

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 señalada en el oficio mencionado en el resultando II de la presente determinación, conforme a la fundamentación y motivación expresada en el mismo y 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 26 de junio de 2025. ----------

COMITÉ DE TRANSPARENCIA

_____

CLAUDIA TAPIA RANGEL
Integrante
Unidad de Transparencia

_____

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante
Dirección de Seguridad y Organización de la Información

_____

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente
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
27/06/2025 19:15:02	Edgar Miguel Salas Ortega	3eef1be2e416f1b7b0b6b887bf564163cf0e4c66d267a12d0ae97d8f55c1721e
27/06/2025 20:20:50	VICTOR MANUEL DE LA LUZ PUEBLA	64072cfd14743cf6719591eb74651c5118cb80c3e3ffebf0b34b55e29190dfbb
30/06/2025 09:26:47	Claudia Tapia Rangel	5d3f7ae3e390e48657951dd374be71ffaa03d98bed53474b36f991b22cb9cfdd

"ANEXO 8"

BANCO DE MÉXICO®

"2025, Año de la mujer indígena"

Ciudad de México, 21 de mayo de 2025

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

Nos referimos a la clasificación de reserva realizada, en su momento, para la atención de una solicitud de acceso a la información por la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados B, la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A, la Gerencia de Seguridad de Tecnologías de la Información y la Subgerencia del Centro de Defensa de Ciberseguridad, respecto de diversa información contenida en el documento que se señala a continuación:

TÍTULO DEL DOCUMENTO CLASIFICADO
Comunicación CASP de fecha 04 de julio de 2018

Al respecto, nos permitimos resaltar que dicha clasificación fue confirmada por el Comité de Transparencia mediante resolución de 03 de septiembre de 2020, emitida en la sesión ordinaria 29/2020, en términos de la fundamentación y motivación expresadas en el oficio con referencia D40-041-2020 del 28 de agosto de 2020, suscrito por la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados B, la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A, la Gerencia de Seguridad de Tecnologías de la Información y la Subgerencia del Centro de Defensa de Ciberseguridad; 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 03 de septiembre de 2020 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **03 de septiembre 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, 20, 20 Ter, 15 Bis 1 y 18 Bis, del Reglamento Interior del Banco de México (RIBM); Segundo, fracciones IX y XVII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; nos permitimos informarles que estas unidades administrativas **estiman 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 las pruebas de daño correspondientes, que se ponen a disposición de ese Comité de Transparencia.**

Por lo expuesto, y con fundamento en el artículo 104, párrafo tercero, de la LGTAIP; **solicitamos 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, informamos 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 Operación y Continuidad de Sistemas de Pagos e Infraestructuras

de Mercados (Director), Gerencia de Operación de Sistemas de Pagos e Infraestructuras de Mercados (Gerente), Gerencia de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados (Gerente), Subgerencia de Continuidad y Gestión de Sistemas de Pagos e Infraestructuras de Mercados (Subgerente), Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructuras 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 B (Subgerente) y Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados A (Subgerente); así como la Dirección General de Tecnologías de la Información (Director General), Dirección de Seguridad y Organización de la Información (Director), Gerencia de Seguridad de Tecnologías de la Información (Todo el personal).

Atentamente

ANA LAURA MORALES GUZMÁN
Gerente de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados

CARLOS HERNÁNDEZ LÓPEZ
Gerente de Tecnologías Innovadoras de Sistemas de Pagos e Infraestructuras de Mercados

ARTURO GARCÍA HERNÁNDEZ
Gerente de Seguridad de Tecnologías de la Información

MARIA DEL CARMEN PRUDENTE TIXTECO
Subgerente del Centro de Defensa de Ciberseguridad

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
21/05/2025 19:52:02	ANA LAURA MORALES GUZMAN	7f3a5709ec9e9283e1ffa4146ad256a77791ad55cf91d092995e7c8e0c8a590c
21/05/2025 20:46:26	CARLOS HERNANDEZ LOPEZ	1308aa8142618ace5b03d4e98f5e700a0c337baf3a31de04a7f591d07f102200
23/05/2025 12:36:45	ARTURO GARCIA HERNANDEZ	decbc8bfc811b2c3c673e1142a58af6332140ba57848a3e3a8298a33969fa8ed
23/05/2025 12:57:02	MARIA DEL CARMEN PRUDENTE TIXTECO	cd3141e59d94baf8b69afe858ea9a86bc77e0234736b458fb28468604e19e7b7

"ANEXO 9"

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 relativa a la solicitud cuyos datos se señalan a continuación, y:

RESULTANDO

I. DATOS DE LA SOLICITUD

De conformidad a lo establecido en los artículos 124 y 125 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), el Banco de México recibió, en su oportunidad, la solicitud de acceso a la información cuyos datos se indican en la tabla siguiente:

FOLIO:	**6110000014620**
TRANSCRIPCIÓN PÚBLICA DE LA SOLICITUD:	
"De acuerdo con el informe del Banxico del primer semestre de 2019 se informa lo siguiente: "...así como controles de conciliación y un análisis de compromiso de la infraestructura del Banco de México por parte de un tercero especializado en ciberseguridad y, en particular, aquella utilizada por el SPEI. Solicito saber en documentos: --Copia del contrato en versión pública del "tercero especializado en ciberseguridad" contratado por el Banco de México. --Copia del diagnóstico elaborado por este experto, en versions públicas. --Copia de los oficios girados por este concepto (el experto en ciberseguridad) entre bancos y BAnxico. Todo en versions públicas."	

II. SOLICITUD DE LA UNIDAD ADMINISTRATIVA

Toda vez que el plazo de clasificación inicial que se llevó a cabo para atender la solicitud citada está por concluir, 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 21 de mayo de 2025.	Ana Laura Morales Guzmán (Gerencia de Continuidad, Control y Soporte de Sistemas de Pagos e Infraestructuras de Mercados, unidad administrativa adscrita a la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados) y Carlos Hernández López (Gerencia de Tecnologías Innovadoras de Sistemas de Pagos e Infraestructuras de Mercados, unidad administrativa adscrita a la Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructuras de Mercados), ambas unidades administrativas adscritas a la Dirección	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 las pruebas de daño correspondientes: **A)** *"INFORMACIÓN QUE PUEDE HACER IDENTIFICABLE A LOS PARTICIPANTES DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS (SPEI®) QUE ESTUVIERON INVOLUCRADOS DE MANERA DIRECTA O INDIRECTA EN LOS EVENTOS DE CIBERSEGURIDAD DE 2018."* **B)** *"Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México."*	**Plazo de reserva inicial:** 5 años, a partir del 03 de septiembre de 2020. **Plazo de reserva con ampliación:** 5 años, a partir del 04 de septiembre de 2025.

	General de Sistemas de Pagos e Infraestructuras de Mercados; así como Arturo García Hernández (Gerencia de Seguridad de Tecnologías de la Información) y María del Carmen Prudente Tixteco (Subgerencia del Centro de Defensa de Ciberseguridad) ambas unidades administrativas adscritas a la Dirección de Seguridad y Organización de la Información, a su vez adscrita a la Dirección General de Tecnologías de la Información del Banco de México.			

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva que soliciten las personas titulares de las unidades administrativas 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 II, así como en las correspondientes pruebas de daño, 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 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 las pruebas de daño respectivas, la divulgación de la información correspondiente: **A)** *"(…) podría disminuir la efectividad de las medidas que en su caso fueron adoptadas dificultando la consecución de su objetivo, podría menoscabar la efectividad de las medidas implementadas en el sistema financiero y económico del país, poniendo en riesgo el funcionamiento de esos sistemas; o bien, otorgaría una ventaja indebida, generando distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pagos (…)"y* **B)** *"(…)* ***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;*

[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).

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 (…)", ***es*****te 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 II de la presente determinación, así como en términos de las pruebas de daño correspondientes, **y toma conocimiento del nuevo plazo de reserva determinado por las unidades administrativas.**

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 señalada en el oficio mencionado en el resultando II de la presente determinación, conforme a la fundamentación y motivación expresadas en el mismo y en las pruebas de daño correspondientes, 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 26 de junio de 2025. ----------

COMITÉ DE TRANSPARENCIA

_____

CLAUDIA TAPIA RANGEL
Integrante
Unidad de Transparencia

_____

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante
Dirección de Seguridad y Organización de la Información

_____

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente
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
27/06/2025 19:15:05	Edgar Miguel Salas Ortega	62e5326a5397768b94b4617b92485098a3be2379ad8ada4bcf3fee42a0a6dfe5
27/06/2025 20:20:55	VICTOR MANUEL DE LA LUZ PUEBLA	5e5394f60bac6b303776dd5d6eab65478323591353f06d14494b8d13ce250b7c
30/06/2025 09:26:55	Claudia Tapia Rangel	cf22bb7f1be1410f109b18c8b1551ab5e390df16a6fd5f2661a5219eb879055c

"ANEXO 10"

BANCO DE MÉXICO®

"2025. Año de la Mujer Indígena"

Ciudad de México, 28 de mayo de 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 la atención de una solicitud de acceso a la información, por esta unidad administrativa, respecto de la información que se señala a continuación:

> ***"… con quien se han celebrado (contraparte) los contratos de coberturas petroleras…" en los años 2002, 2005 al 2013, 2018 y 2019"***

Al respecto, me permito resaltar que dicha clasificación fue confirmada por ese Comité mediante resolución de 03 de septiembre de 2020, emitida en la sesión Ordinaria 29/2020, en términos de la fundamentación y motivación expresadas en el oficio de 28 de agosto 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 03 de septiembre de 2020 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **03 de septiembre 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 y 19, del Reglamento Interior del Banco de México (RIBM); así como Segundo, fracción VI, 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 Operaciones de Banca Central (Director), Dirección de Operaciones Internacionales (Director), Gerencia de Operaciones Internacionales (Gerente) y Subgerencia de Cambios Internacionales y Metales (todo el personal)

Atentamente

_____

JOAQUÍN TAPIA MACÍAS
Director de Operaciones Internacionales

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
29/05/2025 10:21:09	JOAQUIN TAPIA MACIAS	d5b803b4e652b46fa915861e92d658fad238747b5adca70a250daf73aed6ffc7

BANCO DE MÉXICO®

"2025. Año de la Mujer Indígena"

Ciudad de México, 28 de mayo de 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 la atención de una solicitud de acceso a la información, por esta unidad administrativa, respecto de la información que se señala a continuación:

> ***"… los contratos… de coberturas petroleras que se hayan celebrado para los ejercicios…" "2006 al 2008"***

Al respecto, me permito resaltar que dicha clasificación fue confirmada por ese Comité mediante resolución de 03 de septiembre de 2020, emitida en la sesión Ordinaria 29/2020, en términos de la fundamentación y motivación expresadas en el oficio de 28 de agosto 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 03 de septiembre de 2020 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **03 de septiembre 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 y 19, del Reglamento Interior del Banco de México (RIBM); así como Segundo, fracción VI, 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 Operaciones de Banca Central (Director), Dirección de Operaciones Internacionales (Director), Gerencia de Operaciones Internacionales (Gerente) y Subgerencia de Cambios Internacionales y Metales (todo el personal)

Atentamente

_____

JOAQUÍN TAPIA MACÍAS
Director de Operaciones Internacionales

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
29/05/2025 10:21:10	JOAQUIN TAPIA MACIAS	627fb02244b7e2afc49bea3f09d3825b9f8193eea38fcffd64a737837e6094c1

"ANEXO 11"

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 relativa a la solicitud cuyos datos se señalan a continuación, y:

RESULTANDO

I. DATOS DE LA SOLICITUD

De conformidad a lo establecido en los artículos 124 y 125 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), el Banco de México recibió, en su oportunidad, la solicitud de acceso a la información cuyos datos se indican en la tabla siguiente:

FOLIO:	**6110000013320**
TRANSCRIPCIÓN PÚBLICA DE LA SOLICITUD:	
"1. Monto/costo por ejercicio de los contratos de coberturas petroleras de los ejercicios 2000 al 2019. *2. Por ejercicio, con quien se han celebrado (contraparte) los contratos de coberturas petroleras para los ejercicios 2000 al 2019.* *3. Se piden los contratos, de ser el caso en versión pública, de coberturas petroleras que se hayan celebrado para los ejercicios 2006 al 2019. Agradezco la atención"*	

II. SOLICITUD DE LA UNIDAD ADMINISTRATIVA

Toda vez que el plazo de clasificación inicial que se llevó a cabo para atender la solicitud citada está por concluir, 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 28 de mayo de 2025.	Joaquín Tapia Macías (Dirección de Operaciones Internacionales 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 RELATIVA A LAS COBERTURAS PETROLERAS"*	**Plazo de reserva inicial:** 5 años, a partir del 03 de septiembre de 2020. **Plazo de reserva con ampliación:** 5 años, a partir del 04 de septiembre de 2025.
Oficio de fecha 28 de mayo de 2025.	Joaquín Tapia Macías (Dirección de Operaciones Internacionales 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:	**Plazo de reserva inicial:** 5 años, a partir del 03 de septiembre de 2020.

			"INFORMACIÓN RELATIVA A LAS COBERTURAS PETROLERAS"	**Plazo de reserva con ampliación:** 5 años, a partir del 04 de septiembre de 2025.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva que soliciten las personas titulares de las unidades administrativas 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 los oficios referidos en el resultando II, así como en las correspondientes pruebas de daño, los cuales se tienen aquí por reproducidos como si a la letra se insertasen.[1]

Al respecto, de conformidad con lo expresado en los oficios señalados 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 correspondiente representa un riesgo **de perjuicio significativo al interés público**, toda vez que puede: *"(…) poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda incrementar el costo de las operaciones financieras que realizan los sujetos obligados del sector público federal, o menoscabar la efectividad de las medidas implementadas en el sistema financiero (…)",* ***e*ste Comité de Transparencia aprueba la ampliación al periodo de reserva de la información señalada** de conformidad con lo expresado en los oficios citados en el resultando II de la presente determinación, así como en términos de las pruebas de daño correspondientes, **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** señalada en los oficios mencionados en el resultando II de la presente determinación, conforme a la fundamentación y motivación expresadas en los mismos y 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 26 de junio de 2025.----------

COMITÉ DE TRANSPARENCIA

_____

CLAUDIA TAPIA RANGEL
Integrante
Unidad de Transparencia

_____

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante
Dirección de Seguridad y Organización de la Información

_____

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente
Dirección Jurídica

PAJC
NMDS

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
27/06/2025 19:15:06	Edgar Miguel Salas Ortega	f25364c32e1bd736665b35053de923d10d839c39f74cb110c0008567ab9efd8e
27/06/2025 20:20:57	VICTOR MANUEL DE LA LUZ PUEBLA	3fd38d4dc54710fcd5994162a110c82cd0685d595373f96f5438c7635fa5ebb1
30/06/2025 09:26:32	Claudia Tapia Rangel	eb98bd8c820b2b3747172a4e7cc2c434d470812d6cde92d722749b50763fd2cd

"ANEXO 12"

BANCO DE MÉXICO®

"2025, Año de la mujer indígena"

Ciudad de México, 21 de mayo de 2025

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

Nos referimos a la clasificación de reserva realizada, en su momento, para la atención de una solicitud de acceso a la información por la Dirección de Infraestructura de Tecnologías de la Información, la Gerencia de Seguridad de Tecnologías de la Información, la Subgerencia del Centro de Defensa de Ciberseguridad, la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados B y la Subgerencia de Control del Desarrollo de Sistemas de Pagos e Infraestructuras de Mercados, respecto de diversa información contenida en el documento que se señala a continuación:

TÍTULO DEL DOCUMENTO CLASIFICADO
Consultorías contratadas a solicitud de la DGTI durante los años 2019 y 2020

Al respecto, nos permitimos resaltar que dicha clasificación fue confirmada por el Comité de Transparencia mediante resolución de 10 de septiembre de 2020, emitida en la sesión ordinaria 30/2020, en términos de la fundamentación y motivación expresadas en el oficio del 31 de agosto de 2020, suscrito por la Dirección de Infraestructura de Tecnologías de la Información, la Gerencia de Seguridad de Tecnologías de la Información, la Subgerencia del Centro de Defensa de Ciberseguridad, la Subgerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados B y la Subgerencia de Control del Desarrollo de Sistemas de Pagos e Infraestructuras de Mercados; y en las pruebas de daño correspondientes.

Dicha clasificación se realizó por el periodo de 5 años contados a partir de la confirmación de la misma, lo cual ocurrió el 10 de septiembre de 2020 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **10 de septiembre 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, 20, 15 Bis 1, 18 Bis y 28 Bis 1, del Reglamento Interior del Banco de México (RIBM); Segundo, fracciones IX y XVII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; nos permitimos informarles que estas unidades administrativas **estiman 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 las pruebas de daño correspondientes, que se ponen a disposición de ese Comité de Transparencia.**

Por lo expuesto, y con fundamento en el artículo 104, párrafo tercero, de la LGTAIP; **solicitamos 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, informamos 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 Infraestructuras 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 Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados B (Subgerente) y Subgerente de Control del Desarrollo de Sistemas de Pagos e Infraestructuras de Mercados (Subgerente); así como Dirección de Infraestructura de Tecnologías de la Información (Director), Gerencia de Seguridad de Tecnologías de la Información (Todo el personal), Gerencia de Telecomunicaciones (Gerente), Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Todo el personal), Subgerencia de Administración de Servicios de Telecomunicaciones (Todo el personal) y Subgerencia de Planeación y Regulación (Todo el personal).

Atentamente

CARLOS HERNÁNDEZ LÓPEZ
Gerente de Tecnologías Innovadoras de Sistemas de Pagos e Infraestructuras de Mercados

AURELIO MARTÍN REYES MONTOYA
Gerente de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados

MARCOS PÉREZ HERNÁNDEZ
Director de Infraestructura de Tecnologías de la Información

ARTURO GARCÍA HERNÁNDEZ
Gerente de Seguridad de Tecnologías de la Información

MARIA DEL CARMEN PRUDENTE TIXTECO
Subgerente del Centro de Defensa de Ciberseguridad

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
21/05/2025 13:30:14	AURELIO MARTIN REYES MONTOYA	c88f6c553e6159391ae364189b0c59d07e7b65de152e3542e49a4502baceb2a6
21/05/2025 13:43:19	CARLOS HERNANDEZ LOPEZ	0034095a11feb5254275cb99e348fa019e189f7bae2637efa61ab7308b02b7aa
22/05/2025 12:20:23	MARCOS PEREZ HERNANDEZ	0327865c8b0b0845f94d0b2dcae37d6839709e56b9f58a720bf36b539fdeb58b
23/05/2025 12:36:16	ARTURO GARCIA HERNANDEZ	b4cd31a09d417fd265d3e52f00f3e98cfe84eca6da647925e570fe2ff9a6b146
23/05/2025 12:54:54	MARIA DEL CARMEN PRUDENTE TIXTECO	285c574bc29082771ebf66d0c96d4eabc06fee17fca0544e5965d0138feee12c

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 relativa a la solicitud cuyos datos se señalan a continuación, y:

RESULTANDO

I. DATOS DE LA SOLICITUD

De conformidad a lo establecido en los artículos 124 y 125 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), el Banco de México recibió, en su oportunidad, la solicitud de acceso a la información cuyos datos se indican en la tabla siguiente:

FOLIO:	**6110000028120**
TRANSCRIPCIÓN PÚBLICA DE LA SOLICITUD:	
"Copia en version electronica del numero de consultorías que ha solicitado esa dependencia durante los años 2019 y 2020, lo anterior desglosado por año, persona que la realizo, objetivo y monto pagado en cada caso"	

II. SOLICITUD DE LA UNIDAD ADMINISTRATIVA

Toda vez que el plazo de clasificación inicial que se llevó a cabo para atender la solicitud citada está por concluir, 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 21 de mayo de 2025.	Carlos Hernández López (Gerencia de Tecnologías Innovadoras de Sistemas de Pagos e Infraestructuras de Mercados), Aurelio Martín Reyes Montoya (Gerencia de Desarrollo Tecnológico de Sistemas de Pagos e Infraestructuras de Mercados), ambas unidades administrativas adscritas a la Dirección de Desarrollo e Innovación de Sistemas de Pagos e Infraestructuras de Mercados, a su vez adscrita a la Dirección General de Sistemas de Pagos e Infraestructuras de Mercados, así como Marcos Pérez Hernández (Dirección de Infraestructura de Tecnologías de la Información), Arturo García Hernández (Gerencia de Seguridad de Tecnologías de la Información) y María del Carmen Prudente Tixteco (Subgerencia del Centro de	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 las pruebas de daño correspondientes: **A)** *"Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México"* **B)** *"INFORMACIÓN REFERENTE A LA CONTRATACIÓN DE CONSULTORÍAS EN SEGURIDAD INFORMÁTICA REALIZADAS A LOS SISTEMAS DE PAGOS 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 10 de septiembre de 2020. **Plazo de reserva con ampliación:** 5 años, a partir del 11 de septiembre de 2025.

	Defensa de Ciberseguridad), ambas unidades administrativas adscritas a la Dirección de Seguridad y Organización de la Información, a su vez adscrita a la Dirección General de Tecnologías de la Información, todas del Banco de México.			

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva que soliciten las personas titulares de las unidades administrativas 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 II, así como en las correspondientes pruebas de daño, 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 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 las pruebas de daño respectivas, la divulgación de la información correspondiente representa un riesgo: **A)***"(…) **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 (…)"* y **B)** *"(…) **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 las empresas contratadas o, en su caso de los sistemas de pagos del Banco de México, la substracción de información técnica y datos*

[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).

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 (…)", ***e*****ste 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 II de la presente determinación, así como en términos de las pruebas de daño correspondientes, **y toma conocimiento del nuevo plazo de reserva determinado por las unidades administrativas.**

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 señalada en el oficio mencionado en el resultando II de la presente determinación, conforme a la fundamentación y motivación expresadas en el mismo y en las pruebas de daño correspondientes, 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 26 de junio de 2025. ----------

COMITÉ DE TRANSPARENCIA

_____

CLAUDIA TAPIA RANGEL
Integrante
Unidad de Transparencia

_____

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante
Dirección de Seguridad y Organización de la Información

_____

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
27/06/2025 19:15:01	Edgar Miguel Salas Ortega	ecdc4e7ba9a311749009867b1cd5193fad3f0a0f01bdca95158524f03438263c
27/06/2025 20:20:46	VICTOR MANUEL DE LA LUZ PUEBLA	2ef99cc4b2273029eb087fc7b8d516a86e33c68fd5d724ef95e765a2f47bd643
30/06/2025 09:26:40	Claudia Tapia Rangel	0caacfd928af297fc956b4cceb654a7bdb1d2d65c00df09cfd188280e9653c02