COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ESPECIAL 19/2026
DEL 02 DE JULIO DE 2026

A las trece horas con treinta minutos del 02 de julio 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 (LGPDPPSO); 4o. del Reglamento Interior del Banco de México (RIBM); así como con la Quinta y Sexta de las Reglas. Por lo anterior, se procedió en los términos siguientes: ----------

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

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

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

PRIMERO. VERSIÓN PÚBLICA ELABORADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE SEGURIDAD 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 23 de junio de 2026, suscrito por quien es titular de la Dirección de Seguridad 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 la carátula y en la prueba de daño correspondiente, y solicitó a este Comité de Transparencia confirmar la clasificación referida.

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

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

SEGUNDO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE SEGURIDAD 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 22 de junio de 2026, suscrito por quien es titular de la Dirección de Seguridad del Banco de México, el cual se agrega a la presente Acta, como **"ANEXO 4"**, por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de ampliar el periodo de reserva de la información referida en dicho

oficio, de conformidad con la fundamentación y motivación señaladas en el mismo, así como en la prueba de daño correspondiente, y solicitó a este Órgano Colegiado aprobar la ampliación del periodo de reserva.----------

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

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

TERCERO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE 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 14 de abril 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 señaladas en el mismo, así como en la prueba de daño correspondiente, y solicitó a este Órgano Colegiado aprobar la ampliación del periodo de reserva.----------

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

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

CUARTO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA GERENCIA DE OPERACIONES INTERNACIONALES, EN SUPLENCIA POR AUSENCIA DE QUIEN ES TITULAR DE LA DIRECCIÓN DE OPERACIONES INTERNACIONALES 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 14 de abril de 2026, suscrito por quien es titular de la Gerencia de Operaciones Internacionales, en suplencia por ausencia de quien es titular de la Dirección de Operaciones Internacionales del Banco de México, el cual se agrega a la presente Acta, como **"ANEXO 8"**, por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de ampliar el periodo de reserva de la información referida en dicho oficio, de conformidad con la fundamentación y motivación señaladas en el mismo, así como en la prueba de daño correspondiente, y solicitó a este Órgano Colegiado aprobar la ampliación del periodo de reserva.----------

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

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

QUINTO. VERSIONES PÚBLICAS ELABORADAS POR QUIENES SON TITULARES DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN; DE LA DIRECCIÓN DE DESARROLLO DE SISTEMAS; ASÍ COMO DE LA GERENCIA DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA SUBGERENCIA DEL CENTRO DE DEFENSA DE CIBERSEGURIDAD, ÉSTAS ÚLTIMAS, UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE SEGURIDAD Y ORGANIZACIÓN DE LA

INFORMACIÓN, TODAS 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 23 de junio de 2026, suscrito por quienes son titulares de la Dirección de Infraestructura de Tecnologías de la Información; de la Dirección de Desarrollo de Sistemas; así como de la Gerencia de Seguridad de Tecnologías de la Información y de la Subgerencia del Centro de Defensa de Ciberseguridad, éstas últimas, unidades administrativas adscritas a la Dirección de Seguridad y Organización de la Información, todas del Banco de México, el cual se agrega a la presente Acta como **"ANEXO 10"**, 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 en la prueba de daño correspondiente, 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 con la Quinta de las Reglas, resolvió confirmar la clasificación de la información referida en términos de la resolución que se agrega al apéndice de la presente Acta como **"ANEXO 11"**. ----------

Al no haber más asuntos que tratar, se da por terminada la sesión a las trece horas con cuarenta y cinco minutos de la misma fecha de su celebración, y en términos de la Quinta de las Reglas, quien ejerce las funciones de Secretariado en este acto, hace constar el voto de los integrantes del Comité de Transparencia que participaron en la misma a través de medios electrónicos de comunicación, la cual se llevó a cabo en tiempo real, y quienes integraron el quórum no la abandonaron durante su desarrollo. La presente Acta se firma por los integrantes del Comité de Transparencia que participaron en la sesión, así como por quien ejerce en este acto las funciones de Secretariado. Conste.----------

COMITÉ DE TRANSPARENCIA

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

PAJC
ASTH
LAMO
MDF

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
03/07/2026 15:52:20	Claudia Tapia Rangel	2bf0dc95aa900b7af83cc32da092cdf9dab87c36e881c3b45088297b7c9272dc
03/07/2026 15:58:57	EDGAR MIGUEL SALAS ORTEGA	90fd305c502eca915f829a058fb5605e37c7336f9354f2cdd36dab4f0d3e1bc5
03/07/2026 17:37:00	SERGIO ZAMBRANO HERRERA	0286e98f36690a094cf849349dd89770f3ea40d9519c65ccc8acbc925ba6fbe7
03/07/2026 19:57:15	VICTOR MANUEL DE LA LUZ PUEBLA	4abe22faca8969c46a06861bec98f1a6137aa9959e4c9780facd2395dd692c96

"ANEXO 1"

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

COMITÉ DE TRANSPARENCIA

ORDEN DEL DÍA

ACTA DE LA SESIÓN ESPECIAL 19/2026
DEL 02 DE JULIO DE 2026

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

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

CUARTO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA GERENCIA DE OPERACIONES INTERNACIONALES, EN SUPLENCIA POR AUSENCIA DE QUIEN ES TITULAR DE LA DIRECCIÓN DE OPERACIONES INTERNACIONALES DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL TÍTULO QUINTO DE LA LGTAIP.

QUINTO. VERSIONES PÚBLICAS ELABORADAS POR QUIENES SON TITULARES DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN; DE LA DIRECCIÓN DE DESARROLLO DE SISTEMAS; ASÍ COMO DE LA GERENCIA DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA SUBGERENCIA DEL CENTRO DE DEFENSA DE CIBERSEGURIDAD, ÉSTAS ÚLTIMAS, UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN DE SEGURIDAD Y ORGANIZACIÓN DE LA INFORMACIÓN, TODAS DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 65 DE LA LGTAIP.

"ANEXO 2"

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

Ciudad de México, 23 de junio de 2026.

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

Me refiero a la obligación prevista en el artículo 56, párrafo primero, 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 el documento que se indica en el cuadro siguiente, de conformidad con la fundamentación y motivación señaladas en la carátula y en la prueba de daño correspondiente.

TÍTULO DEL DOCUMENTO CLASIFICADO	TIPO DE CLASIFICACIÓN
800-24-0353-1 CONV (Convenio modificatorio para adquisición de sistema de detección de intrusión en piso)	**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 al documento referido es el adscrito a:

Dirección de Recursos Materiales (Director), Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (toda la Gerencia), Gerencia de Abastecimiento a Emisión y Recursos Humanos (toda la Gerencia), Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (toda la Gerencia), Dirección de Infraestructura de Tecnologías de la Información (Director), Gerencia de Telecomunicaciones (Gerente), Subgerencia de Desarrollo de Servicios de Telecomunicaciones (todo el personal), Subgerencia de Administración de Sistemas Electrónicos

(todo el personal), Subgerencia de Planeación y Regulación (todo el personal), Dirección de Seguridad (Director), Gerencia de Prevención y Planeación de Seguridad (Gerente), Gerencia de Protección y Traslado de Valores (Gerente), Subgerencia de Resguardo y Traslado de Valores Ciudad de México (Subgerente y Analista), Subgerencia de Resguardo y Traslado de Valores Jalisco (Subgerente y Analista), Subgerencia de Protección (Subgerente y Analista), Subgerencia de Planeación, Formación y Evaluación en Seguridad (Subgerente).

Atentamente

_____

GONZALO MARAÑÓN VILLEGAS
Director de Seguridad

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
24/06/2026 12:50:43	Gonzalo Mara□ □n Villegas	a45db6505a936260aff30200ac36799d5d15cc8e4207aeb8ef2dca999fddd2d8

"ANEXO 3"

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

OBLIGACIONES DE TRANSPARENCIA

Unidad Administrativa: Dirección de Seguridad 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 23 de junio de 2026.	Gonzalo Marañón Villegas (Dirección de Seguridad del Banco de México).	Confirmación de clasificación de información.	**Información reservada** en términos de lo señalado en el oficio y en la prueba de daño correspondiente. "*Marcas, modelos, características, y proveedor de los equipos o sistemas que se utilizan en el Banco de México*"	1 versión pública señalada en el oficio correspondiente.	**Información reservada:** 5 años, a partir de la presente resolución (vencimiento: 02 de julio 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, que se contiene en el oficio referido en el resultando II, así como en la carátula y en la prueba de daño correspondiente, los cuales se tienen aquí por reproducidos como si a la letra se insertasen[1].

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

En consecuencia, y considerando que conforme a lo manifestado en la prueba de daño respectiva, la divulgación de la información "*(…) representa un riesgo de perjuicio significativo al interés público, compromete la seguridad nacional, la seguridad en la provisión de moneda nacional al país, pone en riesgo la vida, seguridad y salud de personas físicas (…)"*, **este Comité de Transparencia confirma la clasificación de la información señalada como reservada**, de conformidad con lo expresado en el oficio referido en el resultando II de la presente resolución, así como en la carátula 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 referida como reservada, 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 la carátula y en la prueba de daño correspondiente, en términos del considerando Segundo de la presente resolución.

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

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en la sesión celebrada el 02 de julio 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

PAJC
LAMO
MDF

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
03/07/2026 15:52:23	Claudia Tapia Rangel	dfb8669217b1c3d775fb25a94461923ec50c8d84241f87830d3afc8619913dba
03/07/2026 15:58:53	EDGAR MIGUEL SALAS ORTEGA	13fac37dedc0b49d1baa4b9c5e696e459500dfcc09b95a20e83376c567be0ad4
03/07/2026 19:57:07	VICTOR MANUEL DE LA LUZ PUEBLA	0eece0477df13948c066977a48826c4545705491443 77e57b97af975828d2969

"ANEXO 4"

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

Ciudad de México, 22 de junio de 2026

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

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

TÍTULO DEL DOCUMENTO CLASIFICADO
Contrato de adquisición de equipo de protección personal para personal operativo de seguridad. (DRM_0000028226)
Contrato de adquisición de equipo de protección personal para personal operativo de seguridad. (DRM_0000028212)

Al respecto, me permito resaltar que dicha clasificación fue confirmada por ese Comité mediante resolución de 28 de octubre de 2021, emitida en la Sesión Especial 37/2021, en términos de la fundamentación y motivación expresadas en el oficio de fecha 21 de octubre 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 28 de octubre de 2021, a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el 28 de octubre 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, 28 Bis, del Reglamento Interior del Banco de México (RIBM); así como Segundo, fracción VIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, me permito informarles que esta unidad administrativa **estima que las causas para mantener clasificada como reservada la información referida en el presente oficio subsisten a la fecha, y lo seguirán al menos por los próximos 5 años, contados a partir de la citada fecha de expiración del plazo de reserva,** referida en el párrafo precedente.

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

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

PERSONAL CON ATRIBUCIONES DE ACCESO AL DOCUMENTO CLASIFICADO
• 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). • Dirección de Seguridad (Director). • Gerencia de Protección y Traslado de Valores (Gerente). • Subgerencia de Resguardo y Traslado de Valores Ciudad de México (todo el personal). • Subgerencia de Protección (Subgerente).

Atentamente

GONZALO MARAÑÓN VILLEGAS
Director de Seguridad

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
22/06/2026 17:58:12	Gonzalo Mara□ □n Villegas	0fb0ff0bc1c36a6da9f434a14dc6fa8e007389c0d099879ff384b39867d4239a

"ANEXO 5"

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

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 22 de junio de 2026.	Gonzalo Marañón Villegas (Dirección de Seguridad 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. *"**Nivel de blindaje de equipos de seguridad del Banco de México**."*	**Plazo de reserva inicial:** 5 años, a partir del 28 de octubre de 2021. **Plazo de reserva con ampliación:** 5 años, a partir del 29 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 insertasen[1].

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

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

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

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

RESUELVE

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

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en la sesión celebrada el 02 de julio 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
NMDS
MDF

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

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
03/07/2026 15:52:24	Claudia Tapia Rangel	11c5a06f433b966f448561a5ea30b10fd3a8ad31ce311554ec43b12d55dc3967
03/07/2026 15:58:56	EDGAR MIGUEL SALAS ORTEGA	48e420e1d0663b942d2ca69b27320a52c5fa6320b60f5143831c53794118c565
03/07/2026 19:57:11	VICTOR MANUEL DE LA LUZ PUEBLA	9cca8862ac73df7e87625b56949e1058976056e028f4f22e70b698f5e703fa59

"ANEXO 6"

BANCO DE MÉXICO®
RECIBIDO
14 ABR 2026
Comité de Transparencia
Por: JIS393 Hora: 12:00

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

Ciudad de México, 14 de abril 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 señalan en el siguiente cuadro:

TÍTULO DEL DOCUMENTO CLASIFICADO
Autorización para adjudicar directamente por monto identificado con ID PAC 21-0799.
General Terms and Conditions. 1 December 2020

Al respecto, me permito resaltar que dicha clasificación fue confirmada por ese Comité mediante resolución de 15 de julio de 2021, emitida en la sesión Especial 23/2021, en términos de la fundamentación y motivación expresadas en el oficio de 09 de julio 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 15 de julio de 2021 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **15 de julio 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**

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 General de Operaciones y Banca Central:

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

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

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

Por parte de la Dirección de Recursos Materiales:

- Director 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)

Por parte de Unidad de Auditoría (todo el personal)
Por parte de la Dirección de Control Interno (todo el personal)

Atentamente

JOAQUÍN RODRIGO CANO JAUREGUI SEGURA MILLAN
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.

Por lo que 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,*** se clasifica 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 su destrucción o incapacidad tendría un impacto negativo en la efectividad de las medidas adoptadas en los sistemas financiero, económico, cambiario o monetaria del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto, o bien pueda incrementar el costo de 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 la infraestructura informática que soporta las operaciones cambiarias, monetaria y de agente financiero que realiza la banca central, lo**

cual posibilita la ejecución de acciones hostiles en contra de las tecnologías de la información de este Instituto Central, así como de las infraestructuras que éste administra, opera y supervisa, lo cual, podría menoscabar la efectividad de las mismas a tal grado, que su destrucción o inhabilitación afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero, económico y cambiario del país, arriesgando el funcionamiento de dichos 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 sus funciones de banca central. Las anteriores son finalidades y funciones que dependen en gran medida de la correcta operación de las tecnologías de la información y comunicaciones 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 cambiaria[1], 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.

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 propia 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

[1] Las políticas en materia cambiaria son decisión de la Comisión de Cambios.

todos sus recursos a ataques concretos 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.

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 necesarios 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 las infraestructuras que soportan las operaciones monetarias, ***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***, 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 éstas infraestructuras.

---

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

2. **Demostrable, ya que es un hecho notorio que los sistemas de los Bancos Centrales han sufrido ataques cibernéticos a través de estas infraestructuras**, como SWIFT, la cual ha sido utilizada para realizar robos de capital, uno de estos casos es el del Banco Central de Bangladesh, que sufrió un robo de 81 millones de dólares. 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. Respecto de lo anterior, a la fecha SWIFT continúa siendo objeto de ataques por diferentes grupos de delincuentes informáticos, y expertos en seguridad informática consideran que este tipo de actividades es susceptible de expandirse a otros servicios y sistemas financieros. Asimismo, los sistemas de empresas como Google, Facebook, PayPal y el New York Times se han visto comprometidos por ataques cibernéticos. 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. Esta serie de ataques se encuentra en una fase avanzada, que comenzó con ensayos desde 2017 y que ha logrado la consecución de sus objetivos en algunos casos. En todos ellos, la detección de vulnerabilidades a nivel aplicativo y sistema operativo son elementos en común, por lo cual es totalmente demostrable que el entregar información precisamente sobre las vulnerabilidades de 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, permitiría a los delincuentes o grupos delictivos el llevar a cabo más ciberataques que pudieran dañar de forma más severa las plataformas a través de las cuales se instrumentan las políticas monetaria y cambiaria, y las actividades de agente financiero del gobierno federal.

   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 polacos[3], el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada;[4]

   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;[5]

---

[3] 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 14 de abril de 2026.

[4] 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 14 de abril de 2026.

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

iii) La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público;

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

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.[7] 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.[8] El ataque producido a las plataformas que son usadas por proveedores externos en algunos bancos en México, en relación con el SPEI, ha sido catalogado como similar al que ocurrió con el sistema de pagos internacional S.W.I.F.T. en Rusia;

vi) La filtración a través de redes sociales de la base de datos de tarjetas de los clientes del Banco de Chile dada a conocer por el grupo de hackers llamado "TheShadowBrokers";

vii) La introducción a la red interna de Pemex de un ransomware el pasado 10 de noviembre de 2019, que forzó a la compañía a apagar equipos de cómputo de sus empleados en todo el país, inhabilitando, entre otros, el sistema de pagos de la empresa;[9]

viii) El Ataque al Sistema de Salud el 27 de mayo del 2020 que tuvo afectación en el sitio web de adquisiciones por un grupo de hackers;[10]

---

6 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 14 de abril de 2026.

7 Banco de México. "Información sobre los ataques a los Participantes del SPEI". Mayo 2018 https://www.banxico.org.mx/spei/d/%7BFFC53F5A-CA04-3098-E8F6-B0F17E533183%7D.pdf consultado el 14 de abril de 2026.

8 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/%7BB806F1E8-686D-B9F1-0452-EC375543C801%7D.pdf consultado el 14 de abril de 2026.

9 Excélsior, Hackers piden cinco millones de dólares a Pemex en ciberataque, 12 de noviembre de 2019. https://www.excelsior.com.mx/nacional/hackers-piden-cinco-millones-de-dolares-a-pemex-en-ciberataque/1347377 consultado el 14 de abril de 2026.

10 Latinus, "Hackean página web de adquisiciones de la Secretaria de Salud" 27 de mayo de 2020 https://latinus.us/2020/05/27/hackean-pagina-web-de-adquisiciones-secretaria-de-salud/ consultado el 14 de abril de 2026.

ix) Los ataques ocurridos a la aplicación de conferencias Zoom utilizada durante la pandemia de coronavirus cuyas reuniones han sido pirateadas;[11]

x) El hackeo al banco estatal chileno BancoEstado. La institución detecto un software malicioso en sus sistemas que afecto unos 12,000 equipos, incapacitando la operación obligando al cierre de sucursales, y[12]

xi) El hackeo a 110 computadoras de la Secretaría de Infraestructura, Comunicaciones y Transportes el pasado 24 de octubre con un virus tipo ransomware provocó que esa institución suspendiera la expedición de licencias federales y certificados en las diversas modalidades de transporte y de aviación civil hasta fines de 2022.[13]

En particular, respecto del sistema financiero mexicano, los ataques han sido focalizados a las tecnologías de la información de las instituciones pertenecientes al mismo y se han incrementado desde 2019. Destaca en el reporte sobre Principales incidentes cibernéticos relevantes ocurridos en 2022 en el sistema financiero nacional que han sido reportados al Banco de México la difusión no autorizada de información crediticia de clientes de una sociedad de información creditia.[14] Dicha situación demuestra la realidad e identificación del riesgo que representan los ataques cibernéticos en el sistema financiero mexicano, por lo que los programas que utiliza el Banco de México para interactuar con el mismo están en alto riesgo de ataques y deben reservarse los datos que, de difundirse, pudieran actualizar una vulneración.

Al respecto, 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,

---

11 Excélsior "FBI investiga a "Zoom" por hackeo durante videocoferencias" 31 de marzo del 2020 https://www.excelsior.com.mx/hacker/fbi-investiga-a-zoom-por-hackeo-durante-videoconferencias/1373244 consultado el 14 de abril de 2026.

12 El economista, Banco estatal chileno cierra sucursales por ataque cibernético, 07 septiembre 2020 https://www.eleconomista.com.mx/sectorfinanciero/Banco-estatal-chileno-cierra-sucursales-por-ataque-cibernetico--20200907-0122.html Consultado el 14 de abril de 2026.

13 Forbes, "Alcanza a 110 computadoras hackeo en la SICT; prevén resolverlo en 2 semanas", Emmanuel Carrillo, octubre 25, 2022 @ 7:14 pm, https://www.forbes.com.mx/alcanza-a-110-computadoras-hackeo-en-la-sict-preven-resolverlo-en-2-semanas/ y "SICT frena todos sus trámites hasta fin de año por el hackeo sufrido", Forbes Staff, noviembre 1, 2022 @ 9:01 pm, https://www.forbes.com.mx/sict-frena-todos-sus-tramites-hasta-fin-de-ano-por-el-hackeo-sufrido/ ambos consultados el 14 de abril de 2026.

14 El Banco de México publica un reporte anual acerca de los principales incidentes cibernéticos ocurridos en el sistema financiero nacional a través de la liga: https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html. Para más detalles, véase El Heraldo de México "Hackean al Buró de Crédito: descubren venta de la información de los clientes en redes sociales" Morales, Luz Elena, 2 de febrero de 2023 (disponible a través de la liga: https://heraldodemexico.com.mx/nacional/2023/2/2/hackean-al-buro-de-credito-descubren-venta-de-la-informacion-de-los-clientes-en-redes-sociales-478457.html). Ambos consultados el 14 de abril de 2026.

con el único objeto de conocer las vulnerabilidades de las instituciones, empresas, sistemas e infraestructura de tecnologías de la información.[15]

Por otro lado, es de destacar que los cibercriminales han utilizado técnicas de ingeniería social para obtener información y con ello acceder o vulnerar incluso los sistemas más seguros. Una de las formas más comunes de vulnerar los sistemas es mediante la obtención de información a través de diversas fuentes y mecanismos que les permita diseñar ataques informáticos encaminados a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros elementos, con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes. Al respecto, un análisis de la empresa ESET encontró que en 2020 se duplicaron las detecciones de ataques de ingeniería social en Latinoamérica donde Perú, Brasil y México como los países que registraron la mayor cantidad de detecciones de ataques. México tuvo el 16.94% de los ataques cibernéticos que recibió América Latina en el 2020, lo que coloca al país en el tercer sitio regional. Perú fue el país que registró el mayor porcentaje, con poco más del 31%, seguido por Brasil con más del 18%.[16]

Por lo anterior, **los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de componentes, arquitectura o configuración 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 su objetivo prioritario y 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 durante 2024, nuestros registros indican un promedio de 2,618 intentos de ataque al mes, llegando a presentarse hasta 10.464 intentos de ataques en el año. Si bien dichos ataques

---

[15] El Financiero, *El sistema financiero mexicano fue víctima de una campaña de ciberataques*, 15 de mayo de 2018. https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html Consultado el 14 de abril de 2026.

[16] El Universal, *México ocupa el tercer sitio en la región por ciberataques,* 21 de enero 2025.. https://www.eluniversal.com.mx/cartera/mexico-ocupa-el-tercer-sitio-en-la-region-por-ciberataques Consultado el 14 de abril de 2026.

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 del Banco de México, entre ellas las que realiza con propósitos de regulación monetaria y cambiaria, y como agente financiero del gobierno federal, cuya seguridad depende de la reserva de la información materia de la presente prueba de daño.

Lo anterior no es ajeno a la banca mundial, la cual es continuamente asediada por grupos denominados "hacktivistas", como ocurrió en junio de 2017, donde se pretendía inutilizar los sitios Web de los bancos centrales: "Anonymous anuncia 07 de junio como inicio de operación #OpIcarus 2017, cuyo objetivo son bancos centrales del mundo y otras instituciones financieras como la Reserva Federal y el Fondo Monetario Internacional en Estados Unidos. La operación iniciará mañana 07 de junio y tendrá una duración de 14 días, como protesta por las decisiones de los gobiernos de todo el mundo que no cumplen con las necesidades de la población."

Adicionalmente, si bien las afectaciones a la infraestructura de las tecnologías de la información y de comunicaciones pueden también deberse a riesgos inherentes a las mismas, es importante considerar que cuando estas afectaciones han ocurrido en el Banco de México, se ha generado alerta y preocupación de forma inmediata entre los participantes del sistema financiero; por lo que de presentarse afectaciones derivadas de ataques orquestados a partir de información de especificaciones o configuraciones de estas tecnologías, entregada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en las políticas que implementa el Banco y por ende en la economía, con lo que esto conlleva.

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 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; y en las órdenes de transferencia de fondos, podrían derivar en una pérdida de patrimonio no sólo para las instituciones financieras del país sino del propio banco central o el mismo gobierno federal.

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 por lo que, 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, 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, del sistema financiero 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.

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 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 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 y 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 la efectividad de las medidas adoptadas en materia cambiaria, 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 prevista en la Ley**, tal y como se demostró en el presente caso.

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 segundo, 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, 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, y los metadatos listados anteriormente***, 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

Accountability * Integrity * Reliability

GAO-10-230T

REFERENCIA 3

BadCyber

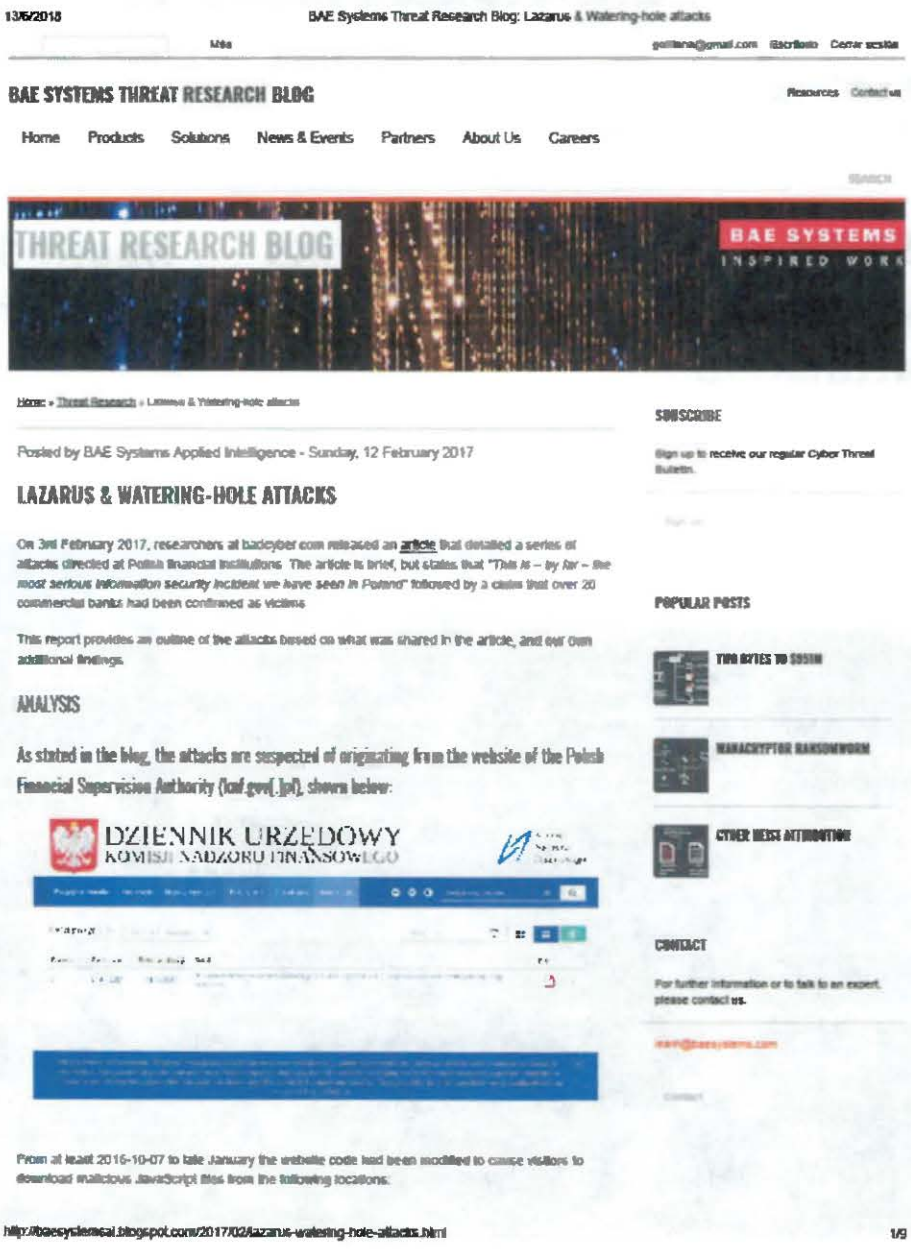
Making infosec journalism great again!

Several Polish banks hacked, information stolen by unknown attackers

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

241

REFERENCIA 4



13/6/2018 BAE Systems Threat Research Blog: Lazarus & Watering-hole attacks

BAE SYSTEMS THREAT RESEARCH BLOG

Home Products Solutions News & Events Partners About Us Careers

THREAT RESEARCH BLOG

BAE SYSTEMS INSPIRED WORK

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:

DZIENNIK URZĘDOWY KOMISJI NADZORU FINANSOWEGO

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:

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin.

POPULAR POSTS

TWO BYTES TO $953M

WANACRYPTOR RANSOMWORM

CYBER HEIST ATTRIBUTION

CONTACT

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

http://baesystemsai.blogspot.com/2017/02/lazarus-watering-hole-attacks.html 1/9

REFERENCIA 5

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. Mattei
Eastern Maine Medical Center
164 PUBLICATIONS 604 CITATIONS

SEE PROFILE

REFERENCIA 6

Ciudad de México a 10 de enero de 2018

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

REFERENCIA 7

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

REFERENCIA 8

BANCO DE MÉXICO

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 9

25 de Junio de 2020

Hackers piden cinco millones de dólares a Pemex en ciberataque

Los hackers dejaron una nota de rescate pidiendo 565 bitcoins, equivalente a cinco millones de dólares

12/11/2019 21:36 REUTERS / FOTO: PIXABAY

Referencia 10

Hackean página web de adquisiciones de la Secretaría de Salud

Latinus | mayo 27, 2020

La **página** de adquisiciones de la **Secretaría de la Salud** fue **hackeada** y no permite el acceso durante la mañana de este miércoles. Al entrar al sitio web, aparece un mensaje que indica **"agujeros de seguridad"**.

Desde la madrugada del miércoles algunos usuarios reportaron los fallos el sitio.

"Su sistema tiene algunos fallos, **fallos humanos** por encima de los técnicos. El administrador **no aprende de sus errores** ni los corrige", se lee en el mensaje del sitio web.

> Te recomendamos: Habrá diálogo y acuerdos con gobernadores por semáforo de reapertura, asegura AMLO

El mensaje incluye la figura de un dibujo con bigote y sombrero y un círculo coloreado que alude a la bandera de **Colombia**. Sin embargo, no se ha confirmado que el ataque provenga de dicho país.

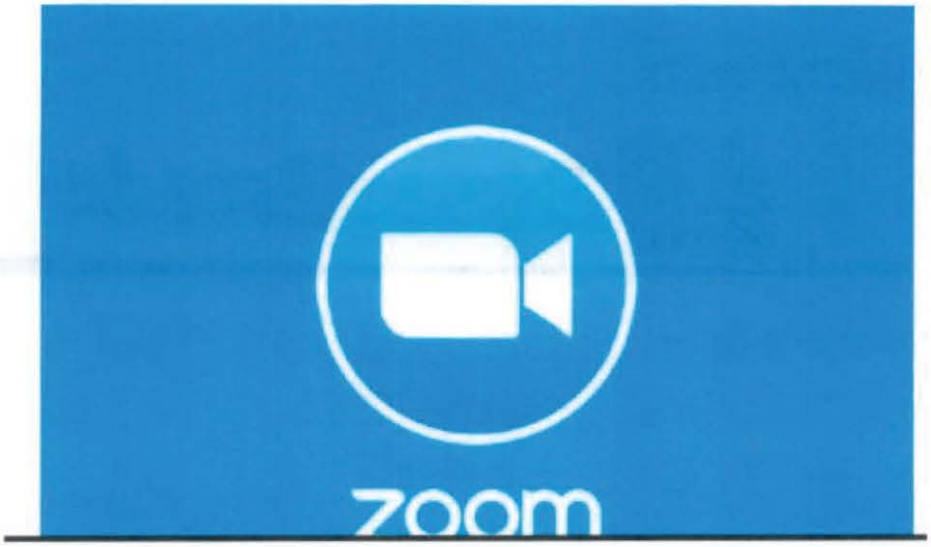
Referencia 11

FBI investiga a 'Zoom' por hackeo durante videoconferencias

Hace unos días fueron hackeadas varias conferencias realizadas en esta plataforma, las autoridades ya investigan

31/03/2020 14:55 AFP / FOTO: ZOOM

COMPARTIR SÍGUENOS



Referencia 12

EL ECONOMISTA | Banco estatal chileno cierra sucursales por ataque ciberné..

ENTIDAD YA INICIÓ ACCIONES LEGALES

Banco estatal chileno cierra sucursales por ataque cibernético

Si bien no se ha registrado afectación alguna a los fondos de sus clientes o al patrimonio de BancoEstado, el gobierno emitió una alerta al sector financiero para que tomen medidas ante el ransomware.

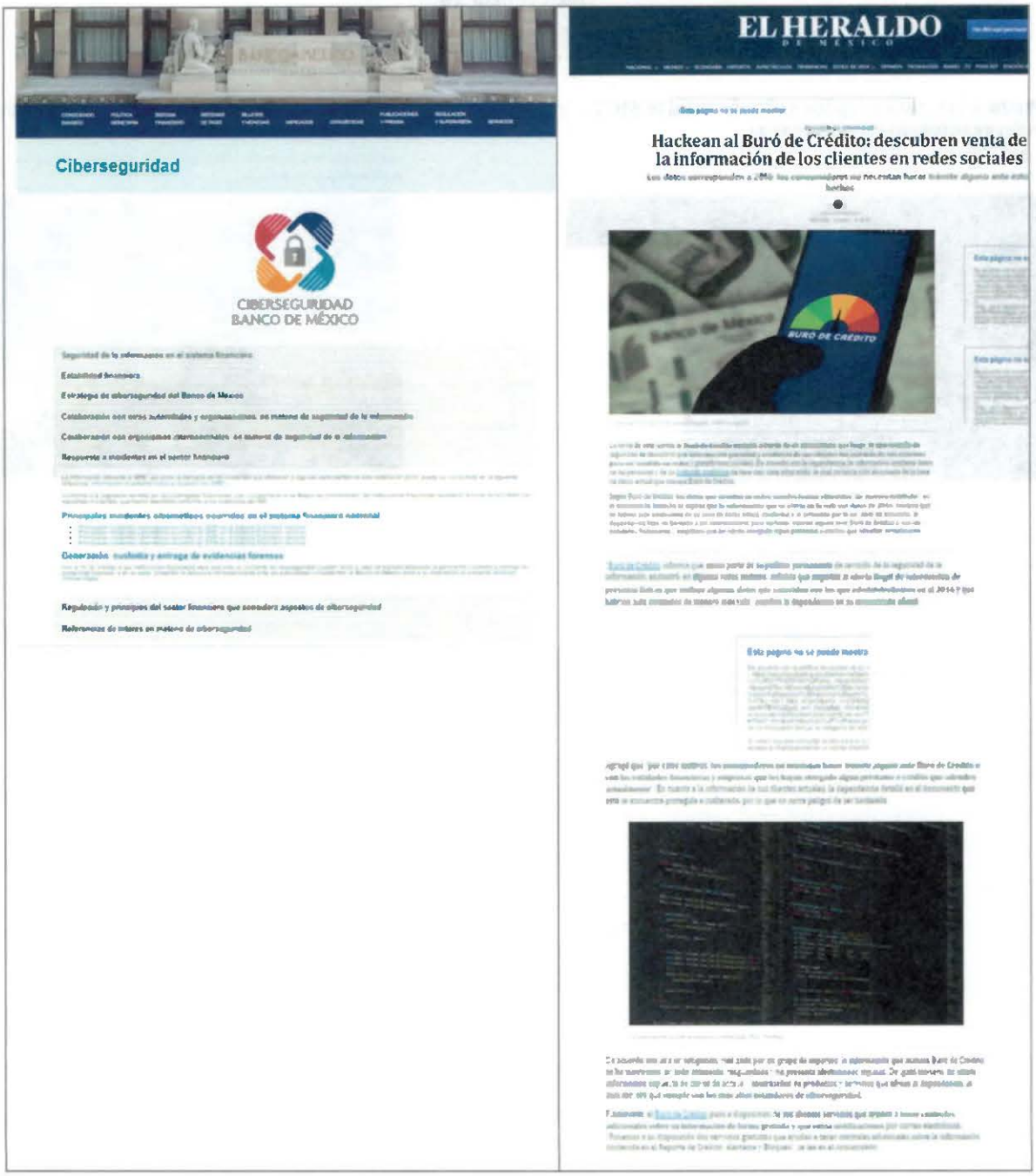
Diario Financiero / Chile
07 de septiembre de 2020, 22:47

Referencia 13

Alcanza a 110 computadoras hackeo en la SICT; prevén resolverlo en 2 semanas

SICT frena todos sus trámites hasta fin de año por el hackeo sufrido

Referencia 14



AFECTACIONES AL SPEI

El sistema financiero mexicano fue víctima de una campaña de ciberataques

Algunas instituciones del sistema financiero en México sufrieron una campaña de ciberataques, a principios del 2017, que afectó los aplicativos y la infraestructura de TI que dan soporte a los servicios de banca en línea.

Rodrigo Riquelme
15 de mayo de 2018, 16:34

REFERENCIA 16

México ocupa el tercer sitio en la región por ciberataques

Los ciberdelincuentes buscan engañar a la víctima para que realice una acción no deseada, como la descarga de malware en el equipo

CARTERA | 07/01/2021 | 14:20 | Actualizada 07/01/2021 14:20

Redacción
VER PERFIL

"ANEXO 7"

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

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 14 de abril 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. ***"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."***	**Plazo de reserva inicial:** 5 años, a partir del 15 de julio de 2021. **Plazo de reserva con ampliación:** 5 años, a partir del 16 de julio 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 insertasen[1].

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

En consecuencia, y considerando que, conforme a lo manifestado en la prueba de daño respectiva, la divulgación de la información correspondiente representa un riesgo de perjuicio significativo al interés público toda vez que: *"(…) pone en riesgo de destrucción, inhabilitación o sabotaje, infraestructura de tal importancia para la economía mexicana que su destrucción o incapacidad tendría un impacto negativo en la efectividad de las medidas adoptadas en los sistemas financiero, económico, cambiario o monetaria del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto, o bien pueda incrementar el costo de 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:

RESUELVE

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

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

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en la sesión celebrada el 02 de julio 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
NMDS
MDF

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
03/07/2026 15:52:20	Claudia Tapia Rangel	2bf0dc95aa900b7af83cc32da092cdf9dab87c36e881c3b45088297b7c9272dc
03/07/2026 15:58:46	EDGAR MIGUEL SALAS ORTEGA	9b477d6d3b9b72384e52d5088b592a2ebe46228e7bc6f2e23a882beaa821f5ba
03/07/2026 19:56:56	VICTOR MANUEL DE LA LUZ PUEBLA	e908487b8084b15999f5d0d3a380b1fa18ef830ef84ccee9b6a71fa13d683377

"ANEXO 8"

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

Ciudad de México, 14 de abril de 2026

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

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

TÍTULO DEL DOCUMENTO CLASIFICADO
Autorización para adjudicar directamente por materia identificado con el ID PAC: 21-0786 (800-21-0786-2)
Conformidad de excepción a la licitación pública para contratar los servicios de información financiera. Fecha 02 de marzo de 2021. (800-21-0786-2)
ORDER No. 24136216 (800-21-0786-2)
Dictamen de excepción para la contratación del servicio. Fecha 26 de febrero de 2021. (800-21-0786-2)

Al respecto, me permito resaltar que dicha clasificación fue confirmada por ese Comité mediante resolución de 15 de julio de 2021, emitida en la sesión Especial 23/2021, en términos de la fundamentación y motivación expresadas en el oficio de 09 de julio de 2021, suscrito por la Dirección de Operaciones Internacionales, 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 15 de julio de 2021 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **15 de julio 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 y 19, del Reglamento Interior del Banco de México (RIBM); así como Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, me permito informarles que esta unidad administrativa **estima que las causas para mantener clasificada como reservada la información referida en el presente oficio subsisten a la fecha, y lo seguirán al menos por los próximos 5 años adicionales, contados a partir de la citada fecha de expiración del plazo de reserva,** referida en el párrafo precedente.

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

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

Asimismo, informo que el personal que por la naturaleza de sus atribuciones tiene acceso a la referida información clasificada es el adscrito a:

Por parte de la DOI:

- Dirección de Operaciones Internacionales (Director)
- Gerencia de Análisis de Mercados Internacionales (Gerente)

Por parte de la DGTI:

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

Por parte de la DRM:

- 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

XIMENA ALFARACHE MORALES
Gerente de Operaciones Internacionales
En suplencia por ausencia del Director de Operaciones Internacionales, en términos del artículo 66 del Reglamento Interior del Banco de México

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.

Por lo que 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***, se clasifica 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 su destrucción o incapacidad tendría un impacto negativo en la efectividad de las medidas adoptadas en los sistemas financiero, económico, cambiario o monetaria del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto, o bien pueda incrementar el costo de 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 la infraestructura informática que soporta las operaciones cambiarias, monetaria y de agente financiero que realiza la banca central, lo**

cual posibilita la ejecución de acciones hostiles en contra de las tecnologías de la información de este Instituto Central, así como de las infraestructuras que éste administra, opera y supervisa, lo cual, podría menoscabar la efectividad de las mismas a tal grado, que su destrucción o inhabilitación afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero, económico y cambiario del país, arriesgando el funcionamiento de dichos 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 sus funciones de banca central. Las anteriores son finalidades y funciones que dependen en gran medida de la correcta operación de las tecnologías de la información y comunicaciones 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 cambiaria[1], 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.

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 propia 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

[1] Las políticas en materia cambiaria son decisión de la Comisión de Cambios.

todos sus recursos a ataques concretos 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.

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 necesarios 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 las infraestructuras que soportan las operaciones monetarias, ***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***, 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 éstas infraestructuras.

---

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

2. **Demostrable, ya que es un hecho notorio que los sistemas de los Bancos Centrales han sufrido ataques cibernéticos a través de estas infraestructuras,** como SWIFT, la cual ha sido utilizada para realizar robos de capital, uno de estos casos es el del Banco Central de Bangladesh, que sufrió un robo de 81 millones de dólares. 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. Respecto de lo anterior, a la fecha SWIFT continúa siendo objeto de ataques por diferentes grupos de delincuentes informáticos, y expertos en seguridad informática consideran que este tipo de actividades es susceptible de expandirse a otros servicios y sistemas financieros. Asimismo, los sistemas de empresas como Google, Facebook, PayPal y el New York Times se han visto comprometidos por ataques cibernéticos. 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. Esta serie de ataques se encuentra en una fase avanzada, que comenzó con ensayos desde 2017 y que ha logrado la consecución de sus objetivos en algunos casos. En todos ellos, la detección de vulnerabilidades a nivel aplicativo y sistema operativo son elementos en común, por lo cual es totalmente demostrable que el entregar información precisamente sobre las vulnerabilidades de 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, permitiría a los delincuentes o grupos delictivos el llevar a cabo más ciberataques que pudieran dañar de forma más severa las plataformas a través de las cuales se instrumentan las políticas monetaria y cambiaria, y las actividades de agente financiero del gobierno federal.

   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 polacos[3], el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada;[4]

   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;[5]

---

[3] 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 14 de abril de 2026.

[4] 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 14 de abril de 2026.

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

iii) La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público;

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

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.[7] 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.[8] El ataque producido a las plataformas que son usadas por proveedores externos en algunos bancos en México, en relación con el SPEI, ha sido catalogado como similar al que ocurrió con el sistema de pagos internacional S.W.I.F.T. en Rusia;

vi) La filtración a través de redes sociales de la base de datos de tarjetas de los clientes del Banco de Chile dada a conocer por el grupo de hackers llamado "TheShadowBrokers";

vii) La introducción a la red interna de Pemex de un ransomware el pasado 10 de noviembre de 2019, que forzó a la compañía a apagar equipos de cómputo de sus empleados en todo el país, inhabilitando, entre otros, el sistema de pagos de la empresa;[9]

viii) El Ataque al Sistema de Salud el 27 de mayo del 2020 que tuvo afectación en el sitio web de adquisiciones por un grupo de hackers;[10]

---

6 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 14 de abril de 2026.

7 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 14 de abril de 2026.

8 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/%7BB806F1E8-686D-B9F1-0452-EC375543C801%7D.pdf consultado el 14 de abril de 2026.

9 Excélsior, Hackers piden cinco millones de dólares a Pemex en ciberataque, 12 de noviembre de 2019. https://www.excelsior.com.mx/nacional/hackers-piden-cinco-millones-de-dolares-a-pemex-en-ciberataque/1347377 consultado el 14 de abril de 2026.

10 Latinus, "Hackean página web de adquisiciones de la Secretaria de Salud" 27 de mayo de 2020 https://latinus.us/2020/05/27/hackean-pagina-web-de-adquisiciones-secretaria-de-salud/ consultado el 14 de abril de 2026.

ix) Los ataques ocurridos a la aplicación de conferencias Zoom utilizada durante la pandemia de coronavirus cuyas reuniones han sido pirateadas;[11]

x) El hackeo al banco estatal chileno BancoEstado. La institución detecto un software malicioso en sus sistemas que afecto unos 12,000 equipos, incapacitando la operación obligando al cierre de sucursales, y[12]

xi) El hackeo a 110 computadoras de la Secretaría de Infraestructura, Comunicaciones y Transportes el pasado 24 de octubre con un virus tipo ransomware provocó que esa institución suspendiera la expedición de licencias federales y certificados en las diversas modalidades de transporte y de aviación civil hasta fines de 2022.[13]

En particular, respecto del sistema financiero mexicano, los ataques han sido focalizados a las tecnologías de la información de las instituciones pertenecientes al mismo y se han incrementado desde 2019. Destaca en el reporte sobre Principales incidentes cibernéticos relevantes ocurridos en 2022 en el sistema financiero nacional que han sido reportados al Banco de México la difusión no autorizada de información crediticia de clientes de una sociedad de información creditia.[14] Dicha situación demuestra la realidad e identificación del riesgo que representan los ataques cibernéticos en el sistema financiero mexicano, por lo que los programas que utiliza el Banco de México para interactuar con el mismo están en alto riesgo de ataques y deben reservarse los datos que, de difundirse, pudieran actualizar una vulneración.

Al respecto, 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,

---

[11] Excélsior "FBI investiga a "Zoom" por hackeo durante videocoferencias" 31 de marzo del 2020 https://www.excelsior.com.mx/hacker/fbi-investiga-a-zoom-por-hackeo-durante-videoconferencias/1373244 consultado el 14 de abril de 2026.

[12] El economista, Banco estatal chileno cierra sucursales por ataque cibernético, 07 septiembre 2020 https://www.eleconomista.com.mx/sectorfinanciero/Banco-estatal-chileno-cierra-sucursales-por-ataque-cibernetico--20200907-0122.html Consultado el 14 de abril de 2026.

[13] Forbes, "Alcanza a 110 computadoras hackeo en la SICT; prevén resolverlo en 2 semanas", Emmanuel Carrillo, octubre 25, 2022 @ 7:14 pm, https://www.forbes.com.mx/alcanza-a-110-computadoras-hackeo-en-la-sict-preven-resolverlo-en-2-semanas/ y "SICT frena todos sus trámites hasta fin de año por el hackeo sufrido", Forbes Staff, noviembre 1, 2022 @ 9:01 pm, https://www.forbes.com.mx/sict-frena-todos-sus-tramites-hasta-fin-de-ano-por-el-hackeo-sufrido/ ambos consultados el 14 de abril de 2026.

[14] El Banco de México publica un reporte anual acerca de los principales incidentes cibernéticos ocurridos en el sistema financiero nacional a través de la liga: https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html. Para más detalles, véase El Heraldo de México "Hackean al Buró de Crédito: descubren venta de la información de los clientes en redes sociales" Morales, Luz Elena, 2 de febrero de 2023 (disponible a través de la liga: https://heraldodemexico.com.mx/nacional/2023/2/2/hackean-al-buro-de-credito-descubren-venta-de-la-informacion-de-los-clientes-en-redes-sociales-478457.html). Ambos consultados el 14 de abril de 2026.

con el único objeto de conocer las vulnerabilidades de las instituciones, empresas, sistemas e infraestructura de tecnologías de la información.[15]

Por otro lado, es de destacar que los cibercriminales han utilizado técnicas de ingeniería social para obtener información y con ello acceder o vulnerar incluso los sistemas más seguros. Una de las formas más comunes de vulnerar los sistemas es mediante la obtención de información a través de diversas fuentes y mecanismos que les permita diseñar ataques informáticos encaminados a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros elementos, con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes. Al respecto, un análisis de la empresa ESET encontró que en 2020 se duplicaron las detecciones de ataques de ingeniería social en Latinoamérica donde Perú, Brasil y México como los países que registraron la mayor cantidad de detecciones de ataques. México tuvo el 16.94% de los ataques cibernéticos que recibió América Latina en el 2020, lo que coloca al país en el tercer sitio regional. Perú fue el país que registró el mayor porcentaje, con poco más del 31%, seguido por Brasil con más del 18%.[16]

Por lo anterior, **los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de componentes, arquitectura o configuración 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 su objetivo prioritario y 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 durante 2024, nuestros registros indican un promedio de 2,618 intentos de ataque al mes, llegando a presentarse hasta 10.464 intentos de ataques en el año. Si bien dichos ataques

---

[15] El Financiero, *El sistema financiero mexicano fue víctima de una campaña de ciberataques*, 15 de mayo de 2018. https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html Consultado el 14 de abril de 2026.

[16] El Universal, *México ocupa el tercer sitio en la región por ciberataques,* 21 de enero 2025.. https://www.eluniversal.com.mx/cartera/mexico-ocupa-el-tercer-sitio-en-la-region-por-ciberataques Consultado el 14 de abril de 2026.

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 del Banco de México, entre ellas las que realiza con propósitos de regulación monetaria y cambiaria, y como agente financiero del gobierno federal, cuya seguridad depende de la reserva de la información materia de la presente prueba de daño.

Lo anterior no es ajeno a la banca mundial, la cual es continuamente asediada por grupos denominados "hacktivistas", como ocurrió en junio de 2017, donde se pretendía inutilizar los sitios Web de los bancos centrales: "Anonymous anuncia 07 de junio como inicio de operación #OpIcarus 2017, cuyo objetivo son bancos centrales del mundo y otras instituciones financieras como la Reserva Federal y el Fondo Monetario Internacional en Estados Unidos. La operación iniciará mañana 07 de junio y tendrá una duración de 14 días, como protesta por las decisiones de los gobiernos de todo el mundo que no cumplen con las necesidades de la población."

Adicionalmente, si bien las afectaciones a la infraestructura de las tecnologías de la información y de comunicaciones pueden también deberse a riesgos inherentes a las mismas, es importante considerar que cuando estas afectaciones han ocurrido en el Banco de México, se ha generado alerta y preocupación de forma inmediata entre los participantes del sistema financiero; por lo que de presentarse afectaciones derivadas de ataques orquestados a partir de información de especificaciones o configuraciones de estas tecnologías, entregada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en las políticas que implementa el Banco y por ende en la economía, con lo que esto conlleva.

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 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; y en las órdenes de transferencia de fondos, podrían derivar en una pérdida de patrimonio no sólo para las instituciones financieras del país sino del propio banco central o el mismo gobierno federal.

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 por lo que, 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, 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, del sistema financiero 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.

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 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 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 y 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 la efectividad de las medidas adoptadas en materia cambiaria, 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 prevista en la Ley**, tal y como se demostró en el presente caso.

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 segundo, 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, 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, y los metadatos listados anteriormente***, 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

Accountability * Integrity * Reliability

GAO-10-230T

REFERENCIA 3

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 Share Tweet

REFERENCIA 4

13/6/2018 BAE Systems Threat Research Blog: Lazarus & Watering-hole attacks

BAE SYSTEMS THREAT RESEARCH BLOG

Home Products Solutions News & Events Partners About Us Careers

THREAT RESEARCH BLOG

BAE SYSTEMS INSPIRED WORK

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:

DZIENNIK URZĘDOWY KOMISJI NADZORU FINANSOWEGO

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:

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin.

POPULAR POSTS

TWO BITES TO $950

WANACRYPTOR RANSOMWORM

CYBER HEIST ATTRIBUTION

CONTACT

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

http://baesystemsai.blogspot.com/2017/02/lazarus-watering-hole-attacks.html 1/9

REFERENCIA 5

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

Article in World Neurosurgery · June 2017

DOI: 10.1016/j.wneu.2017.06.104

CITATION
1

READS
142

1 author:

Tobias A. Mattei
Eastern Maine Medical Center
164 PUBLICATIONS 604 CITATIONS

SEE PROFILE

REFERENCIA 6

80 AÑOS BANCOMEXT

Ciudad de México a 10 de enero de 2018

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

REFERENCIA 7

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

REFERENCIA 8

BANCO DE MÉXICO

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.**

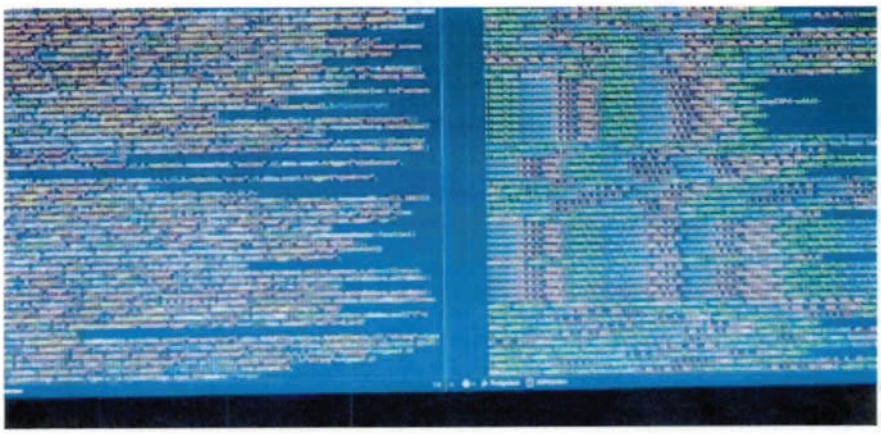
REFERENCIA 9

25 de Junio de 2020

Hackers piden cinco millones de dólares a Pemex en ciberataque

Los hackers dejaron una nota de rescate pidiendo 565 bitcoins, equivalente a cinco millones de dólares

12/11/2019 21:36 REUTERS / FOTO: PIXABAY



Referencia 10

Hackean página web de adquisiciones de la Secretaría de Salud

Latinus | mayo 27, 2020

Foto: Shutterstock

La **página** de adquisiciones de la **Secretaría de la Salud** fue **hackeada** y no permite el acceso durante la mañana de este miércoles. Al entrar al sitio web, aparece un mensaje que indica **"agujeros de seguridad"**.

Desde la madrugada del miércoles algunos usuarios reportaron los fallos el sitio.

"Su sistema tiene algunos fallos, **fallos humanos** por encima de los técnicos. El administrador **no aprende de sus errores** ni los corrige", se lee en el mensaje del sitio web.

> Te recomendamos: Habrá diálogo y acuerdos con gobernadores por semáforo de reapertura, asegura AMLO

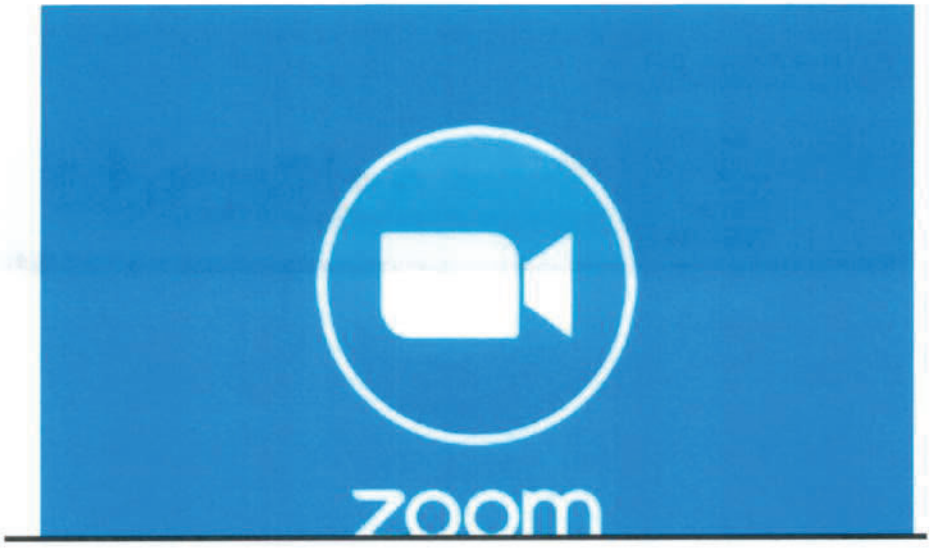
El mensaje incluye la figura de un dibujo con bigote y sombrero y un círculo coloreado que alude a la bandera de **Colombia**. Sin embargo, no se ha confirmado que el ataque provenga de dicho país.

Referencia 11

FBI investiga a 'Zoom' por hackeo durante videoconferencias

Hace unos días fueron hackeadas varias conferencias realizadas en esta plataforma, las autoridades ya investigan

31/03/2020 14:55 AFP / FOTO: ZOOM



Referencia 12

EL ECONOMISTA | Banco estatal chileno cierra sucursales por ataque ciberné..

ENTIDAD YA INICIÓ ACCIONES LEGALES

Banco estatal chileno cierra sucursales por ataque cibernético

Si bien no se ha registrado afectación alguna a los fondos de sus clientes o al patrimonio de BancoEstado, el gobierno emitió una alerta al sector financiero para que tomen medidas ante el ransomware.

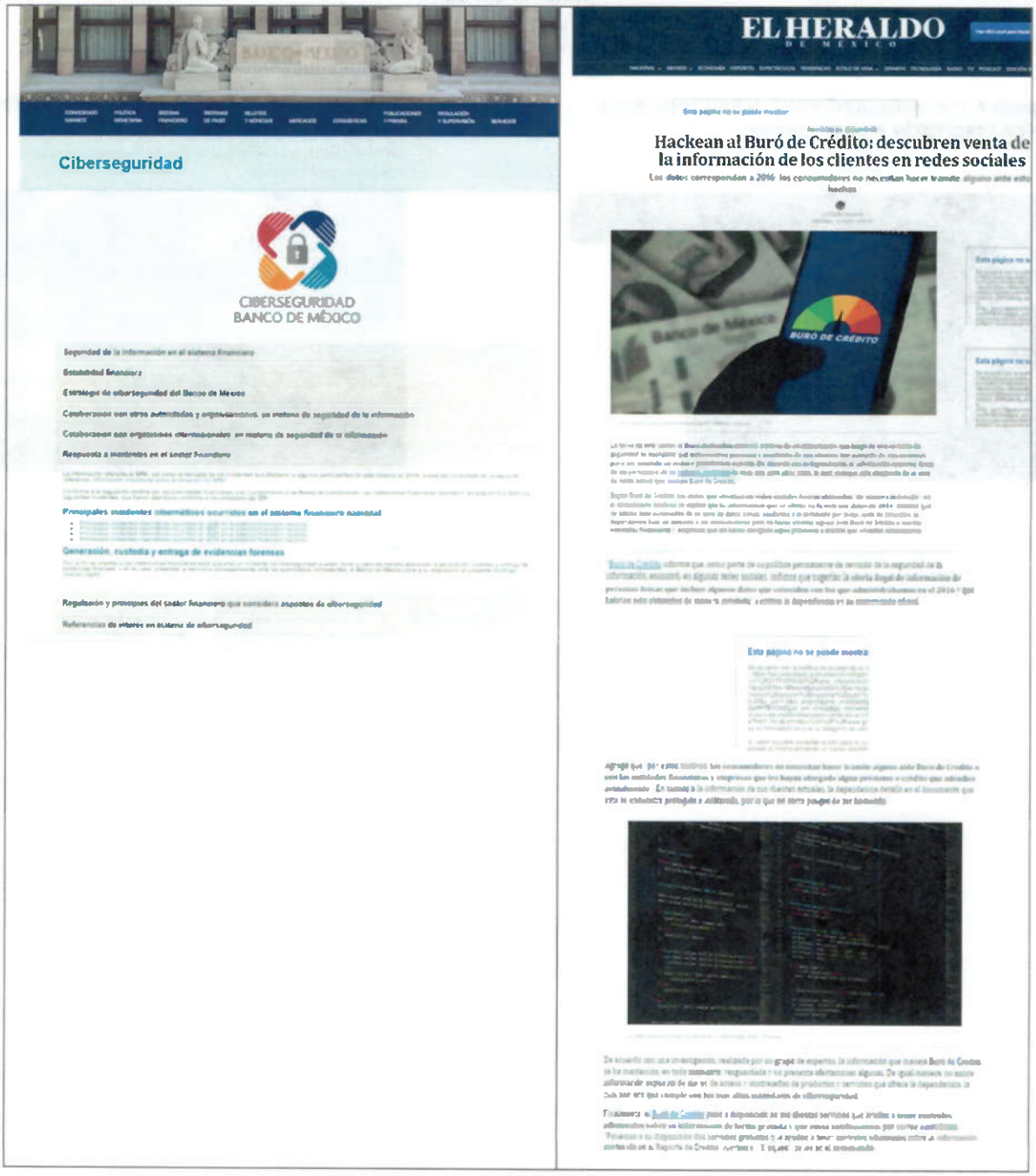
Diario Financiero / Chile
07 de septiembre de 2020, 22:47

Referencia 13

Alcanza a 110 computadoras hackeo en la SICT; prevén resolverlo en 2 semanas

SICT frena todos sus trámites hasta fin de año por el hackeo sufrido

Referencia 14



Ciberseguridad

CIBERSEGURIDAD
BANCO DE MÉXICO

EL HERALDO
DE MÉXICO

Hackean al Buró de Crédito: descubren venta de la información de los clientes en redes sociales

AFECTACIONES AL SPEI

El sistema financiero mexicano fue víctima de una campaña de ciberataques

Algunas instituciones del sistema financiero en México sufrieron una campaña de ciberataques, a principios del 2017, que afectó los aplicativos y la infraestructura de TI que dan soporte a los servicios de banca en línea.

Rodrigo Riquelme
15 de mayo de 2018, 16:34

REFERENCIA 16

México ocupa el tercer sitio en la región por ciberataques

Los ciberdelincuentes buscan engañar a la víctima para que realice una acción no deseada, como la descarga de malware en el equipo

CARTERA | 07/01/2021 | 14:20 | Actualizada 07/01/2021 14:20

Redacción
VER PERFIL

"ANEXO 9"

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

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 14 de abril de 2026.	Ximena Alfarache Morales (Gerencia de Operaciones Internacionales en suplencia por ausencia de quien es titular de la Dirección de Operaciones Internacionales del Banco de México.)	Ampliación del plazo de reserva de la información referida en el citado oficio.	**Información reservada** en términos de lo señalado en el oficio y en las pruebas de daño correspondientes. ***"Información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarías, 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."***	**Plazo de reserva inicial:** 5 años, a partir del 15 de julio de 2021. **Plazo de reserva con ampliación:** 5 años, a partir del 16 de julio 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 insertasen[1].

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

En consecuencia, y considerando que, conforme a lo manifestado en la prueba de daño respectiva, la divulgación de la información correspondiente representa un riesgo de perjuicio significativo al interés público toda vez que: *"(…) pone en riesgo de destrucción, inhabilitación o sabotaje, infraestructura de tal importancia para la economía mexicana que su destrucción o incapacidad tendría un impacto negativo en la efectividad de las medidas adoptadas en los sistemas financiero, económico, cambiario o monetaria del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto, o bien pueda incrementar el costo de 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:

RESUELVE

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

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

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en la sesión celebrada el 02 de julio 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
NMDS
MDF

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
03/07/2026 15:52:21	Claudia Tapia Rangel	efc2b35e6443164248cb0d6a84ddf3d6f6c3e239707bcaaff89d323fdf2f67f0
03/07/2026 15:58:49	EDGAR MIGUEL SALAS ORTEGA	88460d4a0fcc9b1ccefa0329c967aa36ffaa8f7b6dfa78ee70638de9c4f485c8
03/07/2026 19:57:00	VICTOR MANUEL DE LA LUZ PUEBLA	93992e022b93cefc07d2717b398270cb25f4c7567338ff1f3a7559e0d7982ed1

"ANEXO 10"

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

Ciudad de México, a 23 de junio de 2026

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

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

Sobre el particular, en relación con las referidas obligaciones de transparencia, les informamos 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 la prueba de daño correspondientes.

No.	TÍTULO DEL DOCUMENTO CLASIFICADO	TIPO DE CLASIFICACIÓN
1	Justificación de Marca Adobe (800-25-0174-1)	Confidencial y Reservada
2	Justificación de Marca Autodesk (800-25-0174-1).	Reservada
3	Justificación de marca de la suite de productos de software SAS. (800-25-0174-1)	Confidencial
4	Justificación de marca de "Jira Software" como herramienta para la gestión de requerimientos de software (800-26-0358-1).	Confidencial
5	Contrato No. 0000167902 (800-26-0349-1)	Reservada
6	Autorización para adjudicar sistema analizador forense (800-26-0349-1)	Reservada
7	Dictamen de excepción analizador forense (800-26-0349-1)	Reservada
8	Autorización para adjudicar contratación de sistema de protección (800-26-1324-1)	Reservada
9	Contrato No. 0000167885 (800-26-1324-1)	Reservada
10	Ratificación de marca y dictamen de excepción sistema de protección (800-26-1324-1)	Confidencial y 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:

Documentos clasificados	Personal de la Dirección General de Tecnologías de la Información con acceso a documentos clasificados
Justificación de Marca Adobe (800-25-0174-1)	• 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).
Justificación de Marca Autodesk (800-25-0174-1).	
Justificación de marca de la suite de productos de software SAS. (800-25-0174-1)	• Dirección de Desarrollo de Sistemas (Director) • Gerencia de Informática (Gerente) • Subgerencia de Desarrollo de Sistemas para Análisis de Información (todo el personal) • Subgerencia de Planeación y Regulación (todo el personal).
Justificación de marca de "Jira Software" como herramienta para la gestión de requerimientos de software (800-26-0358-1).	
Contrato No. 0000167902 (800-26-0349-1)	• Dirección de Seguridad y Organización de la Información (Director) • Gerencia de Seguridad de Tecnologías de la Información (Gerente) • Subgerencia del Centro de Defensa de Ciberseguridad (todo el personal) • Subgerencia de Planeación y Regulación (todo el personal).
Adjudicación (800-26-0349-1)	
Dictamen de Excepción (800-26-0349-1)	
Autorización para adjudicar contratación (800-26-1324-1)	
Contrato/Pedido No. 0000167885 (800-26-1324-1)	
Ratificación de marca y dictamen de excepción (800-26-1324-1)	

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

MOISÉS RIVERO VÁZQUEZ
Director de Desarrollo de Sistemas

ARTURO GARCÍA HERNÁNDEZ
Gerente de Seguridad de Tecnologías de la Información

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

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
25/06/2026 16:33:05	MOISES RIVERO VAZQUEZ	ecd8ece7f235e6a38dd9c544ffd0b53e2bfebfa5dea1c088f64d0332c789d158
25/06/2026 16:39:31	MARCOS PEREZ HERNANDEZ	736820a19f492b3c69f0028e5a4be98a3581bc34b91d52764da4067ed469ab59
25/06/2026 17:06:04	MARIA DEL CARMEN PRUDENTE TIXTECO	34430b7883b483f1e3e4790692463ea568adb43bfb1ca8e7ab451be6fcc70f88
25/06/2026 17:41:40	ARTURO GARCIA HERNANDEZ	fb06ae29918f27834c5f2252e6c74ece107ab068ddce605c2076bae9fe12b442

"ANEXO 11"

BANCO DE MÉXICO®

"2026, Año de Margarita Maza Parada"

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

OBLIGACIONES DE TRANSPARENCIA

Unidades Administrativas: Dirección de Infraestructura de Tecnologías de la Información, Dirección de Desarrollo de Sistemas, Gerencia de Seguridad de Tecnologías de la Información y Subgerencia del Centro de Defensa de Ciberseguridad, estas últimas, unidades administrativas adscritas a la Dirección de Seguridad y Organización de la Información, todas 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 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 23 de junio de 2026.	Marcos Pérez Hernández (Dirección de Infraestructura de Tecnologías de la Información), Moisés Rivero Vázquez (Dirección de Desarrollo de Sistemas), así como Arturo García Hernández (Gerencia de Seguridad de Tecnologías de la Información) y María del Carmen Prudente Tixteco (Subgerencia del Centro de Defensa de Ciberseguridad), estas últimas unidades administrativas	Confirmación de clasificación de información.	**Información confidencial** en términos de lo señalado en el oficio y en las carátulas correspondientes. Datos personales: • Datos identificativos: -Firma autógrafa de persona física -Nombre de persona física • Datos laborales: -Información laboral (puesto o cargo laboral). • Información protegida por el secreto comercial.	10 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: 02 de julio de 2031).

	adscritas a la Dirección de Seguridad y Organización de la Información, todas ellas del Banco de México.		**Información reservada** en términos de lo señalado en el oficio y en la prueba de daño correspondiente. "Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México"		

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

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 (LGPDPPSO).

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

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en la sesión celebrada el 02 de julio 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

NMDS
PAJC
MDF

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
03/07/2026 15:52:22	Claudia Tapia Rangel	6537037351fa5ffcbbe01fd1babad7c4d5bbce32a20a71977e0295de48abde12
03/07/2026 15:58:51	EDGAR MIGUEL SALAS ORTEGA	87ca8ab63b58daf861df57b5f717fa6e94540a4768d998dc0e3739dbd252d8a2
03/07/2026 19:57:04	VICTOR MANUEL DE LA LUZ PUEBLA	317f51a69dfc6f5bef662b82eb9ebd6c304ba17b934a5692c5201565eeb0b672