

COMITÉ DE TRANSPARENCIA**ACTA DE LA SESIÓN ESPECIAL 28/2026****DEL 24 DE SEPTIEMBRE DE 2026**

A las trece horas con diez minutos del 24 de septiembre de 2026, participan en la presente sesión a través de medios electrónicos de comunicación, Claudia Tapia Rangel, Titular de la Unidad de Transparencia; Edgar Miguel Salas Ortega, Director Jurídico; y Víctor Manuel De La Luz Puebla, Director de Seguridad y Organización de la Información, 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 (LGPDPPO); 4o. del Reglamento Interior del Banco de México (RIBM); así como con la Quinta y Sexta de las Reglas. Por lo anterior, se procedió en los términos siguientes: -----

APROBACIÓN DEL ORDEN DEL DÍA. -----

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

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

PRIMERO. VERSIONES PÚBLICAS ELABORADAS POR QUIEN ES TITULAR DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP.

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de fecha 18 de septiembre de 2026, suscrito por quien es titular de la Dirección de Infraestructura de Tecnologías de la Información, del Banco de México, el cual se agrega a la presente Acta como **"ANEXO 2"**, por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de clasificar la información referida en dicho oficio, de conformidad con la fundamentación y motivación expresadas en el mismo, así como en las carátulas y prueba de daño correspondiente, y solicitó a este Comité de Transparencia confirmar la clasificación referida. -----

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

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 3, fracción XIX, 39, y 40, fracción II, de la LGTAIP; 31, fracción III, del RIBM; así como la Quinta de las Reglas, resolvió confirmar la clasificación de la información referida en términos de la resolución que se agrega al apéndice de la presente Acta como **"ANEXO 3"**. -----

SEGUNDO. VERSIONES PÚBLICAS ELABORADAS POR QUIENES SON TITULARES DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN, ASÍ COMO DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES, AMBAS DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP. -----

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de fecha 21 de septiembre de 2026, suscrito por quienes son titulares de la Dirección de Infraestructura de Tecnologías de la Información, así como de la Dirección de Apoyo a las Operaciones, ambas 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 su determinación de clasificar la información referida en dicho oficio, de conformidad con la

fundamentación y motivación expresadas en el mismo, así como en las carátulas y pruebas de daño correspondientes, y solicitaron a este Comité de Transparencia confirmar la clasificación referida.-----

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

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 3, fracción XIX, 39, y 40, fracción II, de la LGTAIP; 31, fracción III, del RIBM; así como la Quinta de las Reglas, resolvió confirmar la clasificación de la información referida en términos de la resolución que se agrega al apéndice de la presente Acta como **"ANEXO 5"**.-----

TERCERO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL TÍTULO QUINTO DE LA LGTAIP.-----

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de fecha 29 de junio de 2026, suscrito por quien es titular de la Dirección de Apoyo a las Operaciones del Banco de México, el cual se agrega a la presente Acta como **"ANEXO 6"**, por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de ampliar el periodo de reserva de la información referida en dicho oficio, de conformidad con la fundamentación y motivación señalada en el mismo, así como en la prueba de daño correspondiente, y solicitó a este Órgano Colegiado aprobar la ampliación del periodo de reserva. -----

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

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

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, mismo que coordinó la formalización de la misma. Conste. -----

COMITÉ DE TRANSPARENCIA

CLAUDIA TAPIA RANGEL

Integrante

Unidad de Transparencia

EDGAR MIGUEL SALAS ORTEGA

Integrante

Dirección Jurídica

VÍCTOR MANUEL DE LA LUZ PUEBLA

Integrante

Dirección de Seguridad y Organización de la
Información

SERGIO ZAMBRANO HERRERA

Secretario

LAMO

ASTH

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
25/09/2026 19:38:24	EDGAR MIGUEL SALAS ORTEGA	7050b496aaba4633dde6e77276fbc1cd16a68c0326bdf4aeb27f4f4b20de372d
25/09/2026 19:41:25	VICTOR MANUEL DE LA LUZ PUEBLA	bb0379ca4b2c0147183834aa54891c5f0338f895328614a9c2d0b684ee1712a7
25/09/2026 19:49:06	SERGIO ZAMBRANO HERRERA	1dbe9fd4fdb903c79474b1f6140b0c377499f8c05a747ddc1ac2722a8604e97a
28/09/2026 10:27:36	Claudia Tapia Rangel	3b53ead7c63d81ee4fa30d15aa68b0fc172b3d037371607ae880b7353c2036ed

COMITÉ DE TRANSPARENCIA

ORDEN DEL DÍA

**ACTA DE LA SESIÓN ESPECIAL 28/2026
DEL 24 DE SEPTIEMBRE DE 2026**

PRIMERO. VERSIONES PÚBLICAS ELABORADAS POR QUIEN ES TITULAR DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP.

SEGUNDO. VERSIONES PÚBLICAS ELABORADAS POR QUIENES SON TITULARES DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN, ASÍ COMO DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES AMBAS DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP.

TERCERO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL TÍTULO QUINTO DE LA LGTAIP.

Ciudad de México, a 18 de septiembre de 2026

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente.

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

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

No.	TÍTULO DEL DOCUMENTO CLASIFICADO	TIPO DE CLASIFICACIÓN
1	Resolución S22-086-2022 , Expediente TI.EI.CFR.2020.036 , en la cual se impuso una multa a Banco Azteca, S.A., Institución de Banca Múltiple	Reservada
2	Resolución S22-122-2022 , Expediente TI.EI.SNM.2020.175 , en la cual se impuso una multa a Banco Actinver, S.A., Institución de Banca Múltiple, Grupo Financiero Actinver	Reservada y Confidencial
3	Resolución S22-119-2022 , Expediente TI.EI.CFR.2020.012 , en la cual se impuso una multa a MUFG Bank México, S.A., Institución de Banca Múltiple Filial	Reservada y Confidencial
4	Resolución S22-121-2022 , Expediente TI.EI.SNM.2020.167 , en la cual se impuso una multa a Banco J.P. Morgan, S.A., Institución de Banca Múltiple, J.P. Morgan Grupo Financiero	Reservada
5	Resolución S22-123-2022 , Expediente TI.ID.SNM.2020.179 , en la cual se impuso una multa a Banco Base, S.A., Institución de Banca Múltiple, Grupo Financiero Base	Reservada
6	Resolución S22-082-2022 , Expediente TI.EI.SNM.2021.006 , en la cual se impuso una multa a Banco Nacional de México, S. A., Integrante del Grupo Financiero Banamex	Reservada
7	Resolución S22-083-2022 , Expediente TI.EI.BYS.2021.052 , en la cual se impuso una multa a Banco del Bajío, S.A., Institución de Banca Múltiple	Reservada
8	Resolución S22-084-2022 , Expediente TI.EI.BYS.2021.055 , en la cual se impuso una multa a Casa de Bolsa Base, S.A. de C.V., Grupo Financiero Base	Reservada
9	Resolución S22-085-2022 , Expediente TI.EI.BYS.2021.057 , en la cual se impuso una multa a Grupo Bursátil Mexicano, S.A. de C.V., Casa de Bolsa	Reservada
10	Resolución S22-087-2022 , Expediente TI.EI.BYS.2021.058 , en la cual se impuso una multa a Intercam Banco, S.A., Institución de Banca Múltiple, Intercam Grupo Financiero	Reservada
11	Resolución S22-089-2022 , Expediente TI.EI.BYS.2021.072 , en la cual se impuso una multa a Industrial and Commercial Bank of China México, S.A., Institución de Banca Múltiple	Reservada y Confidencial
12	Resolución S22-090-2022 , Expediente TI.EI.BYS.2021.075 , en la cual se impuso una multa a Banco Bancrea, S.A., Institución de Banca Múltiple	Reservada
13	Resolución S22-468-2026 , Expediente TI.EI.BYS.2025.169 , en la cual se impuso una multa a BanCoppel, S.A., Institución de Banca Múltiple	Reservada

Uso Público

Información de acceso público.

No.	TÍTULO DEL DOCUMENTO CLASIFICADO	TIPO DE CLASIFICACIÓN
14	Resolución S22-388-2026 , Expediente TI.EI.FCA.2026.018 , en la cual se impuso una multa a BBVA México, S.A., Institución de Banca Múltiple, Grupo Financiero BBVA México	Reservada
15	Resolución S22-479-2026 , Expediente TI.EI.DIR.2022.084 , en la cual se impuso una multa a Banco Azteca, S.A., Institución de Banca Múltiple	Reservada y Confidencial
16	Resolución S22-480-2026 , Expediente TI.ID.DIR.2022.085 , en la cual se impuso una multa a Banco Azteca, S.A., Institución de Banca Múltiple	Reservada y Confidencial
17	Resolución S22-275-2026 , Expediente TI.EI.FCA.2022.116 , en la cual se impuso una multa a Bansi, S.A., Institución de Banca Múltiple	Reservada
18	Resolución S22-426-2026 , Expediente TI.EI.AET.2023.027 , en la cual se impuso una multa a Fincomún Servicios Financieros, S.A. de C.V., Sociedad Financiera Popular	Reservada
19	Resolución S22-425-2026 , Expediente TI.EI.SNM.2023.028 , en la cual se impuso una multa a Fincomún Servicios Financieros, S.A. de C.V., Sociedad Financiera Popular	Reservada
20	Resolución S22-1038-2024 , Expediente TI.EI.SNM.2023.033 , en la cual se impuso una multa a Skandia Life, S.A. de C.V. (anteriormente denominada Old Mutual Life, S.A. de C.V.)	Reservada y Confidencial
21	Resolución S22-427-2026 , Expediente TI.EI.FCA.2026.012 , en la cual se impuso una multa a Banco Inmobiliario Mexicano, S.A., Institución de Banca Múltiple	Reservada y Confidencial
22	Resolución S22-424-2026 , Expediente TI.ID.FCA.2026.019 , en la cual se impuso una multa a BBVA México, S.A., Institución de Banca Múltiple, Grupo Financiero BBVA México	Reservada
23	Resolución S22-503-2026 , Expediente TI.EI.SRE.2026.026 , en la cual se impuso una multa a Banco del Bienestar, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo	Reservada
24	Resolución S22-391-2026 , Expediente TI.EI.SRE.2026.036 , en la cual se impuso una multa a Banco Nacional del Ejército, Fuerza Aérea y Armada, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo	Reservada
25	Resolución S22-392-2026 , Expediente TI.EI.FCA.2026.043 , en la cual se impuso una multa a Mizuho Bank México, S.A., Institución de Banca Múltiple	Reservada
26	Resolución S22-393-2026 , Expediente TI.ID.FCA.2026.045 , en la cual se impuso una multa a Mizuho Bank México, S.A., Institución de Banca Múltiple	Reservada
27	Resolución S22-423-2026 , Expediente TI.BM.OSI.2026.013 , en la cual se impuso una multa a Banco Actinver, S.A., Institución de Banca Múltiple, Grupo Financiero Actinver	Reservada
28	Resolución S22-444-2026 , Expediente TI.EI.DIR.2026.051 , en la cual se impuso una multa a Banco Nacional del Ejército, Fuerza Aérea y Armada, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo	Reservada
29	Resolución S22-470-2026 , Expediente TI.EI.DIR.2026.055 , en la cual se impuso una multa a Banco Base, S.A., Institución de Banca Múltiple, Grupo Financiero Base	Reservada
30	Resolución S22-525-2026 , Expediente TI.EI.DIR.2026.069 , en la cual se impuso una multa a Ualá, S.A., Institución de Banca Múltiple	Reservada
31	Resolución S22-454-2026 , Expediente TI.EI.FCA.2026.015 , en la cual se impuso una multa a Banco J.P. Morgan, S.A., Institución de Banca Múltiple, J.P. Morgan Grupo Financiero	Reservada y Confidencial
32	Resolución S22-455-2026 , Expediente TI.ID.FCA.2026.016 , en la cual se impuso una multa a Banco J.P. Morgan, S.A., Institución de Banca Múltiple, J.P. Morgan Grupo Financiero	Reservada y Confidencial
33	Resolución S22-446-2026 , Expediente TI.EI.DIR.2026.058 , en la cual se impuso una multa a HSBC México, S.A., Institución de Banca Múltiple, Grupo Financiero HSBC	Reservada

Uso Público

Información de acceso público.

No.	TÍTULO DEL DOCUMENTO CLASIFICADO	TIPO DE CLASIFICACIÓN
34	Resolución S22-445-2026 , Expediente TI.El.DIR.2026.059 , en la cual se impuso una multa a MUFG Bank México, S.A., Institución de Banca Múltiple Filial	Reservada

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

Asimismo, informo que el personal que por la naturaleza de sus atribuciones tiene acceso a los documentos referidos, es el adscrito a la Dirección de Infraestructura de Tecnologías de la Información (Director), Gerencia de Telecomunicaciones (Gerente), Subgerencia de Supervisión y Sanciones de Infraestructura de Tecnologías de la Información (todo el personal), Dirección de Autorizaciones y Sanciones de Banca Central (Director), Gerencia de Sanciones de Banca Central (Gerente), Subgerencia de Sanciones de Banca Central (todo el personal).

Atentamente,

MARCOS PÉREZ HERNÁNDEZ

Director de Infraestructura de Tecnologías de la Información

Uso Público

Información de acceso público.

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
18/09/2026 13:48:17	MARCOS PEREZ HERNANDEZ	8c574e70b4212e4af13b0e2a252b51d65e0f2579a65aa0a596ae03e8c84d1de6

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

OBLIGACIONES DE TRANSPARENCIA

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

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

RESULTANDO

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

II. SOLICITUD DE LA UNIDAD ADMINISTRATIVA

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

FECHA O REFERENCIA DEL OFICIO	UNIDAD(ES) ADMINISTRATIVA (S) SOLICITANTE(S) Y NOMBRE(S) DE SU(S) TITULAR(ES)	SOLICITUD DEL OFICIO	INFORMACIÓN CLASIFICADA	VERSIONES PÚBLICAS	PLAZO DE CLASIFICACIÓN
Oficio de fecha 18 de septiembre de 2026.	Marcos Pérez Hernández (Dirección de Infraestructura de Tecnologías de la Información del Banco de México.)	Confirmación de clasificación de información.	Información confidencial en términos de lo señalado en el oficio y en las carátulas correspondientes. - Datos personales: Datos identificativos: - Nombre de persona física - Información presentada por particulares con el carácter de confidencial. Información reservada en términos de lo señalado en el oficio y en la prueba de daño correspondiente. <i>"Información relacionada con el incumplimiento en que incurrió el Participante en el sistema de pagos que administra, opera y supervisa el Banco de México, respecto a los requisitos de seguridad informática y especificaciones técnicas que debía observar la infraestructura tecnológica con la que opera con tal sistema de pagos"</i>	34 versiones públicas señaladas en el oficio correspondiente.	Información confidencial: No está sujeta a temporalidad, en términos del artículo 115, segundo párrafo, de la LGTAIP. Información reservada: 5 años, a partir de la presente resolución (vencimiento: 24 de septiembre de 2031).

CONSIDERANDO

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

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

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

Asimismo, este Comité de Transparencia advierte que no se actualiza alguno de los supuestos de excepción previstos en ley para que el Banco de México se encuentre en posibilidad de permitir el acceso a la información señalada, en términos de los artículos 119 de la LGTAIP y 16 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO).

En consecuencia, y considerando que, conforme a lo manifestado en la prueba de daño respectiva, la divulgación de la información representa un riesgo de perjuicio significativo al interés público *"(...) provocaría un menoscabo en la efectividad de las medidas implementadas en los sistemas financieros o económico del país, poniendo en riesgo el funcionamiento de esos sistemas, incluidos los sistemas de pagos o, en su caso, de la economía nacional en su conjunto; asimismo, pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país o finalmente, también podría obstruir la prevención de delitos y obstaculizar las acciones implementadas por este Banco Central para evitar su comisión (...)"*, **este Comité de Transparencia confirma la clasificación de la información señalada como confidencial y como reservada, respectivamente**, de conformidad con lo expresado en el oficio referido en el resultando II de la presente resolución, así como en las carátulas y en la prueba de daño correspondiente, **y toma conocimiento del plazo de reserva determinado por la unidad administrativa correspondiente.**

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

RESUELVE

ÚNICO. Se confirma la clasificación de la información señalada como confidencial y como reservada, respectivamente, en el oficio citado en el resultando II de la presente determinación, conforme a la fundamentación y motivación expresadas en los mismos, así como en las carátulas y en la prueba de daño correspondiente, en términos del considerando Segundo de la presente resolución.



"2026, Año de Margarita Maza Parada"

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en la sesión celebrada el 24 de septiembre de 2026. -----

COMITÉ DE TRANSPARENCIA

CLAUDIA TAPIA RANGEL

Integrante

Unidad de Transparencia

EDGAR MIGUEL SALAS ORTEGA

Integrante

Dirección Jurídica

VÍCTOR MANUEL DE LA LUZ PUEBLA

Integrante

Dirección de Seguridad y Organización de la
Información

LAMO
ASTH

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
25/09/2026 19:38:26	EDGAR MIGUEL SALAS ORTEGA	588691079e695f84df69b97b89c34bba53305e60dc1d19375f34d0f41ea752e5
25/09/2026 19:41:23	VICTOR MANUEL DE LA LUZ PUEBLA	24b0901cb47f5a56bd577354b4750452d251d5111808f94765abf4492c9d27d2
28/09/2026 10:27:50	Claudia Tapia Rangel	2c876c6cbf7e6c7822bb5b8d671944dc72f4bd57e2e707b9839e59d27bdf0bc8

Ciudad de México, 21 de septiembre de 2026

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

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

Sobre el particular, en relación con las referidas obligaciones de transparencia, nos permitimos informarles que estas unidades administrativas, de conformidad con los artículos 102 y 103, fracción III, de la LGTAIP, han determinado clasificar diversa información contenida en los documentos que se indican en el cuadro siguiente, de conformidad con la fundamentación y motivación señaladas en las carátulas y en las pruebas de daño correspondientes.

TÍTULO DEL DOCUMENTO CLASIFICADO	TIPO DE CLASIFICACIÓN
Autorización para adjudicar identificado con el ID PAC 25-0522 (800-25-0522-1)	Reservada
Contrato No. 163488 (800-25-0522-1)	Reservada
Dictamen de excepción. Mayo 2025 (800-25-0522-1)	Reservada

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

Asimismo, informamos que el personal que por la naturaleza de sus atribuciones tiene acceso a los documentos referidos 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 Cómputo (Gerente).
- Subgerencia de Administración de Servicios de Cómputo (todo el personal).
- Subgerencia de Planeación y Regulación (todo el personal).

Por parte de la Dirección de Apoyo a las Operaciones:

- Dirección de Apoyo a las Operaciones (Director).
- Gerencia de Desarrollo de Sistemas Operativos (Gerente).
- Oficina de Pruebas de Sistemas de Banca Central (Jefe).

Uso Público

Información de acceso público.

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,

MARCOS PÉREZ HERNÁNDEZ

Director de Infraestructura de Tecnologías de la
Información

JOAQUÍN RODRIGO CANO JAUREGUI

SEGURA MILLAN

Director de Apoyo a las Operaciones

Uso Público

Información de acceso público.

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
21/09/2026 14:39:49	JOAQUIN RODRIGO CANO JAUREGUI SEGURA ...	d4e63e1666c48c7593f98fce58bf1b6adc4055b1f39f62e90dc086967a9af9ad
21/09/2026 16:48:25	MARCOS PEREZ HERNANDEZ	731f78f3b32278897078910f14d65d602aeeaf3cc889ec93d27a508f3c9d57e6

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO**OBLIGACIONES DE TRANSPARENCIA**

Unidades Administrativas: Dirección de Infraestructura de Tecnologías de la Información y Dirección de Apoyo a las Operaciones, ambas del Banco de México.

VISTOS, para resolver sobre la clasificación de información determinada por las unidades administrativas al rubro indicadas, y:

RESULTANDO

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

II. SOLICITUD DE LAS UNIDADES ADMINISTRATIVAS

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

FECHA O REFERENCIA DEL OFICIO	UNIDAD(ES) ADMINISTRATIVA(S) SOLICITANTE(S) Y NOMBRE(S) DE SU(S) TITULAR(ES)	SOLICITUD DEL OFICIO	INFORMACIÓN CLASIFICADA	VERSIONES PÚBLICAS	PLAZO DE CLASIFICACIÓN
Oficio de fecha 21 de septiembre de 2026.	Marcos Pérez Hernández (Dirección de Infraestructura de Tecnologías de la Información) y Joaquín Rodrigo Cano Jauregui Segura Millan (Dirección de Apoyo a las Operaciones), ambas del Banco de México.	Confirmación de clasificación de información.	Información reservada en términos de lo señalado en el oficio y en las pruebas de daño correspondientes: <i>A. "Información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales".</i>	3 versiones públicas señaladas en el oficio correspondiente.	Información reservada: 5 años, a partir de la presente resolución (vencimiento: 24 de septiembre de 2031).

			B. “Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México”.		
--	--	--	---	--	--

CONSIDERANDO

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

SEGUNDO. Este Comité de Transparencia, tomando en cuenta que en términos del artículo 102, párrafo tercero, de la LGTAIP, corresponde a las personas titulares de las áreas de los sujetos obligados clasificar la información, advierte que las razones, motivos y circunstancias especiales que llevaron a concluir que en el caso particular se actualiza la necesidad de **clasificar** la información señalada, que se contiene en el oficio referido en el resultando II, así como en las carátulas y en las pruebas de daño correspondientes, los cuales se tienen aquí por reproducidos como si a la letra se insertasen¹.

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

En consecuencia, y considerando que conforme a lo manifestado en las pruebas de daño respectivas, la divulgación de la información **A. “(...) *representa un riesgo de perjuicio significativo al interés público ya que revelar información referente al software que soporta la implementación de las operaciones monetarias, cambiarias y como agente financiero que este Instituto Central lleva a cabo por cuenta propia o a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales, pone en riesgo de destrucción, inhabilitación o sabotaje infraestructura de tal importancia para la economía mexicana que si destrucción o incapacidad tendría un impacto negativo en la efectividad de las medidas adoptadas en los sistemas financiero, económico, cambiario monetario del país, poniendo en riesgo el funcionamiento o, en su caso, de la economía nacional en su conjunto o, bien pueda incrementar el costo de las operaciones financieras que realicen los sujetos obligados del sector público federal; (...)*” 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; pondría en***

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 explicita, 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).

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 con la divulgación de la información referida (...)”, este Comité de Transparencia confirma la clasificación de la información señalada como reservada, de conformidad con lo expresado en el oficio referido en el resultando II de la presente resolución, así como en las carátulas y en las pruebas de daño correspondientes, y toma conocimiento del plazo de reserva determinado por las unidades administrativas correspondientes.

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

RESUELVE

ÚNICO. Se confirma la clasificación de la información referida como reservada, respectivamente, señalada en el oficio citado en el resultando II de la presente determinación, conforme a la fundamentación y motivación expresadas en el mismo, así como en las carátulas y en las pruebas de daño correspondiente, en términos del considerando Segundo de la presente resolución.

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en la sesión celebrada el 24 de septiembre de 2026. -----

COMITÉ DE TRANSPARENCIA

CLAUDIA TAPIA RANGEL

Integrante

Unidad de Transparencia

EDGAR MIGUEL SALAS ORTEGA

Integrante

Dirección Jurídica

VÍCTOR MANUEL DE LA LUZ PUEBLA

Integrante

Dirección de Seguridad y Organización de la
Información

ASTH
LAMO

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
25/09/2026 19:38:25	EDGAR MIGUEL SALAS ORTEGA	a0022dbb7fa1dd479f036448bf344b448c1cba9cfb547f2a542e8073436bfb8b
25/09/2026 19:41:28	VICTOR MANUEL DE LA LUZ PUEBLA	232e3d733d1c36e125ca33ab897b93e1ad97b99d5ec86afbb3da212c7b451a6f
28/09/2026 10:27:41	Claudia Tapia Rangel	e4005260abed3af158432eb0929b1f0cd3eb462d1011ea8f7bb29fc87ee31e66



Ciudad de México, 29 de junio de 2026

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente.

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

No.	TÍTULO DEL DOCUMENTO CLASIFICADO
1	Autorización para adjudicar directamente por monto hasta \$294,401.70 con ID PAC 21-0914 (800-21-0914-1)
2	Pedido No. 0000028133 (800-21-0914-1)

Al respecto, me permito resaltar que dicha clasificación fue confirmada por ese Comité mediante resolución de 30 de septiembre de 2021, emitida en la sesión Especial 32/2021, en términos de la fundamentación y motivación expresadas en el oficio de 23 de septiembre de 2021, 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 30 de septiembre de 2021 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **30 de septiembre de 2026**.

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, 19 Bis 1, 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**

Uso Público

Información de acceso público.



presente oficio, por 5 años adicionales, 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:

Por parte de la Dirección de Apoyo a las Operaciones:

- Dirección de Apoyo a las Operaciones (Director)
- Gerencia de Desarrollo de Sistemas Operativos (Gerente)
- Oficina de Pruebas de Sistemas de Banca Central (Jefe)

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

- Dirección de Infraestructura de Tecnologías de la Información (Director)
- Gerencia de Cómputo (Gerente)
- Subgerencia de Desarrollo de Servicios de Cómputo (todo el personal)
- Subgerencia de Planeación y Regulación (todo el personal)

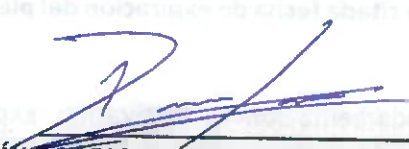
Por parte de la Dirección de Recursos Materiales:

- 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


JOAQUÍN RODRIGO CANO JAUREGUI SEGURA MILLÁN
Director de Apoyo a las Operaciones

Uso Público

Información de acceso público.

PRUEBA DE DAÑO

Información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales.

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

- a) Afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país,
- b) Incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal;
- c) Obstruir la prevención de delitos.

En este sentido, ***Información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales*** es clasificada como reservada, en virtud de lo siguiente:

La divulgación de la citada información representa un riesgo de perjuicio significativo al interés público ya que revelar información referente al software que soporta la implementación de las operaciones monetarias, cambiarias y como agente financiero que este Instituto Central lleva a cabo por cuenta propia o a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales, pone en riesgo de destrucción, inhabilitación o sabotaje, infraestructura de tal importancia para la economía mexicana que si destrucción o incapacidad tendría un impacto negativo en la efectividad de las medidas adoptadas en los sistemas financiero, económico, cambiario monetario del país, poniendo en riesgo el funcionamiento o, en su caso, de la economía nacional en su conjunto o, bien pueda incrementar el costo de las operaciones financieras que realicen los sujetos obligados del sector público federal; toda vez que dicho riesgo es:

1. Real, en razón de que revelar o divulgar ***la Información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas***

internacionales, tales como el nombre del sistema y las especificaciones técnicas, entre otros, , **facilita a una persona o grupo de personas con intenciones delincuenciales identificar - de manera directa o a través de técnicas de ingeniería social aplicada a los proveedores - información relacionada con el esquema informático que soporta las operaciones de banca central administrado por este Instituto Central, lo cual posibilita la realización de acciones hostiles en contra de las tecnologías de la información de este Banco Central**, así como de las infraestructuras que éste administra, opera y supervisa, lo cual, podría menoscabar la efectividad de las infraestructuras a tal grado, que su destrucción o inhabilitación afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, arriesgando el funcionamiento de esos sistemas y, en consecuencia, de la economía nacional en su conjunto.

Al respecto, Debe tenerse presente que los artículos 2o. y 3o. de la Ley del Banco de México, señalan las finalidades y funciones del Banco Central de la Nación, entre las que se encuentran, el objetivo prioritario de **procurar la estabilidad del poder adquisitivo de la moneda nacional**, promover el sano desarrollo del sistema financiero, propiciar el buen funcionamiento de los sistemas de pagos, así como el desempeño de las funciones de regular los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos; operar con las instituciones de crédito como banco de reserva y acreditante de última instancia; **prestar servicios de tesorería al Gobierno Federal y actuar como agente financiero del mismo**, las cuales comprenden de sus funciones de la banca central. Las anteriores son finalidades y funciones que dependen en gran medida de la correcta operación de las tecnologías de la información que el Banco de México ha instrumentado para estos propósitos, mediante el procesamiento de la información que apoya en la ejecución de dichos procesos.

Cabe señalar que las Tecnologías de Información que utiliza y contrata el Banco de México, como son los sistemas que soportan las operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales, son adquiridos, desarrollados o destinados para atender, entre otras, la implementación de las políticas en materia monetaria y cambiaria¹, y para atender las funciones de agente financiero del gobierno federal. Por tal motivo, divulgar información relacionada con el nombre del sistema o las especificaciones técnicas, normatividad interna, o configuraciones de dichos sistemas, puede propiciar su inhabilitación y en un extremo escenario, podría perturbar considerablemente al sistema financiero por su efecto directo en la información y operaciones relativas a la implementación de las políticas monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales. Cabe señalar que los sistemas que utiliza y adquiere el Banco de México, como son los

¹ Las políticas en materia cambiaria son una decisión de la Comisión de Cambios

Los riesgos aludidos tienen mayor probabilidad de materializarse con la entrega de la información, debido a que **los delincuentes podrían diseñar estrategias para llevar a cabo ataques cibernéticos dirigidos específicamente a los sistemas que soportan las operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales**, 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 del sistema financiero; 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 en las operaciones a través de las cuales se implementan las políticas monetaria y cambiaria y las funciones de agente financiero.**

Un ataque cibernético a los sistemas que soportan las operaciones de regulación monetaria, cambiaria y de agente financiero del gobierno federal, puede provocar la sustracción, interrupción o alteración de la información que se recibe, se procesa y se resguarda en relación a, por ejemplo, las asignaciones de las subastas que este Instituto Central lleva a cabo con propósitos de regulación monetaria, regulación cambiaria o de agente financiero del gobierno federal, así como las operaciones cambiarias que realiza como agente financiero del gobierno federal o en la administración de la reserva internacional. Una liquidación errónea derivada de una alteración en los sistemas que generan las órdenes de cobro o pago de las operaciones antes mencionadas puede derivar en un incumplimiento involuntario de las obligaciones del Banco Central o del gobierno federal con el consecuente pago de penas, incremento en el costo de operaciones y daño en la confianza y reputación de estas instituciones. De forma similar, la interrupción o imposibilidad de ejecutar las subastas monetarias, cambiarias y de agente financiero que realiza el Banco Central, generaría desconfianza, nerviosismo y especulación en el sistema financiero sobre la capacidad del Banco para operar en los mercados financieros, originando presiones sobre las tasas de interés y sobre el tipo de cambio y afectando por ende, el cumplimiento del objetivo prioritario del Banco que es la estabilidad del poder adquisitivo de la moneda nacional.

La realización de hechos como los previamente narrados podría traducirse en un menor interés por parte de los intermediarios financieros en participar en las subastas con propósitos de regulación monetaria, cambiaria y de agente financiero del gobierno federal, comprometiendo la implementación de la política monetaria y por ende la consecución del objetivo prioritario de procurar la estabilidad de precios del Banco. De igual forma comprometerían la implementación de la política cambiaria establecida por la Comisión de Cambios con el consecuente deterioro del mercado de cambios local y por ende del sistema financiero del país; e incrementarían el costo de las operaciones del gobierno federal que, al verse imposibilitado de conseguir financiamiento a través de las subastas primarias de

valores gubernamentales, tendría que buscar otros medios de financiamiento a mayores costos.

En efecto, proporcionar 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 o resguardan en ellas o, incluso, dejen fuera de operación a dichas tecnologías.

Incluso, los ataques cibernéticos pueden provocar la sustracción, interrupción o alteración de la información relativa a, por ejemplo: las asignaciones de las subastas que el Instituto central lleva a cabo con propósitos de regulación monetaria, cambiaria y como agente financiero del Gobierno Federal; la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de estos sistemas, la sustracción de información que no debe ser alterada o divulgada de forma no autorizada, lo cual pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de las infraestructuras de los mercados financieros, entre ellas los sistemas de pagos.

En efecto, proporcionar 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.

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.

Otra característica de este tipo de ataques, es la propia evolución de los equipos y sistemas, pues con cada actualización, nueva versión que se genera, o nuevo componente que se instale, se abre la oportunidad a la aparición de vulnerabilidades y, por ende, a nuevas posibilidades de ataque. Por ejemplo, en la actualidad, es común que en materia de sistemas de información se empleen herramientas con licencia de uso libre (p.e. librerías de manejo de memoria, traductores entre distintos formatos electrónicos, librerías para despliegue de gráficos, etc.), y que el proveedor publique las vulnerabilidades detectadas en ellas; contando con esta información y con las especificaciones técnicas de la aplicación o herramienta tecnológica que se quiere vulnerar, aquellos individuos con propósitos delincuenciales pueden elaborar un ataque cuya vigencia será el tiempo que tarde en corregirse la vulnerabilidad y aplicarse la actualización respectiva.

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.²

En el caso en concreto, la información materia de esta prueba de daño contiene detalles sobre los formatos y códigos necesario para la realización de pagos y liquidaciones, nombres del sistema, especificaciones respecto de los servicios prestados, características de los productos, entre otros, por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales aprovechar los puntos débiles de los niveles de servicio y por ende de las infraestructuras que soportan las **operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales, y en consecuencia llevar a cabo ataques informáticos 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. **Demostable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, los sistemas de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo, 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.**

Adicionalmente, **está documentado 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.³

² Wilshusen, G. C., & Powner, D. A. (2009). Cybersecurity: Continued efforts are needed to protect information systems from evolving threats (No. GAO-10-230T). GOVERNMENT ACCOUNTABILITY OFFICE WASHINGTON DC.

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

Por lo anterior, este Instituto Central⁴ y autoridades como la Secretaría de Hacienda y Crédito Público⁵ se han pronunciado sobre la importancia de fortalecer la ciberseguridad para la estabilidad del sistema financiero.

Para demostrar lo anterior, se citan algunos de los ataques más relevantes:

- i) El ataque de tipo "*Watering hole*" en Polonia, que permitió utilizar un servidor de la Autoridad de Supervisión Financiera para distribuir código malicioso a más de 20 bancos polacos⁶, el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada;⁷
- ii) El ataque del ransomware de *WannaCry*, que aprovechó una vulnerabilidad inherente de Microsoft Windows, para cifrar la información contenida en las máquinas y exigir el pago de un "rescate" para devolver el contenido a su forma original, el cual interrumpió significativamente la operación rutinaria de varias instituciones comerciales y gubernamentales, incluidas Fedex, Deutsche Bahn, Megafon, Telefónica, el Banco Central de Rusia, Ferrocarriles de Rusia y el Ministerio del Interior de Rusia;⁸
- iii) El ataque que se perpetuó 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
- iv) Los ataques cibernéticos que han sufrido otros Bancos Centrales a través de la infraestructura de sistemas de pagos conocida como SWIFT, la cual ha sido utilizada para realizar robos de capital, uno de estos casos es el del Banco Central de Bangladesh, que

⁴ En septiembre de 2016, el Banco de México publicó el documento "Política y funciones del Banco de México respecto a las infraestructuras de los mercados financieros" en el cual dedica una sección especial al tema de seguridad informática. Este documento se encuentra disponible en la siguiente dirección [Microsoft Word - Política y funciones del BdeM sobre IMF Final.docx](#) consultado el 04 de marzo de 2018.

⁵ 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 04 de marzo de 2026.

⁶ BadCyber, Author. "Several Polish Banks Hacked, Information Stolen by Unknown Attackers." BadCyber, 9 de febrero de 2017, <http://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/> consultado el 04 de marzo de 2026.

⁷ BAE Systems Applied Intelligence. "BAE Systems Threat Research Blog." Lazarus & Watering-Hole Attacks, 12 de febrero de 2017. <http://baesystemsai.blogspot.mx/2017/02/lazarus-watering-hole-attacks.html> consultado el 04 de marzo de 2026.

⁸ Mattei, T. A. (2017). Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack. *World Neurosurgery*, 104, 972-974.

⁹ BANCOMEXT. "Acción oportuna de BANCOMEXT salvaguarda intereses de clientes y la institución". 10 de enero de 2018. [Acción oportuna de Bancomext salvaguarda intereses de clientes y la institución - BancomextBancomext](#), consultado el 04 de marzo de 2026.

sufrió un robo de 81 millones de dólares.¹⁰ O como el caso del Banco del Austro en Ecuador, en el que los atacantes utilizaron un método muy similar al de Bangladesh, para robar 12 millones de dólares.¹¹

- v) 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.¹² A la fecha de elaboración de la presente prueba de daño, se estima un daño a los participantes del SPEI de aproximadamente 300 millones de pesos.¹³ Este incidente evidenció vulnerabilidades estructurales en los aplicativos de terceros utilizados para la conexión al SPEI y detonó una respuesta regulatoria y estratégica sin precedentes por parte del Banco de México.¹⁴
- vi) El ciberataque a la tienda Coppel en septiembre 2024, que afectó de forma significativa su operación, limitando alrededor de 9,500 servicios de negocio y generando interrupciones en sus 1,800 tiendas a nivel nacional durante aproximadamente tres meses. La afectación se extendió a sistemas clave como ventas, logística, comercio electrónico y distribución, evidenciando la falta de preparación ante un incidente de esta magnitud y provocando pérdidas millonarias. El ataque, atribuido al grupo de ransomware LockBit 3.0, obligó a la empresa a ejecutar un proceso intensivo de recuperación, logrando restablecer el 86% de sus servicios en dos meses y medio y el total en tres meses, apoyándose en soluciones tecnológicas en la nube para acelerar la restauración.¹⁵
- vii) Ciberataque a la plataforma de reclutamiento con IA de McDonald's (McHire) en junio del 2025, donde un error básico de configuración permitió el acceso a un panel administrativo protegido solo con credenciales débiles combinado con una vulnerabilidad tipo IDOR (Control de acceso remoto con explotación simple de alto impacto y confianza excesiva), posibilitó la exposición de hasta 64 millones de solicitudes

¹⁰ Michael Riley, Alan Katz. "Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh". Bloomberg. 26 de Mayo de 2016. <https://www.bloomberg.com/news/articles/2016-05-26/swift-hack-probe-expands-to-up-to-dozen-banks-beyond-bangladesh> consultado el 04 de marzo de 2026.

¹¹ Clavijo R. Felipe, Osorio Daniel y Yanquen Eduardo. (2017). "RIESGO CIBERNÉTICO: RELEVANCIA Y ENFOQUES PARA SU REGULACIÓN Y SUPERVISIÓN", 92 (Colombia).

¹² Banco de México. "Información sobre los ataques a los Participantes del SPEI". Mayo 2018 <https://www.banxico.org.mx/spei/d/%7BFFC53F5A-CA04-3098-EBF6-B0F17E533183%7D.pdf>, consultado el 04 de marzo de 2026.

¹³ Acorde con los "Puntos importantes sobre la situación actual del SPEI" publicados en la página de internet del Banco de México, 22 de mayo 2018 <https://www.banxico.org.mx/spei/d/%7B8806F1E8-686D-B9F1-0452-EC375543C801%7D.pdf> consultados el 04 de marzo de 2026.

¹⁴ Banco de México. "Estrategia de Ciberseguridad del Banco de México, 2024-2027" publicados en la página de internet del Banco de México. El 20 de junio del 2024. <https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf> consultado el 08 de mayo del 2026.

¹⁵ El Financiero, Coppel admite hackeo en 1800 tiendas, limitó sus operaciones por 3 meses. Septiembre 2024. <https://www.elfinanciero.com.mx/empresas/2024/09/05/tuviste-problemas-con-coppel-admite-que-hackeo-en-1800-tiendas-limito-sus-operaciones-por-3-meses/> consultado 15 de abril de 2026.

de empleo con datos personales y conversaciones de entrevistas; aunque el proveedor corrigió rápidamente la falla tras ser notificado, esta prueba de daño evidencia, que incluso sistemas avanzados basados en inteligencia artificial pueden ser altamente vulnerables por fallos elementales de seguridad, subrayando la necesidad de controles robustos, gestión adecuada de accesos y supervisión de terceros tecnológicos.¹⁶

viii) United Natural Foods Inc. (UNFI), principal distribuidor de productos para Whole Foods en Estados Unidos, Un ataque cibernético en junio del 2025, que provocó una interrupción masiva de suministro de alimentos en Estados Unidos, obligando a la empresa a desconectar sus sistemas para contener la intrusión y generando retrasos en pedidos y entregas; como consecuencia, múltiples tiendas experimentaron estantes vacíos y limitaciones operativas, mientras empleados reportaron imposibilidad de procesar órdenes y realizar actividades normales, evidenciando la alta dependencia de sistemas tecnológicos en la logística alimentaria y cómo un incidente de ciberseguridad puede impactar directamente en el abastecimiento nacional y la experiencia del consumidor. Esta prueba de daño causada por una intrusión no autorizada que evoluciono a movimientos laterales dentro de la red, alcanzando los sistemas centrales y comprometiéndolos causando un mecanismo extremo para su contención.¹⁷

ix) Banco central de Brasil sufrió un ataque informático a su sistema de pagos "PIX" en julio de 2025, este incidente generó pérdidas superiores a 540 millones de reales, evidenció vulnerabilidades críticas en la cadena de suministro tecnológica del sector financiero, particularmente por el uso indebido de credenciales internas vendidas por un empleado, lo que permitió a los atacantes desviar fondos hacia cuentas controladas y posteriormente convertirlos en criptomonedas; esta prueba de daño resalta que la ciberseguridad en instituciones financieras no solo depende de la tecnología, sino también del factor humano y de terceros proveedores, subrayando la necesidad de adoptar estrategias como autenticación multifactor, monitoreo, arquitectura de cero confianza, mínimo privilegio y cumplimiento regulatorio, ya que la creciente digitalización incrementa la superficie de ataque y pone en riesgo tanto los recursos financieros como la confianza de los usuarios en el sistema.¹⁸

x) Investigadores de Estados Unidos demostraron la alta vulnerabilidad de las comunicaciones satelitales en México al acceder, de forma pasiva y con equipo accesible como una antena parabólica y una tarjeta de televisión, a información sensible del

¹⁶ Instituto nacional de ciberseguridad, *Fallo de seguridad en la IA de selección de McDonald's expone datos de millones de solicitantes*. Agosto 2025. <https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/fallo-de-seguridad-en-la-ia-de-seleccion-de-mcdonalds-expone-datos-de> consultado 15 de abril del 2026.

¹⁷ Telemundo San Antonio, EEUU, *Un ciberataque a UNFI provoca escasez en Whole Foods; afecta a todo el país*. Junio 2025. <https://www.telemundosanantonio.com/noticias/eeuu/ciberataque-a-unfi-provoca-escasez-whole-foods-afecta-todo-el-pais/2434649/> consultado el 15 de abril del 2026.

¹⁸ Tiiside, *La importancia de la ciberseguridad en las instituciones financieras: lecciones del ataque Pix*, Julio 2025. <https://tiiside.com.br/es/14/07/2025/a-importancia-da-ciberseguranca-nas-instituicoes-financeiras-liceo-do-ataque-ao-pix-em-2025/> consultado el 15 de abril del 2026.

Gobierno, fuerzas armadas y empresas privadas. El estudio evidenció que una cantidad significativa de datos, incluyendo llamadas telefónicas, mensajes, inventarios militares y datos de infraestructura crítica se transmitían sin ningún tipo de cifrado, lo que permitió su interceptación sin necesidad de hackear directamente los sistemas. Esta prueba de daño expone la urgencia de implementar mecanismos de cifrado en las comunicaciones para prevenir accesos no autorizados.¹⁹

- xi) Deficiencias en controles de calidad y seguridad del portal de Telcel para el registro de líneas telefónicas en México en enero del 2026, permitieron la explotación de fallas de acceso, esta prueba de daño tuvo con consecuencia la exposición de datos personales sensibles. Este incidente generó desconfianza en los usuarios, afectación reputacional para la empresa y cuestionamientos al Gobierno Federal sobre la efectividad de la estrategia para combatir la extorsión. La ausencia de pruebas adecuadas y de medidas sólidas de ciberseguridad que provocó la interrupción temporal del sistema para su corrección, evidenciando que la información pudo ser expuesta sin necesidad de un ciberataque sofisticado, sino por debilidades estructurales en el desarrollo y falta de testados.²⁰

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

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

¹⁹ El País, *Científicos en EEUU acceden a datos sensibles sin encriptar del gobierno mexicano con apenas una antena parabólica y una tarjeta de televisión*. Octubre del 2025. <https://elpais.com/mexico/2025-10-16/cientificos-en-eeuu-acceden-a-datos-sensibles-sin-encriptar-del-gobierno-mexicano-con- apenas-una-antena-parabolica-y-una-tarjeta-de-television.html> consultado el 15 de abril del 2026.

²⁰ El País, *Los errores y la fuga de datos personales manchan el primer intento masivo de registrar los celulares mexicanos*, enero 2026. <https://elpais.com/mexico/2026-01-17/los-errores-y-la-fuga-de-datos-personales-manchan-el-primer-intento-masivo-de-registrar-los-celulares-mexicanos.html> consultado el 15 de abril del 2026.

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, configuración y normatividad de los programas o dispositivos a personas cuyo rol no esté autorizado**, 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.

Sea cual fuere el origen o motivación del ataque contra las tecnologías de la información y de comunicaciones administradas por el Banco Central, éste puede conducir al incumplimiento de sus obligaciones hacia los participantes del sistema financiero y/o provocar que, a su vez, estos no puedan cumplir con sus propias obligaciones, y en consecuencia, generar un colapso del sistema financiero nacional, lo que iría en contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.

3. **Identificable, puesto que el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques.** Sin perjuicio de lo anterior, se puede mencionar que en el año 2024 nuestros registros indican un promedio de 2,618 intentos de ataque al mes, llegando a presentarse hasta 10,464 intentos de ataque en un único mes. 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 que soportan las operaciones de banca central 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 información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales, podría resultar en la afectación y alteración de:**

1. **Las asignaciones de las subastas que este instituto lleva a cabo con propósitos de regulación monetaria, cambiaria y de agente financiero del Gobierno Federal.** A su vez estas afectaciones podrían, en caso de alterar las asignaciones de las subastas, menoscabar el efecto de las medidas adoptadas en las políticas monetaria, cambiaria y del sistema financiero del país; e incrementar el costo financiero del Gobierno Federal.
2. **Las operaciones relacionadas con la administración de la Reserva Internacional.**

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 monetario, cambiario, 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 referente a la **información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacional**, no satisface un interés público, por el contrario, es información que pone en riesgo la efectividad de las medidas adoptadas en los sistemas monetario, cambiario y del sistema financiero, así como 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 del buen funcionamiento de los mercados financieros del país.

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 que soportan las operaciones de banca central administrados 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 resultados de las subastas que realiza este instituto o de las operaciones relacionadas con la administración de la Reserva Internacional o 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 de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales evitará poner en riesgo la efectividad de las medidas en materia monetaria y cambiaria, 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 Ley**, tal y como se demostró en el presente caso.

"2026. Año de Margarita Maza Parada"

En razón de lo anterior, y vistas las consideraciones expuestas en el presente documento, con fundamento en lo establecido en los artículos 6o., párrafo cuarto, apartado A, fracciones I y VIII, párrafo cuarto, 28, párrafos séptimo y octavo, de la CPEUM; 1, 102, 103, 104, párrafo tercero, 106, 107, 108, 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, del Reglamento Interior del Banco de México, se clasifica como reservada, **información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales**, deberá mantenerse como reservada, por cinco años más, contados a partir de la fecha de vencimiento de plazo reserva actual, toda vez que el Banco Central continuará utilizando la infraestructura tecnológica protegida por la presente prueba de daño para el ejercicio de sus funciones, considerando que los periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones, se extienden a rangos de entre diez y quince años.

REFERENCIA 2

United States Government Accountability Office

GAO

Statement for the Record
To the Subcommittee on Terrorism and
Homeland Security, Committee on the
Judiciary, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Tuesday, November 17, 2009

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues



GAO-10-230T



"2026. Año de Margarita Maza Parada"

REFERENCIA 3

Order Code RL32331

CRS Report for Congress

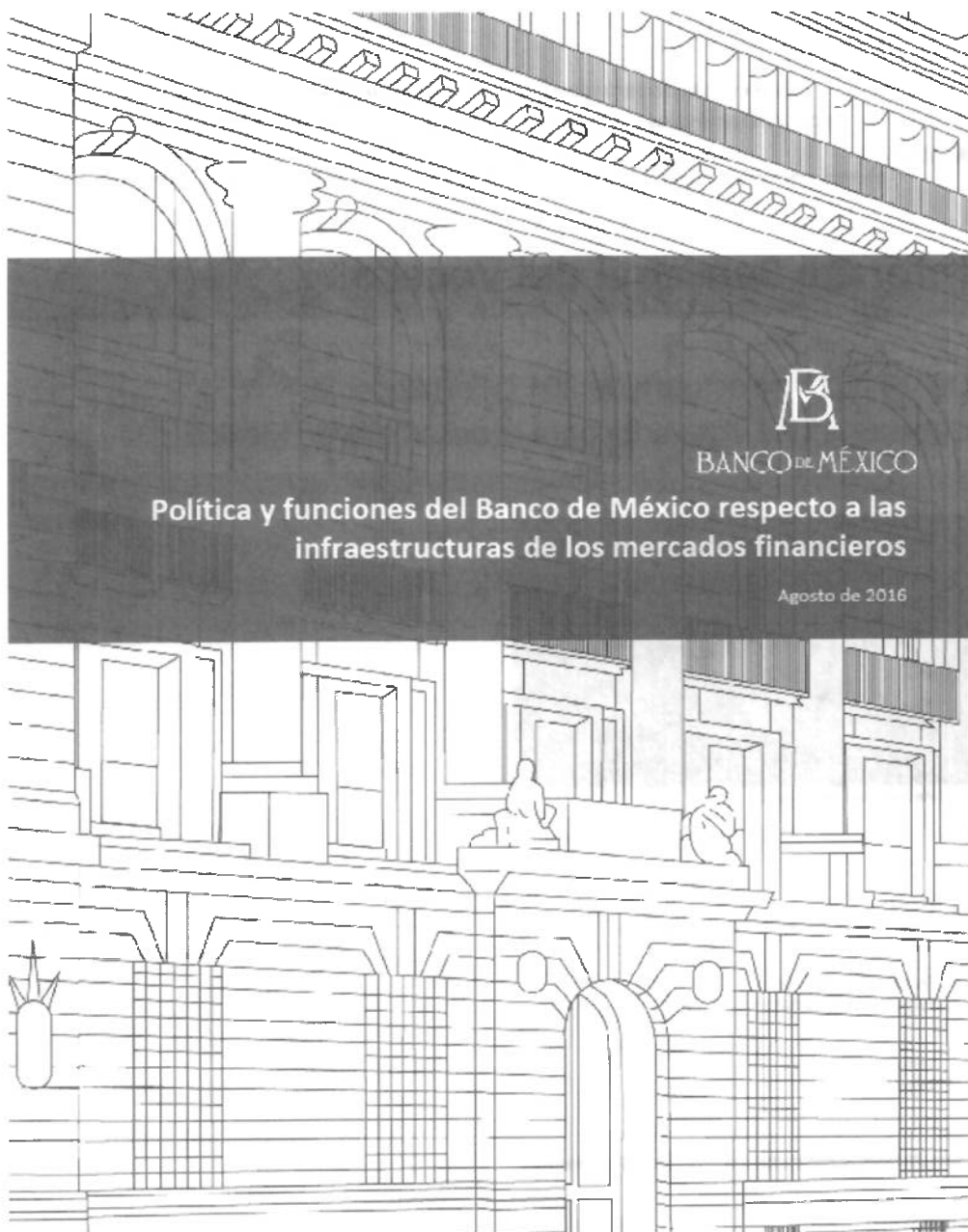
Received through the CRS Web

The Economic Impact of Cyber-Attacks

April 1, 2004

Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel
Government and Finance Division

REFERENCIA 4



REFERENCIA 5

13/5/2018

Informe Semanal del Vocero | Secretaría de Hacienda y Crédito Público | Gobierno | gob.mx

Este contenido será modificado temporalmente en atención a las disposiciones legales y normativas en materia electoral, con motivo del inicio de periodo de campaña

 (<http://>

Informe Semanal del Vocero

Del 23 al 27 de octubre de 2017. Fortalecer la ciberseguridad, relevante para el desarrollo de México.



Informe Semanal del Vocero

Autor
Secretaría de Hacienda y Crédito Público

Fecha de publicación
29 de octubre de 2017

Categoría
Comunicado

<https://www.gob.mx/whop/prensa/informe-semanal-del-vocero-132251?idiom=es>

1/8

REFERENCIA 6

13/6/2018

Several Polish banks hacked, information stolen by unknown attackers — BadCyber

BadCyber

Making infosec journalism great again!

Several Polish banks hacked, information stolen by unknown attackers

badcyber / February 3, 2017 / Crime, Investigation / banking, malware, Poland



241

f Share

🐦 Tweet

<https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/>

1/14

REFERENCIA 7

13/6/2018
BAE Systems Threat Research Blog: Lazarus & Watering-hole attacks
Mas
galliana@gmail.com
Subscribe
Contact Us

BAE SYSTEMS THREAT RESEARCH BLOG
Resources
Contact Us

Home
Products
Solutions
News & Events
Partners
About Us
Careers

THREAT RESEARCH BLOG
BAE SYSTEMS
INSPIRED WORK

Home » Threat Research » Lazarus & Watering-hole attacks

Posted by BAE Systems Applied Intelligence - Sunday, 12 February 2017

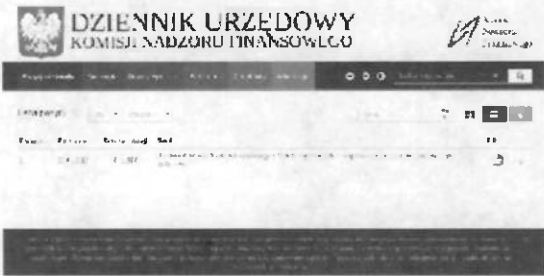
LAZARUS & WATERING-HOLE ATTACKS

On 3rd February 2017, researchers at badcyber.com released an [article](#) that detailed a series of attacks directed at Polish financial institutions. The article is brief, but states that "This is – by far – the most serious information security incident we have seen in Poland" followed by a claim that over 20 commercial banks had been confirmed as victims.

This report provides an outline of the attacks based on what was shared in the article, and our own additional findings.

ANALYSIS

As stated in the [blog](#), the attacks are suspected of originating from the website of the Polish Financial Supervision Authority (knf.gov.pl), shown below:



From at least 2016-10-07 to late January the website code had been modified to cause visitors to download malicious JavaScript files from the following locations:

<http://baesystemsai.blogspot.com/2017/02/lazarus-watering-hole-attacks.html>

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin.

[Sign up](#)

POPULAR POSTS

- TWO STATES IN DISMAY
- KARACHOFF ON RANSOMWARE
- CYBER HEIST ATTEMPTION

CONTACT

For further information or to talk to an expert, please contact us.

icr@baesystems.com

Contact

REFERENCIA 8

ResearchGate

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/317789228>

Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack

Article · World Neurosurgery · June 2017

DOI: 10.1016/j.wneu.2017.06.104

CITATION

1

READS

142

1 author:



Tobias A. Matter

Eastern Maine Medical Center

164 PUBLICATIONS 804 CITATIONS

[SEE PROFILE](#)

All content following this page was uploaded by Tobias A. Matter on 09 October 2017.

The user has requested enhancement of the downloaded file.

REFERENCIA 9

7/2/2018

Acción oportuna de Bancomext salvaguarda intereses de clientes y la institución | Bancomext

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

El Banco Nacional de Comercio Exterior (Bancomext), informa que, a pesar de las robustas medidas de seguridad con que cuenta, el día 9 de enero fue víctima de una afectación en su plataforma de pagos internacionales provocada por un tercero.

Las autoridades han confirmado que el modus operandi de los presuntos "hackers" es similar a intromisiones ocurridas en otras instituciones en México y América Latina.

Afortunadamente, el protocolo y la oportuna reacción de las áreas responsables de la operación, con el apoyo de los bancos, las autoridades correspondientes y el Banco de México, lograron contener este hecho.

Cabe destacar que los intereses de nuestros clientes y los del propio Banco se encuentran a salvo y que Bancomext está reanudando operaciones para sus clientes y contrapartes.

A medida que exista mayor información se hará del conocimiento del público.

Teléfono de Comunicación Social: 15551024

Descarga el comunicado (<http://www.bancomext.com/vwp-content/uploads/2018/01/2 COMUNICADO DE PRENSA BANCOMEXT-180110.pdf>)

REFERENCIA 10

13/6/2018

Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh - Bloomberg

Technology

Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh

By [Michael Riley](#) and [Alan Kretz](#)

26 de mayo de 2016 8:36 GMT-5

Updated on 26 de mayo de 2016 15:21 GMT-5

-
- FireEye said to investigate broad campaign in Southeast Asia
 - No indication in latest disclosures whether money was taken
-



Swift Hack Investigation Expands to Southeast Asia

Investigators are examining possible computer breaches at as many as 12 banks linked to Swift's global payments network that have irregularities similar to those in the theft of \$81 million from the Bangladesh central bank, according to a person familiar with the probe.

REFERENCIA 11

Recuadro 7

RIESGO CIBERNÉTICO: RELEVANCIA Y ENFOQUES PARA SU REGULACIÓN Y SUPERVISIÓN

Felipe Clavijo Ramírez
Daniel Osorio
Eduardo Yanquen*

Durante los últimos años el mundo financiero ha sido testigo del desarrollo vertiginoso de tecnologías innovadoras en el área de los servicios financieros, las cuales han resultado en nuevos modelos de negocio y nuevos procesos o productos. Según el Financial Stability Board (FSB, 2017a), el desarrollo e implementación de estas tecnologías puede llegar a generar múltiples e importantes beneficios para la estabilidad financiera (e. g.: descentralización, diversificación, eficiencia, transparencia y mayor inclusión financiera), pero al mismo tiempo propiciaría la generación de nuevos riesgos. El FSB divide estos riesgos en dos categorías: microfinancieros y macrofinancieros. Dentro de la primera clasificación se incluye el riesgo cibernético, el cual es el tema central del presente recuadro.

1. ¿Qué es el riesgo cibernético y por qué es relevante para la estabilidad financiera?

Según el Instituto de Gestión de Riesgos (Institute of Risk Management), organismo líder a nivel mundial en todo lo que compete a la gestión de los riesgos que enfrentan las empresas, el riesgo cibernético se define como cualquier riesgo de pérdida financiera, afectación o daño de la reputación de una organización derivado de algún tipo de falla de sus sistemas tecnológicos de información. El FSB (2017a) clasifica al cibernético como un riesgo microfinanciero de carácter operativo, debido a que puede surgir de fallas en los sistemas de información, error humano o influencias externas.

La forma más común como se ha materializado el riesgo cibernético en años recientes ha sido mediante lo que se conoce como ataques cibernéticos. En esencia, estos son acciones ilegales realizadas por hackers, con el objetivo principal de obtener cierto beneficio, al generar daños en los sistemas tecnológicos de una organización, dominarlos o robar información contenida en ellos. A raíz del desarrollo de nuevas tecnologías y soluciones digitales, la exposición de las entidades al riesgo cibernético se ha incrementado, debido a que estas innovaciones han expandido el rango y el número de puntos de entrada que los hackers pueden atacar en busca de deficiencias o debilidades en los sistemas.

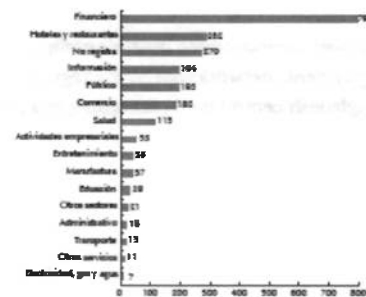
* Los autores pertenecen al Departamento de Estabilidad Financiera del Banco de México. Sus opiniones no comprometen al Banco de México ni a su Junta Directiva. Los errores u omisiones que persistan son responsabilidad exclusiva de los autores.

De acuerdo con el Fondo Monetario Internacional (FMI, 2017), existen dos tipos de costos asociados a los ataques cibernéticos. Por un lado, están los costos directos, que incluyen investigaciones forenses, asesoría legal, notificaciones al cliente, protección y seguridad al consumidor, y medidas postataque para mitigar sus efectos. Por otro lado, se encuentran los costos indirectos, los cuales son menos visibles, con efectos de más largo plazo y más difíciles de cuantificar ante. En esta categoría se encuentran los efectos adversos sobre la marca de la institución afectada (riesgo reputacional), la depreciación del valor de la propiedad intelectual, mayores gastos operacionales para prevenir futuros ataques y el impacto sobre las primas que paga el afectado para asegurarse contra futuros eventos. Según el FMI (2017), el 90% de los costos derivados de incidentes cibernéticos es atribuible a factores indirectos.

En el ámbito internacional se ha podido evidenciar que, en los últimos años, los ataques cibernéticos se han intensificado contra las infraestructuras financieras. Esto es preocupante debido a que estos ataques tienen el potencial de propagarse y ser sistémicos. De acuerdo con una encuesta realizada por Verizon (2016), la industria financiera fue la más afectada en 2015 por este tipo de incidentes (Gráfico R7.1).

Algunos ejemplos recientes que han prendido las alarmas en la industria financiera sobre los efectos de los ataques cibernéticos, debido a la importancia de las instituciones afectadas y la magnitud de las pérdidas incurridas, sucedieron en Rusia, Bangladesh y Ecuador. En septiembre de 2014 hackers lograron acceder al sistema electrónico de negociación de

Gráfico R7.1
Número de ataques cibernéticos en 2015 con pérdida confirmada de información, por sector económico

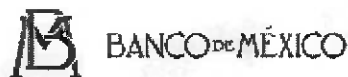


Fuente: Verizon (2016).

REFERENCIA 12



REFERENCIA 13



22 de mayo de 2018

Puntos Importantes sobre la Situación Actual del SPEI.

1. Se tienen registrados 5 participantes con vulneraciones de ciberseguridad. Todos los ataques que se han observado han sido dirigidos hacia los bancos, casas de bolsa y otros participantes del sistema de pagos. Estos han estado enfocados en los sistemas de los participantes con los que se conectan al SPEI.
2. El sistema central del SPEI, que opera el Banco de México, no se ha visto afectado y no ha sido blanco de ningún ataque. El sistema central opera de manera segura y eficiente como lo ha hecho desde su creación.
3. Los recursos de los clientes de instituciones financieras están seguros, no estuvieron en peligro y no han sido el objetivo de los ataques. Los recursos que se han extraído han sido de los participantes (bancos, casas de bolsa, etc.). Los atacantes han buscado vulnerar las conexiones de las instituciones con el SPEI, inyectando instrucciones de pago fraudulentas a partir de cuentas inexistentes, lo cual afecta la cuenta transaccional de los participantes en el SPEI, pero no las cuentas de los clientes finales. Los recursos de los clientes están seguros porque radican en un sistema separado con validaciones individuales por operación.
4. Para salvaguardar la continuidad operativa, el Banco de México alertó a los participantes en el SPEI y solicitó a los participantes con un mayor perfil de riesgo migrar la operación a una plataforma contingente. Este esquema de operación contingente y las validaciones adicionales que han implementado los participantes han propiciado la ralentización de los flujos de pagos.
5. Una vez recibidas en el SPEI, el 100% de las operaciones son procesadas y enviadas a los participantes receptores en segundos. Por otra parte, desde que se recibe la solicitud por parte de un cliente en los sistemas del participante hasta el abono final el 55% de las operaciones fluye por el sistema y los participantes con normalidad en cuestión de segundos, mientras que el 99% se opera en menos de dos horas. No obstante, en algunos casos estas acreditaciones pueden tardar uno o más días. El Banco de México, consciente de la preocupación y malestar de los clientes, trabaja arduamente para que los participantes agilicen sus procesos para abonar en el menor tiempo posible los recursos de sus clientes y con ello minimizar la afectación a los mismos.
6. Con la información disponible, los montos involucrados en envíos irregulares y sujetos a revisión son de aproximadamente 300 millones de pesos.

REFERENCIA 14



REFERENCIA 15

 EL FINANCIEROEconomía Mercados Nacional Opinión Televisión
Economía, Mercados y Propósitos en alianza con Bloomberg

Síguenos     

Empresas

¿Tuviste problemas con Coppel? Admite que hackeo en 1,800 tiendas limitó sus operaciones por 3 meses

Coppel admitió que un hackeo limitó al menos 9 mil 500 servicios de negocio por 3 meses y afectó las operaciones de las mil 800 tiendas que tiene la empresa en todo el país.

Por Christopher Calderón

septiembre 05, 2024 | 16:28 hrs

REFERENCIA 16



The screenshot shows the homepage of the Instituto Nacional de Ciberseguridad (INCIBE). The header includes the INCIBE and INCIBE-CERT logos, and a navigation menu with links to INCIBE, INCIBE-CERT, CIUDADANÍA, MENORES, EMPRESAS, EVENTOS, and ESPAÑA DIGITAL 2026. Below the header, there is a secondary navigation bar with links to Alerta temprana, Blog, Publicaciones (highlighted), Incidentes, Servicios, Sectores Estratégicos, and Sobre INCIBE-CERT. The main content area features a large headline: "Fallo de seguridad en la IA de selección de McDonald's expone datos de millones de solicitantes". Below the headline, it states "Fecha de publicación 19/08/2025".

Fallo de seguridad en la IA de selección de McDonald's expone datos de millones de solicitantes

Fecha de publicación 19/08/2025

"2026. Año de Margarita Maza Parada"

REFERENCIA 17



60 SAN ANTONIO LOCAL EL TIEMPO INMIGRACIÓN AL DÍA VIDEOS ENTRETENIMIENTO DEPORTES 79° Noticias 24/7

TENDENCIAS Inmigración y sus derechos La Casa de los Famosos Telemundo 60 Responde Norma el Atletista de la Semana Crimen en San Ant...

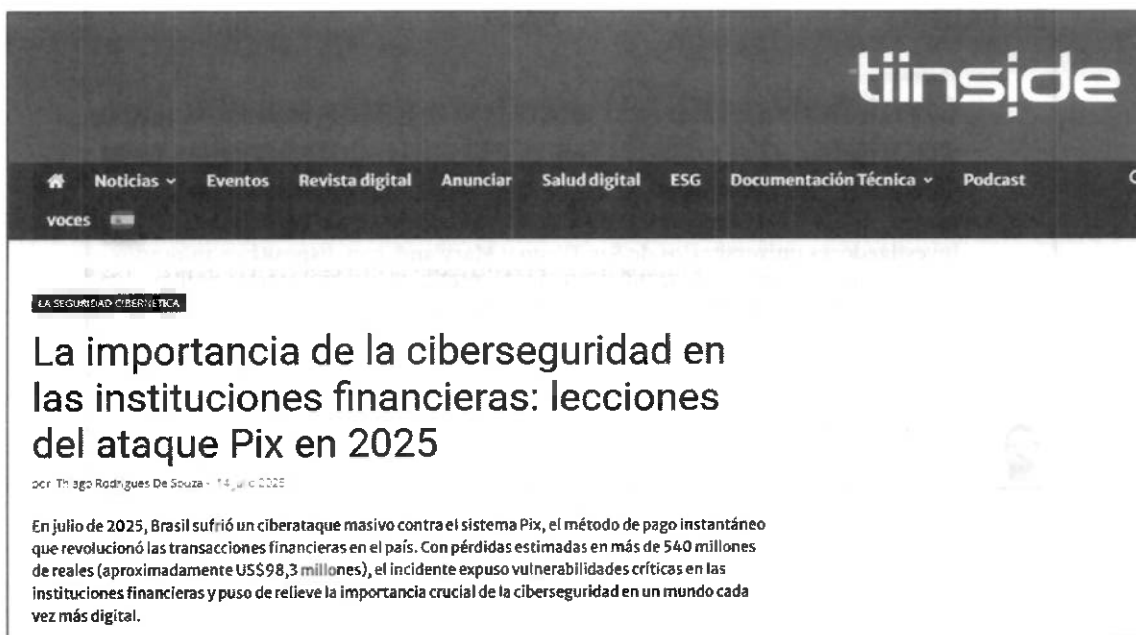
ESTADOS UNIDOS

Un ciberataque a UNFI provoca escasez en Whole Foods; afecta todo el país

Un importante distribuidor de alimentos naturales, United Natural Foods Inc., afirma haber sido afectado la semana pasada por un ciberataque.

Por Kevin Collier, NBC News • Publicado el 12 de junio del 2025 •
Actualizado a las 7:11 pm del 12 de junio del 2025

REFERENCIA 18



REFERENCIA 19

EL PAÍS 50 México

CIBERSEGURIDAD >

Científicos en EE UU acceden a datos sensibles sin encriptar del Gobierno mexicano con apenas una antena parabólica y una tarjeta de televisión

Investigadores universitarios de San Diego y Maryland, con dispositivos valorados en 650 dólares, logran captar información de inteligencia o inventarios militares de la Guardia Nacional, CFE, Telmex y el Banco Santander

 **ANDRÉS RODRÍGUEZ**
México - 16 OCT 2025 - 03:30 | Actualizado: 16 OCT 2025 - 08:01 CST

Los errores y la fuga de datos personales manchan el primer intento masivo de registrar los celulares mexicanos

La meta de registrar más de un millón de líneas móviles al día ha sido cuestionada por fuga de datos y registros falsos en las plataformas de las operadoras móviles

**DARINKA RODRÍGUEZ**

México · 18 ENE 2026 · 22:50 CST

Hugo Navarro tardó tres días para poder realizar el registro de su línea celular con su nombre y su CURP, tal y [como lo ha ordenado el Gobierno de México](#). "No la pude hacer en una oficina de Telcel en San Luis Potosí y la aplicación no alcanzaba a guardar mis datos biométricos en tiempo y se botaba el proceso, fue hasta después que ya pude hacerlo", comenta este trabajador de 30 años, en consulta. Esta misma semana, Claudia Macedo decidió posponer el registro de su línea telefónica. "No hay seguridad para nuestros datos, yo me esperaré hasta que vea mayor certeza", admite.

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DEL PERIODO DE RESERVA

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

RESULTANDO

- I. Que, con la finalidad de cumplir con las obligaciones de transparencia comunes, los sujetos obligados pondrán a disposición del público, en sus respectivos medios electrónicos y en la Plataforma Nacional de Transparencia, de acuerdo con sus facultades, atribuciones, funciones u objeto social, la información de los temas, documentos y políticas que se señalan en el artículo 65 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).
- II. Que, del análisis realizado a la información que en su momento fue clasificada como reservada, se han puesto a consideración de este Órgano Colegiado los motivos y fundamentos para ampliar el periodo de reserva próximo a concluir.
- III. Que, considerando lo anterior, se solicitó al Comité de Transparencia aprobar la ampliación del plazo de reserva de la información, como se indica enseguida:

FECHA O REFERENCIA DEL OFICIO	UNIDAD(ES) ADMINISTRATIVA(S) SOLICITANTE(S) Y NOMBRE(S) DE SU(S) TITULAR(ES)	SOLICITUD DEL OFICIO	INFORMACIÓN CLASIFICADA	PLAZO DE CLASIFICACIÓN
Oficio de fecha 29 de junio de 2026.	Joaquín Rodrigo Cano Jauregui Segura Millan (Dirección de Apoyo a las Operaciones), 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. <i>"Información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias, como agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales."</i>	Plazo de reserva inicial: 5 años, a partir del 30 de septiembre de 2021. Plazo de reserva con ampliación: 5 años, a partir del 01 de octubre de 2026.

CONSIDERANDO

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

SEGUNDO. Este Comité de Transparencia, tomando en cuenta que en términos de los artículos 102, párrafo tercero, y 106, párrafo segundo, de la LGTAIP, corresponde a las personas titulares de las áreas de los sujetos obligados clasificar la información, advierte que las razones, motivos y circunstancias especiales que llevaron a concluir que en el caso particular se actualiza la necesidad de **ampliar el periodo de reserva** de la información señalada, se contienen en el oficio referido en el resultando III, así como en la prueba de daño correspondiente, los cuales se tienen aquí por reproducidos como si a la letra se insertasen¹.

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

En consecuencia, y considerando que, conforme a lo manifestado en la prueba de daño respectiva, la divulgación de la información correspondiente: *"(...) representa un riesgo de perjuicio significativo al interés público ya que revelar información referente al software que soporta la implementación de las operaciones monetarias, cambiarias y como agente financiero que este Instituto Central lleva a cabo por cuenta propia o a nombre del gobierno federal, así como aquellas relacionadas con la gestión de las reservas internacionales, pone en riesgo de destrucción, inhabilitación o sabotaje, infraestructura de tal importancia para la economía mexicana que si destrucción o incapacidad tendría un impacto negativo en la efectividad de las medidas adoptadas en los sistemas financiero, económico, cambiario monetario del país, poniendo en riesgo el funcionamiento o, en su caso, de la economía nacional en su conjunto o, bien pueda incrementar el costo de las operaciones financieras que realicen los sujetos obligados del sector público federal (...)"*, **este Comité de Transparencia aprueba la ampliación al periodo de reserva de la información señalada** de conformidad con lo expresado en el oficio citado en el resultando III de la presente determinación, así como en términos de la prueba de daño correspondiente, **y toma conocimiento del nuevo plazo de reserva determinado por la unidad administrativa.**

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

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 explicita, pues resulta obvio que al fundarse en la tesis recoge los diversos argumentos contenidos en ella."* (Suprema Corte de Justicia de la Nación; Registro digital: 192898; Instancia: Pleno; Novena Época; Materias(s): Común; Tesis: P./J. 126/99; Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo X, Noviembre de 1999, página 35; Tipo: Jurisprudencia).

RESUELVE

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

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en la sesión celebrada el 24 de septiembre de 2026. -----

COMITÉ DE TRANSPARENCIA**CLAUDIA TAPIA RANGEL****Integrante**

Unidad de Transparencia

EDGAR MIGUEL SALAS ORTEGA**Integrante**

Dirección Jurídica

VÍCTOR MANUEL DE LA LUZ PUEBLA**Integrante**Dirección de Seguridad y Organización de la
InformaciónLAMO
ASTH

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
25/09/2026 19:38:26	EDGAR MIGUEL SALAS ORTEGA	588691079e695f84df69b97b89c34bba53305e60dc1d19375f34d0f41ea752e5
25/09/2026 19:41:30	VICTOR MANUEL DE LA LUZ PUEBLA	7ecdca3728ec0b1076c0af77f1d5e2446a26c745e127cd1c51c51f71691ec0f
28/09/2026 10:27:45	Claudia Tapia Rangel	538b913a6bfbe3eed9ecb60878e58650b1cba37e54231ba1d337f7758e54659f