COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ORDINARIA 37/2021
DEL 9 DE SEPTIEMBRE DE 2021

A las trece horas del 9 de septiembre de 2021, participan en la presente sesión a través de medios electrónicos de comunicación Claudia Tapia Rangel, Titular de la Unidad de Transparencia, Erik Mauricio Sánchez Medina, Director Jurídico y Víctor Manuel De La Luz Puebla, Director de Seguridad y Organización de la Información, todos ellos integrantes del Comité de Transparencia, 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 siete de mayo de dos mil veinte (Reglas). Acto seguido, 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 43 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 64, párrafos segundo y tercero, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); 83 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 Quinta y Sexta de las Reglas. Por lo anterior, se procedió en los términos siguientes: ----------

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

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

Este Comité de Transparencia del Banco de México, con fundamento en los artículos 43, párrafo segundo, 44, fracción IX, de la LGTAIP; 64, párrafo segundo; 65, fracción IX, de la LFTAIP; 83 de la LGPDPPSO; 4o. y 31, fracciones III y XX, del RIBM, y Quinta, de las Reglas, por unanimidad, aprobó el orden del día en los términos del documento que se adjunta a la presente como **"ANEXO 1"** y procedió a su desahogo, conforme a lo siguiente: ----------

PRIMERO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA GERENCIA JURÍDICA CONSULTIVA Y DE LA SUBGERENCIA DE APOYO A LA FORMALIZACIÓN JURÍDICA DE ACTOS, UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN JURIDICA DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000029616. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de 6 de septiembre de 2021 suscrito por quien es titular de la Gerencia Jurídica Consultiva y de la Subgerencia de Apoyo a la Formalización Jurídica de Actos, unidades administrativas adscritas a la Dirección Jurídica del Banco de México, el cual se agrega a la presente acta como **"ANEXO 2"**, por medio del cual hicieron del conocimiento de este Comité de Transparencia su determinación de ampliar el periodo de reserva de la información señalada en dicho oficio, de conformidad con la fundamentación y motivación señaladas en el mismo y en la prueba de daño correspondiente, y solicitaron a este órgano colegiado confirmar dicha ampliación del periodo de reserva y aprobar la versión pública respectiva. ----------

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, 23, 43, 44, fracción VIII, de la LGTAIP; 1, 9, 64, 65 fracción VIII, de la

LFTAIP; 31, fracción IX, del RIBM; Quinta de las Reglas; resolvió aprobar la ampliación del periodo de reserva de la información referida, en términos de la resolución que se agrega a la presente acta como **"ANEXO 3"**. ----------

SEGUNDO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000021416.----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de 16 de julio de 2021 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 4"**, por medio del cual hicieron del conocimiento de este Comité de Transparencia su determinación de ampliar el periodo de reserva de la información señalada en dicho oficio, de conformidad con la fundamentación y motivación señaladas en el mismo y en la prueba de daño correspondiente, y solicitaron a este órgano colegiado confirmar dicha ampliación del periodo de reserva y aprobar la versión pública respectiva. ----------

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, 23, 43, 44, fracción VIII, de la LGTAIP; 1, 9, 64, 65 fracción VIII, de la LFTAIP; 31, fracción IX, del RIBM; 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"**. ----------

Al no haber más asuntos que tratar, se da por terminada la sesión en 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
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

SERGIO ZAMBRANO HERRERA
Secretario

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
09/09/2021 15:43:40	Claudia Tapia Rangel	dc11a1c73577d3dd1e5edcacc50175529c66b18b8dca0b74e583dc0c08093e6b
09/09/2021 16:34:02	SERGIO ZAMBRANO HERRERA	c53ac295b75ca7a8e981746f04c9a40b4d3a0f8f3d9b2a0e30d7c1cc349ae45c
09/09/2021 16:37:06	VICTOR MANUEL DE LA LUZ PUEBLA	89bbbcfe77161e779e6d4660acba85bedcabfff8d8b6667e96cbe95574ec88d4
09/09/2021 16:54:19	ERIK MAURICIO SANCHEZ MEDINA	c2a701a90f6631a1336e0ec387305df2822896ba8ba8c14a05e9c73b3522bf1c

"ANEXO 1"

BANCO DE MÉXICO®

"2021, Año de la Independencia"

COMITÉ DE TRANSPARENCIA

ORDEN DEL DÍA

SESIÓN ORDINARIA 37/2021
9 DE SEPTIEMBRE DE 2021

PRIMERO. SOLICITUD DE APROBACIÓN DE LA AMPLIACIÓN DEL PERIODO DE RESERVA DE INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA GERENCIA JURÍDICA CONSULTIVA Y DE LA SUBGERENCIA DE APOYO A LA FORMALIZACIÓN JURÍDICA, AMBAS UNIDADES ADMINISTRATIVAS ADSCRITAS A LA DIRECCIÓN JURÍDICA DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000029616.

SEGUNDO. 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, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000021416.

"ANEXO 2"

BANCO DE MÉXICO®

"2021, Año de la Independencia"

Ciudad de México, a 7 de septiembre de 2021

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

Nos referimos a la clasificación de reserva realizada, en su momento, para la atención de una solicitud de acceso a la información, por quienes eran los titulares de la Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales, unidad administrativa adscrita a la Dirección de Recursos Materiales, y de la Gerencia Jurídica Consultiva, unidad administrativa adscrita a la Dirección Jurídica, respecto de diversa información contenida en el documento que se señala en el siguiente cuadro:

TÍTULO DEL DOCUMENTO CLASIFICADO
"Contrato No. BM-SACRH-146-14-1, formalizado con Baker&Mckenzie, S.C., relativo a la realización de los servicios de acciones legales."

Al respecto, nos permitimos resaltar que dicha clasificación fue confirmada por ese Comité mediante resolución de **7 de diciembre de 2016**, emitida en la sesión 30/2016, en términos de la fundamentación y motivación expresadas en el oficio de fecha 5 de diciembre de 2016, suscrito por quien era el titular de la Dirección de Recursos Materiales, así como en la carátula y en la prueba de daño correspondientes.

Dicha clasificación se realizó por el periodo de 5 años contados a partir de la confirmación de la misma, lo cual ocurrió el 7 de diciembre de 2016 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **7 de diciembre de 2021.**

Sobre el particular, con fundamento en los artículos 101, párrafo tercero, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 99, párrafo tercero, de la Ley Federal de Transparencia y Acceso a la información Pública (LFTAIP); 2o., 3o. y 4o., de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero y tercero, y 10 del Reglamento Interior del Banco de México (RIBM); Segundo, fracción X, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como el Trigésimo Quinto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes (Lineamientos); nos permitimos informarles que estas unidades administrativas **estimamos que las causas para mantener clasificada como reservada la información referida en el presente oficio subsisten a la fecha, y es posible que sigan por los**

próximos 5 años, contados a partir de la citada fecha de expiración del plazo de reserva, referida en el párrafo precedente, o inclusive más allá de ese periodo.

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

Por lo expuesto, y con fundamento en los artículos 101, párrafo tercero, de la LGTAIP; 99, párrafo tercero de la LFTAIP; así como el Trigésimo Quinto y el así como Quincuagésimo sexto de los Lineamientos, **solicitamos atentamente a ese Comité de Transparencia confirme la ampliación del plazo de reserva de la información referida en el presente oficio, por 5 años más,** contados a partir de la fecha de expiración del plazo de reserva respectivo, y que apruebe la versión pública referida en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados Lineamientos, informamos que el personal que por la naturaleza de sus atribuciones tiene acceso a la referida información clasificada es el adscrito a: Dirección Jurídica (Director), Gerencia Jurídica Consultiva (Gerente), Subgerencia de Apoyo a la Formalización Jurídica de Actos (Subgerente, Abogado en Jefe y Abogado), Dirección de Recursos Materiales (Director), Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Gerente), Subgerencia de Programación de Contratación y Mejora Continua (Subgerente).

Atentamente

SEBASTIÁN ACOSTA GUEVARA	**ANA LUISA LEAL AGUIRRE**
Gerente Jurídico Consultivo	Subgerente de Apoyo a la Formalización Jurídica de Actos

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
07/09/2021 13:53:35	Ana Luisa Leal Aguirre	a387357ac0c812cc07ea636f6178aa2e7f1b212a4558213ee9f76d0f5bccd927
07/09/2021 14:03:48	SEBASTIAN ACOSTA GUEVARA	685d9fe70f71230108623cda159b21c99f0f678462af7b1b4a86747323f6b43e

"ANEXO 3"

BANCO DE MÉXICO®

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DEL PERIODO DE RESERVA

VISTOS, para resolver sobre la ampliación del periodo de reserva de información relativa a la solicitud cuyos datos se señalan a continuación, y

RESULTANDO

I. DATOS DE LA SOLICITUD

De conformidad a lo establecido en los artículos 122 y 123 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), el Banco de México recibió la solicitud de acceso a la información cuyos datos se indican en la tabla siguiente:

FOLIO:	**6110000029616.**
TRANSCRIPCIÓN PÚBLICA DE LA SOLICITUD:	
"Solícito copia de los anexos técnicos y contratos por adjudicación directa para contratación de abogados externos en los últimos 5 años".	

II. SOLICITUD DE LA UNIDAD ADMINISTRATIVA

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

FECHA DEL OFICIO	UNIDADES ADMINISTRATIVAS SOLICITANTES	SOLICITUD DEL OFICIO	INFORMACIÓN CLASIFICADA	VERSIONES PÚBLICAS	PLAZO DE CLASIFICACIÓN
Oficio de 6 de septiembre de 2021	Gerencia Jurídica Consultiva y Subgerencia de Apoyo a la Formalización Jurídica de Actos, ambas unidades administrativas adscritas a la Dirección Jurídica del Banco de México	Ampliación del plazo de reserva de la información referida en ese oficio.	**Información reservada en términos de la Prueba de daño:** "Particularidades del objeto de contratos, servicios contratados y datos que revelan estrategias Procesales."	"Contrato No. BM-SACRH-146-14-1, formalizado con Baker & Mckenzie, S.C., relativo a la realización de los servicios de acciones legales."	**Plazo de reserva inicial:** 5 años, a partir del 7 de diciembre de 2016. **Plazo de reserva con ampliación:** 5 años, a partir del 8 de diciembre de 2021.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva que soliciten los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 44, fracción VIII y 101 párrafo tercero de la LGTAIP; 65, fracción VIII y 99, párrafo

tercero de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); 31, fracción IX, del Reglamento Interior del Banco de México (RIBM), así como Trigésimo cuarto, párrafo tercero, y Trigésimo quinto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, vigentes (Lineamientos).

Asimismo, este órgano colegiado es competente para aprobar las versiones públicas que someten a su consideración, en términos del Quincuagésimo sexto y el Sexagésimo segundo, párrafos primero y segundo, inciso a), de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes (Lineamientos).

SEGUNDO. Este Comité de Transparencia, tomando en cuenta que en términos del Trigésimo quinto de los Lineamientos, corresponde a los titulares de las áreas de los sujetos obligados el fundar y motivar las razones que sustentan la solicitud de ampliación del periodo de reserva de la información que hubieran clasificado como reservada, 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 en el oficio referido en el resultando II, así como en la correspondiente prueba de daño, los cuales se tienen aquí por reproducidos como si a la letra se insertasen en obvio de repeticiones innecesarias.[1]

Al respecto, se comprobó que en dicha documentación 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, **este Comité confirma la ampliación al periodo de reserva de la información señalada** de conformidad con lo expresado en el oficio referido en el resultando II de la presente determinación, así como en términos de la prueba de daño correspondiente **y toma conocimiento del nuevo plazo de reserva determinado por las unidades administrativas.**

Asimismo, este órgano colegiado **aprueba la versión pública señalada en el oficio precisado en el resultando II de la presente resolución.**

Por lo expuesto con fundamento en los artículos 44, fracción VIII y 101, párrafo tercero, de la LGTAIP; 65, fracción VIII y 99, párrafo tercero, de la LFTAIP; y 31, fracción IX, del RIBM; Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

[1] Conforme a los principios de elaboración de sentencias en materia civil, de aplicación al presente procedimiento en términos de los artículos 7 de la LFTAIP y 2 de la Ley Federal de Procedimiento Administrativo, contenidos en la tesis *"SENTENCIA. CUANDO EL JUEZ CITA UNA TESIS PARA FUNDARLA, HACE SUYOS LOS ARGUMENTOS CONTENIDOS EN ELLA. Cuando en una sentencia se cita y transcribe un precedente o una tesis de jurisprudencia, como apoyo de lo que se está resolviendo, el Juez propiamente hace suyos los argumentos de esa tesis que resultan aplicables al caso que se resuelve, sin que se requiera que lo explicite, pues resulta obvio que al fundarse en la tesis recoge los diversos argumentos contenidos en ella."* (Suprema Corte de Justicia de la Nación; Registro digital: 192898; Instancia: Pleno; Novena Época; Materias(s): Común; Tesis: P./J. 126/99; Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo X, Noviembre de 1999, página 35; Tipo: Jurisprudencia).

RESUELVE

ÚNICO. Se **confirma la ampliación al periodo de reserva de la información referida como reservada** en el oficio mencionado en el resultando II de la presente determinación, conforme a la fundamentación y motivación expresadas en dicho oficio y en la prueba de daño referida, y se aprueba la versión pública respectiva, en términos del considerando Segundo de la presente resolución.

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en sesión celebrada el 9 de septiembre de 2021. ----------

COMITÉ DE TRANSPARENCIA

CLAUDIA TAPIA RANGEL
Integrante

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
09/09/2021 15:43:43	Claudia Tapia Rangel	84b8e2affbca3c3d84d620a06f7776753c40c87dc115cda24eb86882aea41a4e
09/09/2021 16:37:00	VICTOR MANUEL DE LA LUZ PUEBLA	cebde24afe7431111f7c5f5ff885602d30ded92ced9a9b55f000aae0d786a952
09/09/2021 16:54:28	ERIK MAURICIO SANCHEZ MEDINA	32a6ce11bc6bb6356945768faefe76e3262e587ea06a4f4457e21722aebd7a14

"ANEXO 4"

BANCO DE MÉXICO

Ciudad de México, a 16 de julio de 2021

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

Me refiero a la clasificación de reserva realizada, en su momento, para la atención de una solicitud de acceso a la información por la Dirección de Apoyo a las Operaciones, respecto de la información que se señala a continuación:

TÍTULO DEL DOCUMENTO CLASIFICADO
Pedido No. DRM-0000009419

Al respecto, me permito resaltar que dicha clasificación fue confirmada por ese Comité mediante resolución de 17 de octubre de 2016, emitida en la sesión 24/2016, en términos de la fundamentación y motivación expresadas en el oficio de 11 de octubre de 2016, suscrito por quienes eran titulares de la Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales y de la Subgerencia de Planeación y Regulación, ambas del Banco de México, en la carátula y en la prueba de daño contenida en la versión pública correspondiente, la cual se tiene por reproducida para los efectos del presente.

Dicha clasificación se realizó por el periodo de 5 años contados a partir de la confirmación de la misma, lo cual ocurrió el 17 de octubre de 2016 a través de la referida resolución, por lo que la fecha en que expira el referido plazo de reserva es el **17 de octubre de 2021.**

Sobre el particular, con fundamento en los artículos 101, párrafo tercero, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 99, párrafo tercero, de la Ley federal de Transparencia y Acceso a la información Pública (LFTAIP); 2o., 3o. y 4o., de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, y tercero, 10, párrafo primero, 12 y 19, del Reglamento Interior del Banco de México (RIBM); Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como el Trigésimo Quinto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes (Lineamientos); me permito informarles que esta unidad administrativa **estima que, en el presente caso, se acreditan las causas para mantener clasificada como reservada la información referida en el presente oficio, y lo seguirán al menos por los próximos 5 años, contados a partir de la citada fecha de expiración del plazo de reserva,** referida en el párrafo precedente.

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

Por lo expuesto, y con fundamento en los artículos 101, párrafo tercero, de la LGTAIP; 99, párrafo tercero de la LFTAIP; así como el Trigésimo Quinto y Quincuagésimo sexto de los Lineamientos, **solicito atentamente a ese Comité de Transparencia confirme la ampliación del plazo de reserva de la información materia del presente oficio, por 5 años más,** contados a partir de la fecha de expiración del plazo de reserva respectivo, y que apruebe la versión pública referida en el cuadro precedente.

BANCO DE MÉXICO

Asimismo, de conformidad con el Décimo de los señalados Lineamientos, informo que el personal que por la naturaleza de sus atribuciones tiene acceso a la referida información clasificada es el siguiente: Gerencia de Desarrollo de Sistemas Operativos (Gerente), Subgerencia de Servicios de Computo (Todo el personal)

Atentamente

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

BANCO DE MÉXICO
RECIBIDO
16 JUL 2021
Comité de Transparencia
Por: B12322 Hora: 10:30

BANCO DE MÉXICO

PRUEBA DE DAÑO

Información de la contratación de las tecnologías de información que soportan las operaciones cambiarias del Banco de México.

En términos de lo dispuesto en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 113, fracciones IV y VII de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), 110, fracciones IV y VII, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como, con el Lineamiento Vigésimo segundo, fracciones I y el Vigésimo sexto párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes (Lineamientos), podrá clasificarse como información reservada aquella cuya divulgación pueda 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 o, en su caso, de la economía nacional en su conjunto, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal, así como aquella que obstruya la prevención de los delitos, por lo que la ***Información de la contratación de las tecnologías de información que soportan las operaciones cambiarias del Banco de México***, 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 cambiarias que este Instituto Central lleva a cabo por cuenta propia o a nombre del Gobierno Federal, 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 y cambiario 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 realizan los sujetos obligados del sector público federal; asimismo, revelar dicha información obstruiría la prevención de delitos, toda vez que dicho riesgo es:

1. **Real**, en razón de que revelar o divulgar la *información de la contratación de las tecnologías de información que soportan las operaciones cambiarias del Banco de México*, tales como las especificaciones técnicas, los nombres de proveedores, el domicilio de los proveedores, 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 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 cambiarias que realiza éste por cuenta propia y a nombre del gobierno federal, son adquiridos, desarrollados o destinados para atender, entre otras, la implementación de la política en materia cambiaria[1], y para atender las funciones de agente financiero del gobierno federal. Por tal motivo, divulgar información relacionada con las especificaciones técnicas, nombres de proveedores, funcionamiento, 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 la política cambiaria y de agente financiero que realiza Banco de México.

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 cambiarias que realiza el Banco de México por cuenta propia y a nombre del Gobierno Federal.** Dichos ataques focalizados podrían tener mayor probabilidad de éxito debido a que los delincuentes tendrían la posibilidad de dedicar 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 cambiarias 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 el Instituto central lleva a cabo con propósitos de regulación cambiaria o las operaciones

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

cambiarias que realiza por cuenta propia en la administración de la reserva internacional y como agente financiero del gobierno federal. Una liquidación errónea derivada de una alteración en los sistemas que generan las órdenes de cobro o pago de las operaciones cambiarias que realiza el Banco por cuenta propia o a nombre del gobierno federal puede derivar en un incumplimiento involuntario de las obligaciones de estos organismos con el consecuente pago de penas, incremento en el costo de operaciones y daño en la confianza y reputación del Banco y del gobierno federal. De manera similar una interrupción o imposibilidad de ejecutar las subastas cambiarias que realiza el Banco Central por instrucciones de la Comisión de Cambios, generaría desconfianza, nerviosismo y especulación en el sistema financiero sobre la capacidad del Banco para operar en el mercado cambiario, originando presiones 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 cambiaria y comprometer la adecuada 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.

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 de proveedores, especificaciones respecto de los servicios prestados, 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 cambiarias, 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. **Demostrable, ya que es un hecho notorio que los sistemas de los Bancos Centrales han sufrido ataques cibernéticos a través de estas infraestructuras**, las cual han sido utilizadas 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 las infraestructuras continúan 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 y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, 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.

[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.

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]

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

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

---

[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 29 de enero de 2021.

[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 29 de enero 2021.

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

[6] BANCOMEXT. "Acción oportuna de BANCOMEXT salvaguarda intereses de clientes y la institución". 10 de enero de 2018. http://www.bancomext.com/comunicados/18443, consultado el 29 de septiembre de 2021.

[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 29 de septiembre de 2021.

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 ransomeware el pasado 10 de noviembre, 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]

Inclusive, uno de los *modus operandi* de los ciberataques es precisamente a través de la obtención de información pública, información fácilmente accesible o información inaccesible, lo cual puede ocurrir mediante solicitudes de acceso a la información, o bien, a través de las organizaciones que operan o tienen acceso a los sistemas, en complicidad o no, con el único objeto de conocer las vulnerabilidades de las instituciones, empresas, sistemas e infraestructura de tecnologías de la información.[10]

Por otro lado, es de destacar que los cibercriminales han utilizado técnicas de ingeniería social para obtener información y con ello acceder o vulnerar incluso los sistemas más seguros. Una de las formas más comunes de vulnerar los sistemas es mediante la obtención de información a través de diversas fuentes y mecanismos que les permita diseñar ataques informáticos encaminados a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros elementos, con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes. Las corporaciones multinacionales y las agencias de noticias han sido víctimas de sofisticados ataques dirigidos contra sus sistemas de información derivado de la aplicación de técnicas de ingeniería social.[11]

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**

---

[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 consultados el 29 de enero de 2021.

[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 29 de enero de 2021.

[10] 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 29 de enero de 2021.

[11] Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, 18 de diciembre de 2001. https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics consultado el 24 de septiembre de 2019.

cuyo rol no esté autorizado,[12] 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 2020, se registraron un promedio de 705 intentos de ataque al mes, llegando a presentarse hasta 1276 intentos de ataque en un único mes. Si bien dichos ataques no han logrado irrumpir en los sistemas del Banco de México, resulta claramente identificable que el objeto final de dichos ataques son los sistemas que soportan las operaciones del Banco de México, entre ellas las que realiza con propósitos de regulación 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

[12] Ver por ejemplo las 10 medidas básicas de ciberseguridad de la Security Information Center, en particular la relacionada con “Implementar un programa de capacitación en seguridad cibernética para empleados“ en donde recomiendan sensibilizar sobre los temas de ingeniería social que buscan obtener información mediante diversos canales de comunicación solicitando información sensible. https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_0.pdf consultado el 29 de enero de 2021.

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 la contratación de las tecnologías de información que soportan las operaciones cambiarias del Banco de México por cuenta propia y a nombre del Gobierno Federal, podría resultar en la afectación y alteración de las liquidaciones que este instituto lleva a cabo por cuenta propia y a nombre de terceros para cumplir con la implementación de la política cambiaria y con sus funciones 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 la política 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 soportan las operaciones cambiarias del Banco de México,* 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 cambiarias del Banco de México por cuenta propia y a nombre del gobierno federal 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 soportan las operaciones cambiarias del Banco de México* **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 de 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.

Por otra parte, se hace referencia a lo establecido en el artículo 70 de la LGTAIP, así como en la parte conducente de la LFTAIP, donde se contempla que los sujetos obligados, entre los cuales se encuentra el Banco de México, deberán poner a disposición del público y mantener actualizada diversa información, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, en los respectivos medios electrónicos, por lo menos, de los temas, documentos y políticas señalados en las fracciones I a XLVIII, de dicho artículo.

Cabe destacar que con la finalidad de establecer la forma en que los sujetos obligados deben dar cumplimiento al citado artículo 70 de la LGTAIP, el Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales (INAI), publicó en el Diario Oficial de la Federación de fecha 4 de mayo de 2016, el "*Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia*" (en lo sucesivo, Lineamientos Técnicos Generales).

En dichos Lineamientos Técnicos Generales, dentro de su anexo 1, se establecen los criterios sustantivos de contenido (metadatos)[13], en razón de la fracción correspondiente al artículo 70 de la LGTAIP, que los sujetos obligados deben publicar en los respectivos medios electrónicos a efecto de cumplir con las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la mencionada ley.

En tal virtud, debe destacarse que dichos metadatos comprenden información relativa al contenido de la contratación que se reserva con fundamento y motivación en las consideraciones vertidas en

[13] Los metadatos son " es el conjunto de datos que describen el contexto, contenido y estructura de los documentos de archivo y su administración, a través del tiempo, y que sirven para identificarlos, facilitar su búsqueda, administración y control de acceso" Fuente: Glosario - PNT (plataformadetransparencia.org.mx) , consultado el 15 de enero de 2021.

la presente prueba de daño, cuya publicación podría poner en riesgo la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto, puedan incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal, u obstruya la prevención de delitos, tal como se ha manifestado en la presente justificación.

En ese sentido, es evidente que las consideraciones formuladas en la presente prueba de daño respecto de la reserva de la contratación objeto de clasificación, son aplicables a los metadatos relativos a dichos documentos, por lo que son de clasificarse como reservados de conformidad con el artículo 113, fracción IV, de la LGTAIP, el cual dispone que: "como información reservada podrá clasificarse aquella cuya publicación pueda afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal".

En consecuencia, es claro que revelar la **información** contenida en los "metadatos" derivados de la ***Información de la contratación de las tecnologías de información que soportan las operaciones cambiarias del Banco de México,*** actualizan el supuesto previsto del artículo 113, fracción IV, de la LGTAIP, toda vez que contiene información cuya divulgación "pondría en riesgo la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, , o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal".

Adicionalmente, los Lineamientos Técnicos Generales permiten reservar esta información, publicando en la pestaña correspondiente del portal de Internet una leyenda con el fundamento legal que especifique la información se encuentra clasificada.

Por lo anterior, se clasifica como reservada la información contenida en los metadatos siguientes: Fracción XXVIII art. 70 de la LGTAIP: *Descripción de las obras, los bienes, servicios, requisiciones u orden de servicio contratados y/o adquiridos, Nombre completo o razón social de los posibles contratantes, Registro Federal de Contribuyentes (RFC) de las personas físicas o morales posibles contratantes, Nombre o razón social del adjudicado, Registro Federal de Contribuyentes (RFC) de la persona física o moral adjudicada, Hipervínculo en su caso, al (los) Informe(s) de avance físicos en versión pública si así corresponde, Hipervínculo, en su caso, al (los) Informe(s) de avance financieros, en versión pública si así corresponde, Hipervínculo al acta de recepción física de los trabajos ejecutados u homóloga.*, toda vez que al revelar dicha información al público en general, se pondrían en riesgo las funciones del Banco de México, el funcionamiento del sistema financiero y de la economía nacional en su conjunto.

Fracción XXXII art. 70 de la LGTAIP: *Nombre, denominación o razón social del proveedor o contratista, Estratificación, Origen del proveedor o contratista, País de origen si la empresa es una filial extranjera, Registro Federal de Contribuyentes (RFC) de la persona física o moral, Entidad federativa de la persona física o moral, El proveedor o contratista realiza subcontrataciones, Actividad económica de la empresa, Domicilio fiscal de la empresa, Domicilio en el extranjero, Nombre del representante legal de la empresa, Datos de contacto, Correo electrónico, Tipo de acreditación legal que posee, Dirección electrónica que corresponda a la página web del proveedor o contratista, Teléfono oficial del proveedor o contratista, Correo electrónico comercial del proveedor o contratista*, toda vez que al revelar dicha información al público en general, se pondrían en riesgo las funciones del Banco de México, el funcionamiento del sistema financiero y de la economía nacional en su conjunto.

En razón de lo anterior, y vistas las consideraciones expuestas en el presente documento, con fundamento en lo establecido en los artículos 6o., apartado A, fracciones I y VIII, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, segundo párrafo, 104, 105, 107, 108, último párrafo, 109, 113, fracciones IV y VII, y 114 de la LGTAIP; 97, 100, 102, 103, 110, fracciones IV y VII, y 111 de la LFTAIP, 1o., 2o. y 3o., fracción I, de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, y tercero, 10, párrafo primero, del Reglamento Interior del Banco de México; así como, así como Primero, Segundo, fracción XIII, Cuarto, Sexto, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, Vigésimo sexto, párrafo primero, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo de los Lineamientos, se clasifica como reservada, **por el plazo de 5 años a partir de la fecha de clasificación,** la ***información de las tecnologías de información que soportan las operaciones cambiarias del Banco de México,*** toda vez que el Banco Central continuará utilizando la infraestructura tecnológica protegida por la presente prueba de daño para el ejercicio de sus funciones, considerando que los periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones, se extienden a rangos de entre diez y quince años.

REFERENCIA 2

United States Government Accountability Office

GAO

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

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

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues

GAO-10-230T

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

Más goilliana@gmail.com Escritorio Cerrar sesión

BAE SYSTEMS THREAT RESEARCH BLOG

Resources Contact us

Home Products Solutions News & Events Partners About Us Careers

SEARCH

Home » Threat Research » Lazarus & Watering-hole attacks

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

LAZARUS & WATERING-HOLE ATTACKS

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

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

ANALYSIS

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

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

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin.

Sign up

POPULAR POSTS


TWO BYTES TO $951M


WANACRYPTOR RANSOMWORM


CYBER HEIST ATTRIBUTION

CONTACT

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

learn@baesystems.com

Contact

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

BANCO DE MÉXICO

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

BANCO DE MÉXICO

REFERENCIA 7

BANCO DE MÉXICO

REFERENCIA 8

BANCO DE MÉXICO

22 de mayo de 2018

Puntos Importantes sobre la Situación Actual del SPEI.

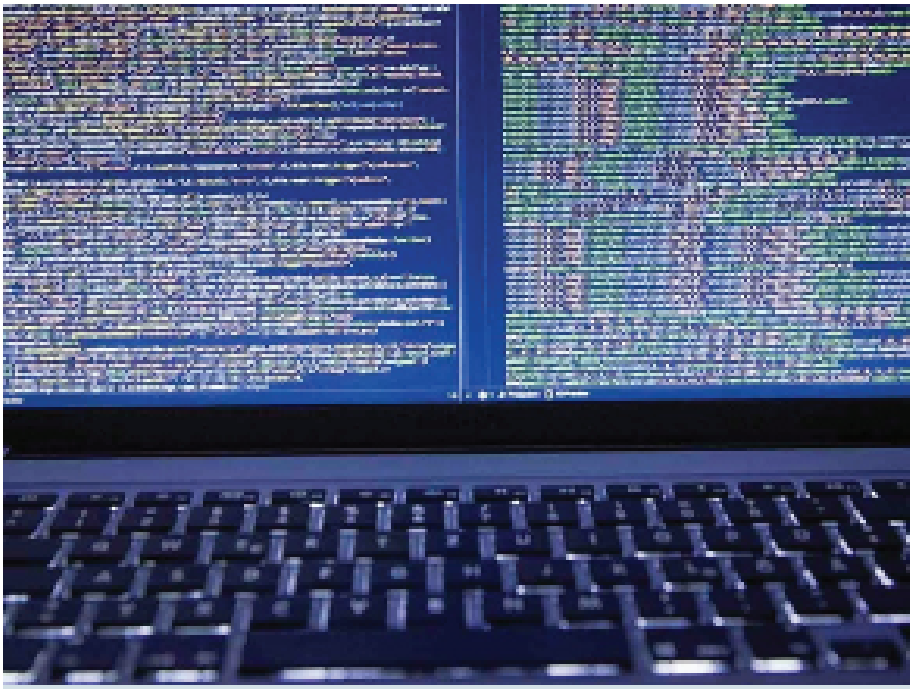
1. **Se tienen registrados 5 participantes con vulneraciones de ciberseguridad. Todos los ataques que se han observado han sido dirigidos hacia los bancos, casas de bolsa y otros participantes del sistema de pagos.** Estos han estado enfocados en los sistemas de los participantes con los que se conectan 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

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

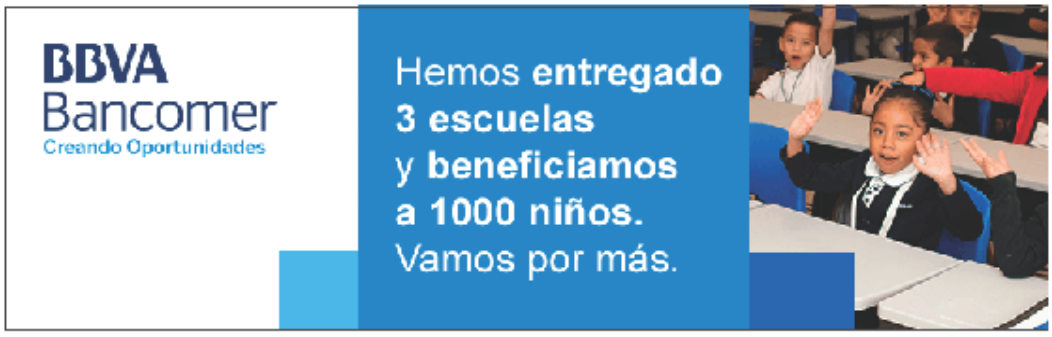
12/11/2019 21:36 REUTERS / FOTO: PIXABAY



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

BANCO DE MÉXICO

REFERENCIA 10



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 11

+2
2 Votes

Social Engineering Fundamentals, Part I: Hacker Tactics

By: ()

Created 18 Dec 2001 0 Comments

0 0

(http://en-us.reddit.com/submit?url=http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics)

(/connect/forward?path=node/1256241) Like 2

by Sarah Granger

Social Engineering Fundamentals, Part I: Hacker Tactics
by Sarah Granger (mailto:sarah@grangers.com)
last updated December 18, 2001

A True Story

One morning a few years back, a group of strangers walked into a large shipping firm and walked out with access to the firm's entire corporate network. How did they do it? By obtaining small amounts of access, bit by bit, from a number of different employees in that firm. First, they did research about the company for two days before even attempting to set foot on the premises. For example, they learned key employees' names by calling HR. Next, they pretended to lose their key to the front door, and a man let them in. Then they "lost" their identity badges when entering the third floor secured area, smiled, and a friendly employee opened the door for them.

The strangers knew the CFO was out of town, so they were able to enter his office and obtain financial data off his unlocked computer. They dug through the corporate trash, finding all kinds of useful documents. They asked a janitor for a garbage pail in which to place their contents and carried all of this data out of the building in their hands. The strangers had studied the CFO's voice, so they were able to phone, pretending to be the CFO, in a rush, desperately in need of his network password. From there, they used regular technical hacking tools to gain super-user access into the system.

BANCO DE MÉXICO

REFERENCIA 12

WaterISAC
Security Information Center

10 Basic Cybersecurity Measures

Best Practices to Reduce Exploitable Weaknesses and Attacks

June 2015

Developed in partnership with the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the FBI, and the Information Technology ISAC. WaterISAC also acknowledges the Multi-State ISAC for its contributions to this document.

"ANEXO 5"

BANCO DE MÉXICO®

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DEL PERIODO DE RESERVA

VISTOS, para resolver sobre la ampliación del periodo de reserva de información relativa a la solicitud cuyos datos se señalan a continuación, y

RESULTANDO

I. DATOS DE LA SOLICITUD

De conformidad a lo establecido en los artículos 122 y 123 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), el Banco de México recibió la solicitud de acceso a la información cuyos datos se indican en la tabla siguiente:

FOLIO:	**6110000021416.**
TRANSCRIPCIÓN PÚBLICA DE LA SOLICITUD:	
"Se solicita entregar en formato electrónico, copia de los contratos (incluyendo sus anexos técnicos) que haya celebrado la dependencia del 2013 a la fecha, cuyo objeto se encuentre relacionado con las tecnologías de la información (por ejemplo cómputo, impresión, energía, fotocopiado, centros de datos, digitalización, telecomunicaciones, red de datos, etc)".	

II. SOLICITUD DE LA UNIDAD ADMINISTRATIVA

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

FECHA DEL OFICIO	**UNIDAD ADMINISTRATIVA SOLICITANTE**	**SOLICITUD DEL OFICIO**	**INFORMACIÓN CLASIFICADA**	**VERSIONES PÚBLICAS**	**PLAZO DE CLASIFICACIÓN**
Oficio de 16 de julio de 2021	Dirección de Apoyo a las Operaciones del Banco de México.	Ampliación del plazo de reserva de la información referida en ese oficio.	**Información reservada en términos de la Prueba de daño denominada,** Información de la contratación de las tecnologías de información que soportan las operaciones cambiarias del Banco de México "Se eliminaron los elementos SWIFT a evaluar y la	"Pedido No. DRM-0000009419."	**Plazo de reserva inicial:** 5 años, a partir del 17 de octubre de 2016. **Plazo de reserva con ampliación:** 5 años, a partir del 18 de octubre de 2021.

			ubicación dónde se realizó el servicio.” “Nombre, domicilio, teléfono y correo de trabajo de la persona que recibe el entregable.”		

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para aprobar la ampliación del periodo de reserva que soliciten los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 44, fracción VIII y 101 párrafo tercero de la LGTAIP; 65, fracción VIII y 99, párrafo tercero de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); 31, fracción IX, del Reglamento Interior del Banco de México (RIBM), así como Trigésimo cuarto, párrafo tercero, y Trigésimo quinto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, vigentes (Lineamientos).

Asimismo, este órgano colegiado es competente para aprobar las versiones públicas que someten a su consideración, en términos del Quincuagésimo sexto y el Sexagésimo segundo, párrafos primero y segundo, inciso a), de los “Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas”, vigentes (Lineamientos).

SEGUNDO. Este Comité de Transparencia, tomando en cuenta que en términos del Trigésimo quinto de los Lineamientos, corresponde a los titulares de las áreas de los sujetos obligados el fundar y motivar las razones que sustentan la solicitud de ampliación del periodo de reserva de la información que hubieran clasificado como reservada, 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 en el oficio referido en el resultando II, así como en la correspondiente prueba de daño, los cuales se tienen aquí por reproducidos como si a la letra se insertasen en obvio de repeticiones innecesarias.[1]

Al respecto, se comprobó que en dicha documentación 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.

[1] Conforme a los principios de elaboración de sentencias en materia civil, de aplicación al presente procedimiento en términos de los artículos 7 de la LFTAIP y 2 de la Ley Federal de Procedimiento Administrativo, 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).

En consecuencia, **este Comité confirma la ampliación al periodo de reserva de la información señalada** de conformidad con lo expresado en el oficio referido en el resultando II de la presente determinación, así como en términos de la prueba de daño correspondiente **y toma conocimiento del nuevo plazo de reserva determinado por la unidad administrativa.**

Asimismo, este órgano colegiado **aprueba la versión pública señalada en el oficio precisado en el resultando II de la presente resolución.**

Por lo expuesto con fundamento en los artículos 44, fracción VIII y 101, párrafo tercero, de la LGTAIP; 65, fracción VIII y 99, párrafo tercero, de la LFTAIP; y 31, fracción IX, del RIBM; Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

ÚNICO. Se **confirma la ampliación al periodo de reserva de la información referida como reservada** en el oficio mencionado en el resultando II de la presente determinación, conforme a la fundamentación y motivación expresadas en dicho oficio y en la prueba de daño referida, y se aprueba la versión pública respectiva, en términos del considerando Segundo de la presente resolución.

Así lo resolvió, por unanimidad de sus integrantes, el Comité de Transparencia del Banco de México, en sesión celebrada el 9 de septiembre de 2021. ----------

COMITÉ DE TRANSPARENCIA

CLAUDIA TAPIA RANGEL
Integrante

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

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

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
09/09/2021 15:43:42	Claudia Tapia Rangel	2e4a187684866a5708b1ab3c6a85c69b53bfbbccc40133512234fa4def178752
09/09/2021 16:37:11	VICTOR MANUEL DE LA LUZ PUEBLA	5ab9825a2b494c20ea031154ba58c82457feb5f6342e4cf557bd15b33551dbbc
09/09/2021 16:54:24	ERIK MAURICIO SANCHEZ MEDINA	fe218ea0a191f46356e6cc03babe9cd97d15737929018cddeec499d0f70c90d7